AD-E501 531
Copy 315 of 317 copies

AD-A252 201

(2)

IDA PAPER P-2686

ATCCIS WORKING PAPER 25

TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs)

EDITION 3

DTIC
ELECTE
JUN 16 1992
S A D

T. F. Maggelet, *Project Leader*
R. P. Walker, *Principal Author*

January 1992

This document has been approved for public release and sale; its distribution is unlimited.

Prepared for

Office of the Assistant Secretary of Defense (C^3I)
(Theater and Tactical Command, Control and Communications)
and
Office of the Director of Information Systems for C^4,
Headquarters, Department of the Army

92-15376

Public release/unlimited distribution (20 April 1992).

92 6 12 036

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311-1772

IDA Log No. HQ 92-40762

DEFINITIONS

IDA publishes the following documents to report the results of its work.

Reports

Reports are the most authoritative and most carefully considered products IDA publishes. They normally embody results of major projects which (a) have a direct bearing on decisions affecting major programs, (b) address issues of significant concern to the Executive Branch, the Congress and/or the public, or (c) address issues that have significant economic implications. IDA Reports are reviewed by outside panels of experts to ensure their high quality and relevance to the problems studied, and they are released by the President of IDA.

Group Reports

Group Reports record the findings and results of IDA established working groups and panels composed of senior individuals addressing major issues which otherwise would be the subject of an IDA Report. IDA Group Reports are reviewed by the senior individuals responsible for the project and others as selected by IDA to ensure their high quality and relevance to the problems studied, and are released by the President of IDA.

Papers

Papers, also authoritative and carefully considered products of IDA, address studies that are narrower in scope than those covered in Reports. IDA Papers are reviewed to ensure that they meet the high standards expected of refereed papers in professional journals or formal Agency reports.

Documents

IDA Documents are used for the convenience of the sponsors or the analysts (a) to record substantive work done in quick reaction studies, (b) to record the proceedings of conferences and meetings, (c) to make available preliminary and tentative results of analyses, (d) to record data developed in the course of an investigation, or (e) to forward information that is essentially unanalyzed and unevaluated. The review of IDA Documents is suited to their content and intended use.

The work reported in this document was conducted under contract MDA 903 89 C 0003 for the Department of Defense. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 1992	Final

4. TITLE AND SUBTITLE
ATCCIS WORKING PAPER 25, TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs), EDITION 3

5. FUNDING NUMBERS
MDA 903 89-C-0003

T-J1-246

6. AUTHOR(S)
Robert P. Walker, Theodore F. Maggelet, Kevin J. Saeger, Sarah H. Nash, David A. Arthur

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street
Alexandria, VA 22311

8. PERFORMING ORGANIZATION REPORT NUMBER
IDA PAPER P-2686

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ASD (C3I)
Room 3D174, The Pentagon
Washington, DC 20301

Director, FFRDC Programs
1801 N. Beauregard Street
Alexandria, VA 22311

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Public release/unlimited distribution (20 April 1992)

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This paper is a reprint of a document prepared by IDA in support of the SHAPE-sponsored Army Tactical Command and Control Information System (ATCCIS) Phase III study effort for the year 2000 and beyond. The focus of the paper is on technical standards to support interoperability of command and control information systems (CCISs). The status of open commerical standards for eight service areas (as defined by the CIM Reference Model) is described using, where possible, generic CCIS requirements. This document is a major revision of Edition 2 (August 1990) and incorporates work conducted by IDA for the WWMCCS ADP Modernization program's generic architecture (IDA Paper P-2457, *A Survey of Technical Standards for CCISs*, September 1991).

This paper describes a methodology, using interoperability parameters, for identifying the technical standards that will be required to support implementation of the ATCCIS architecture and for assessing the degree to which existing and emerging international standards support ATCCIS requirements. Profiles of standards reflecting agreements on interoperability parameters are described. In addition, the report summarizes a wide range of US DoD architectures and reference models and provides examples of the use of commercial open standards in current and emerging CCISs.

14. SUBJECT TERMS
Army, Tactical Command and Control, Interoperability, NATO, SHAPE, Open Systems, Open Systems Interconnection (OSI), Portability, Standards, Profiles, GOSIP, Stacks, Options, Assessment, Data Communications, Data Transmission, Architectures, Reference Models, Data Management, Network Services, Operating System Interfaces, Security and Management Services, Data Interchange Formats, User Interfaces, Graphics, Programming Services, Application Interfaces.

15. NUMBER OF PAGES
733

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	Same as Report

IDA PAPER P-2686
ATCCIS WORKING PAPER 25

TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs)

EDITION 3

T. F. Maggelet, *Project Leader*
R. P. Walker, *Principal Author*
K. J. Saeger
S. H. Nash
D. A. Arthur

Accesion For
NTIS CRA&I
DTIC TAB
Unannounced
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1



January 1992

Public release/unlimited distribution (20 April 1992).



INSTITUTE FOR DEFENSE ANALYSES

Contract MDA 903 89 C 0003
Task T-J1-246

FOREWORD

The purpose of this paper is to make available substantive work done in response to a major interactive technical support activity. Specifically, this paper is a reprint of a working paper prepared[1] by the Institute for Defense Analyses (IDA) in support of the Supreme Headquarters Allied Powers Europe (SHAPE)-sponsored Army Tactical Command and Control Information System (ATCCIS) Phase III study effort. The contents of this document were developed and agreed to in the international ATCCIS forum. Comments from NATO and National Commands and Agencies were solicited and have been incorporated into this update of ATCCIS Working Paper 25 (WP25). In January 1992, the Working Paper was reviewed and approved by a panel of field-grade officers representing SHAPE, Allied Forces Central Europe (AFCENT), France, Germany, the Netherlands, the United Kingdom, and the United States. SHAPE has distributed this paper to all NATO nations and to those NATO commands and agencies that have expressed an interest in the ATCCIS study. Background information relating to the overall ATCCIS effort is contained in the Preface to this paper. It should be noted that Oxford English spelling conventions are used throughout the report in accordance with standing NATO guidelines.

This Third Edition of WP25 is a major revision of a previous edition provided in August 1990. The focus remains the identification of open standards that could be used to achieve interoperability of command and control information systems (CCISs). WP25 (Third Edition) has had significant contributions from the Services, Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Office (JIEO), and other organizations. In particular, it is the result of close coordination at IDA between support for ATCCIS and support (directed by Mr. James Robinette, DISA) for the WAM Target Architecture and applicable standards. The September 1991 version of IDA Paper P-2457, *A Survey of Technical Standards for Command and Control Information Systems*, incorporated (with substantial enhancements) almost all of the Second Edition (August 1990) of WP25, and in turn, the Third Edition of WP25 incorporates (with substantial enhancements) almost all of P-2457.

WP25 (Third Edition) has added new sections on ATCCIS (including a summary of the Phase II findings and the ATCCIS architecture), architectures and

---

1 This document was prepared in response to a request from the Office of the Assistant Secretary of Defense (C3I), Theater and Tactical Command, Control, and Communications under Contract MDA 903 89 C-0003, Task Order T-J1-246.

reference models in use in NATO and the United States, initiatives in the Nations (primarily the United States) to use open architectures and standards in CCISs, and profiles of open standards in example CCISs. The organization of the document (into eight service areas) is based on the Corporate Information Management (CIM) Reference Model. The document places increased emphasis on the use of profiles to achieve interoperability.

The Office of the Director of Information Systems for Command, Control, Communications and Computers (ODISC4), Headquarters Department of the Army, provides the U.S. delegate to the ATCCIS Permanent Working Group, which consists of military, technical, and analytical representatives from France, Germany, the United Kingdom, the United States, SHAPE, AFCENT, and SHAPE Technical Centre. The Command and Control Division, U.S. Army Combined Arms Command, provides military expertise; the U.S. Army Communications-Electronics Command and IDA provide technical expertise; and IDA provides analytical expertise in support of the U.S. contributions to the overall ATCCIS effort. ODISC4 also furnishes the U.S. delegate to the ATCCIS Steering Group, which provides overall direction and approval of the ATCCIS PWG work effort and includes representatives from the PWG Nations and Commands, plus Belgium, Canada, and the Netherlands, with additional representation (observers) from the Allied Data Systems Interoperability Agency (ADSIA), the NATO Communications and Information Systems Agency (NACISA), and the Tri-Service Group for Communications and Electronics (TSGCE). Further details concerning the ATCCIS Phase III effort can be found in the ATCCIS Project Brief and Work Plan.[2]

This document should be of primary interest to the combat development and system development communities of those U.S. Commands and Agencies whose focus is on longer term command and control requirements (i.e., the year 2000 and beyond).

The authors would like to acknowledge the following persons for contributions that are contained in Appendix C and provide examples of military initiatives to use open standards: Major Michael Mascarenas (USMC), Mr. Joseph Onufer (US Army CECOM), Mr. Henry Saphow (OPM FATDS, US Army), Mr. Stan Levine (OPM CHS, US Army), and Ms. Judy Simpson (LOGICON/Eagle Technologies).

---

2 See IDA Paper P-2673, *ATCCIS Phase III Project Brief and Work Plan*, December 1991, UNCLASSIFIED.

PREFACE

1. In 1978, NATO's Long Term Defense Plan (LTDP) Task Force on Command and Control (C2) recommended that an analysis be undertaken to determine if the future tactical Automatic Data Processing (ADP) requirements of the Nations, including that of interoperability, could be obtained at a significantly reduced cost when compared with the approach that has been adopted in the past. The Task Force also recommended that the analysis should determine whether tactical ADP systems could be developed according to technical standards prescribed by NATO and agreed upon by the Nations.

2. In early 1980 the then Deputy Supreme Allied Commander Europe initiated a study to investigate the possibilities of implementing the Task Force's recommendations. Three Nations, those with experience in fielding automated tactical command and control information systems, participated in Phase I of the study, with Supreme Headquarters Allied Powers Europe (SHAPE) as leader and coordinator. The study group reported, at the end of Phase I, that the Nations could increase interoperability and potentially reduce costs by using a common development approach.

3. The Army Tactical Command and Control Information System (ATCCIS) Phase II study, under the direction of a steering group chaired by SHAPE and consisting of representatives from the Central Region (CR) Nations and Allied Forces Central Europe (AFCENT), was established in 1984. Concurrently, a permanent working group (PWG) was formed, which consisted of military, technical, and analytical representatives from France, Germany, the United Kingdom, the United States, SHAPE and AFCENT, and technical support from SHAPE Technical Centre (STC) to progress the Phase II effort. The Phase II study effort commenced in January 1985 and finished in October 1990; it recommended that all NATO Nations, as well as the Allied Command Europe (ACE) Northern and Southern Regions, be invited to participate in a Phase III (Implementation) effort.

4. ATCCIS Phase III, sponsored by SHAPE, commenced in January 1992. The work of the PWG Operational Subgroup will support the Military Agency for Standardization (MAS) initiative to modernize critical C2-related STANAGs; the PWG Technical Subgroup will work in coordination with the Tri-Service Group on Communications and Electronics (TSGCE).

(This page intentionally left blank.)

CONTENTS

FOREWORD iii

PREFACE v

LIST OF FIGURES xxi

LIST OF TABLES xxiii

TECHNICAL STANDARDS FOR CCISs 1

1. INTRODUCTION 1

1.1 Derivation 1

1.2 Purpose 1

1.3 Scope 2

1.4 Information Sources 2

1.5 Methodology 3

1.5.1 Identifying Standard Services Required for Basic and Enhanced Interoperability 3

1.5.2 Identifying Base Standards 4

1.5.3 Assuring Coverage by Standards 5

1.6 Structure of the Paper 6

2. BACKGROUND ON THE ATCCIS ARCHITECTURE 9

2.1 Background for ATCCIS 9

2.1.1 ATCCIS Phase I and Phase II (1984-1990) 9

2.1.2 ATCCIS Objectives 9

2.1.3 ATCCIS Phase II Findings 11

2.1.4 ATCCIS Method of Work for Technical Analyses 13

2.2 Fundamental Concepts of the ATCCIS Architecture 14

2.2.1 Information Exchange 14

2.2.2 Information Models 15

2.2.3 Information Transfer 16

2.2.4 Transaction Processing 16

2.2.5 Support for Applications 16

2.2.6 Support for Human-Computer Interfaces (HCIs) 17

2.2.7 Information Exchange With Nonconformant Systems 17

2.3 Overview of the Architecture 17
2.4 ATCCIS Facilities 18
2.4.1 Basic and Application-Level Facilities 18
2.4.2 Other Facilities 19
2.4.3 Facilities and Operational Activities 19
2.4.4 Interaction Between Facilities 20
2.5 Ensembles and Components 20
2.5.1 Basic Ensemble 20
2.5.2 Interaction Between Ensembles 20
2.5.3 Components and Their Relationship to Ensembles 21
2.5.4 ATCCIS-Conformant Systems 22
2.5.5 System Management 23
2.6 The Four Basic Facilities 23
2.6.1 Data Management Facility (DMF) 23
2.6.2 Transfer Facility (TF) 25
2.6.3 Service Control Facility (SCF) 25
2.6.4 System Management Facility (SMF) 26
2.7 Application-Level Facilities 26
2.8 Other Facilities 26
2.8.1 MMI Service Facility (MSF) 26
2.8.2 Non-ATCCIS Input/Output Facilities (IOFs) 26
3. STANDARDIZATION PROCESS IN RELATION TO CCISs 29
3.1 Role of Interoperability in Future C2 Processes 29
3.2 Services Requiring Standardization for CCISs 29
3.3 Using Standards and Profiles to Specify Open Aspects of CCISs 31
3.4 Overview of the Standards in the Eight Service Areas 32
3.5 Limitations on the Role of Standards 32
3.6 Overview of the Standards Development Process 33
3.6.1 Role of Standards 34
3.6.2 Standards Organizations 35
3.6.3 Organizations Producing Standardized Profiles 39
3.7 Proposed Definitions for Terms Used in Standardization and CCIS Architectures 40
3.8 Assessments of Standards 40

4. ARCHITECTURES AND REFERENCE MODELS 43
4.1 OSI Reference Model 43
4.1.1 Basic Options in OSI Standards 44
4.1.2 Connection-Oriented and Connectionless-Oriented Transmission Modes 46
4.2 Military Requirements for OSI 49
4.3 NATO C3 Architecture 50
4.3.1 Relation to NATO C3 Master Plan 50
4.3.2 Background to the NATO C3 Architecture 50
4.3.3 Attributes of the NATO C3 Architecture 50
4.4 NATO Tactical Communications Architecture Post-2000 52
4.5 US DoD CIM Reference Model 54
4.6 Example Defense-Wide CCiS Architectures 57
5. DATA MANAGEMENT SERVICE STANDARDS 65
5.1 Requirements 65
5.1.1 Partitioned, Partially Replicated Database System 66
5.1.2 Conceptual Schema 66
5.1.3 Domains 66
5.1.4 Required Services 67
5.2 Standards for Database Services 68
5.2.1 ISO Reference Model for Data Management 68
5.2.2 Data Definition and Manipulation Language Standards 69
5.2.2.1 Database Language NDL 69
5.2.2.2 Database Language SQL 70
5.2.3 Remote Data Access (RDA) 72
5.2.4 Information Resource Dictionary System (IRDS) Standards 75
5.2.5 Conceptual Data Modelling Facility Standards 81
5.2.5.1 Conceptual Schema 81
5.2.5.2 Conceptual Schema Standardization 82
5.2.5.3 Conceptual Data Modelling Facility 83
5.2.5.4 Object-Oriented Database Support 84
5.2.5.5 Full Text Manipulation in Structured Data 84
5.2.6 Distributed Transaction Processing (TP) Standards 85
5.2.6.1 TP Reference Model 85
5.2.6.2 TP Requirements 85
5.2.6.3 TP Standards 85
5.2.6.4 TP New Work Items 87

5.2.7 Open Distributed Processing (ODP) Standards 88
5.2.8 Other Database Service Standards 91
5.3 Standards for Data Management 91
5.3.1 Data Element Standardization 91
5.3.2 Policy and Issues for Data Management 92
5.3.2.1 NACISC Policy on Data Management 92
5.3.2.2 ADSIA Recommendations on Data Management 93
5.3.2.3 NATO Interoperability Management Plan (NIMP) 94
5.3.2.4 SHAPE Policy 94
5.3.2.5 STC Work 94
5.3.2.6 NATO Publications on Data Management 95
5.3.2.7 Data Management Issues in EDI 96
5.3.3 Data Management for Distributed Applications 96
5.4 Assessment of Coverage by Standards 97
6. NETWORK SERVICE STANDARDS 101
6.1 Network Service Requirements 101
6.2 OSI Reference Model, Interworking, and Application Layer Structure 101
6.2.1 Status of OSI Reference Model, ISO 7498 102
6.2.2 Interworking of Lower Layers in OSI 103
6.2.3 Application Layer Concepts 105
6.2.3.1 ISO Studies on Application Layer 105
6.2.3.2 Application Layer Structure (ALS) 106
6.2.3.3 Extended ALS 107
6.2.4 Distributed Applications 108
6.3 Standards for Network Services 109
6.3.1 OSI Base Standards and Stacks of Standards 109
6.3.2 MHS and MOTIS 111
6.3.2.1 Message Handling Standards 111
6.3.2.2 MHS-1984 and MHS-1988 Profiles 112
6.3.2.3 ACP 123 Common Message Format 113
6.3.2.4 Manufacturing Message Specification (MMS) 114
6.3.3 File Transfer, Access, and Management (FTAM) 114
6.3.3.1 FTAM Standards 114
6.3.3.2 FTAM Options and Profiles 117
6.3.4 Directory 118
6.3.4.1 Directory Services and Models 118
6.3.4.2 Directory Standards 119
6.3.4.3 Enhancement to Directory Standards 120
6.3.4.4 Example Interoperability Parameters for Directory 123
6.3.5 Job Transfer and Manipulation (JTM) 124

6.3.6 Application Service Elements 125
6.3.6.1 Association Control Service Element (ACSE) 125
6.3.6.2 Commitment, Concurrency, and Recovery (CCR) 126
6.3.6.3 Reliable Transfer Service Element (RTSE) 127
6.3.6.4 Remote Operations Service Element (ROSE) 127
6.3.6.5 Remote Procedure Call (RPC) 128
6.3.7 Abstract Syntax and Basic Encoding Rules 131
6.3.7.1 Abstract Syntax Notation One (ASN.1) 131
6.3.7.2 Basic Encoding Rules (BER) 132
6.3.8 Other Standards 134
6.3.8.1 U.S. DoD Standards for Internetting Networks 134
6.3.8.2 Time Synchronization 136
6.3.8.3 Integrated Services Digital Network (ISDN) 137
6.3.8.4 Broadband ISDN 138
6.3.8.5 Asynchronous Transfer Mode (ATM) 139
6.3.8.6 Fiber Distributed Digital Interface (FDDI) 140
6.4 Assessment of Coverage by Standards 141

7. OPERATING SYSTEM INTERFACE SERVICE STANDARDS 145
7.1 Requirements 145
7.2 Standards for Operating System Services 145
7.2.1 POSIX 146
7.2.1.1 POSIX Development 146
7.2.1.2 POSIX Conformance Testing 149
7.2.2 Consortia Recommendations 150
7.2.3 Operating System Standards 151
7.3 Assessment of Coverage by Standards 152

8. SECURITY, MANAGEMENT, REGISTRATION, AND CONFORMANCE TESTING STANDARDS 153
8.1 Requirements for Security and OSI Management Services 153
8.2 Status of Standards for Security 153
8.2.1 Overview of Civil and Military Security Standards 153
8.2.2 Security Standards Work in ISO 154
8.2.2.1 Security Framework 156
8.2.2.2 Security Models 156
8.2.2.3 Requirements and Approaches for Security 159
8.2.2.4 FTAM Security 160
8.2.2.5 TP Security 160
8.2.2.6 ODA Security 161
8.2.2.7 Directory Security 161
8.2.2.8 Database Security 161

8.2.2.9 International Standardized Profile (ISP) Security 161
8.2.2.10 Proposed ASE for Security 162
8.2.2.11 Security Exchange Information 162
8.2.2.12 Additional Security Standards Work in ISO 163
8.2.3 Security Standards Work in NATO 164
8.2.3.1 TSGCE SG9 AHWG on Security 164
8.2.3.2 NOSA 164
8.2.4 Other Security Standards Work 165
8.2.4.1 Secure Data Network System (SDNS) 165
8.2.4.2 NIST Recommendations 166
8.2.4.3 ECMA Recommendations 167
8.2.4.4 IEEE Work on Secure Local Area Networks (LANs) ... 168
8.2.4.5 BLACKER 168
8.2.4.6 Computer Security (COMPUSEC) Guidance 169
8.3 Status of Standards for OSI Management 170
8.3.1 Development of OSI Management Standards 170
8.3.2 ISO Approach to OSI Management 170
8.3.2.1 Functional Areas 172
8.3.2.2 Focus on Managed Objects 172
8.3.2.3 Distributed Processing Aspects 173
8.3.2.4 Results of Work in OSI Management 173
8.3.2.5 Conformance 174
8.3.3 ISO Standards for OSI Management 175
8.3.3.1 Status of OSI Management Standards 175
8.3.3.2 New Work Items 177
8.3.3.3 Systems Management, DIS 10164 179
8.3.3.4 Major Remaining Issues for DIS 10164 181
8.3.3.5 Structure of Management Information 181
8.3.4 Telecommunication Management Network (TMN) 182
8.3.5 Military Concerns in Network Management 183
8.3.6 Quality of Service (QoS) 184
8.3.7 Special Interest Groups for OSI Management 186
8.3.8 ECMA Model for Management 186
8.4 Standards for Conformance Testing 187
8.4.1 PICS Proformas 191
8.4.2 Formal Description Techniques 191
8.4.2.1 Estelle 192
8.4.2.2 LOTOS 192
8.4.2.3 SDL 193
8.4.2.4 G-LOTOS 193
8.4.2.5 Z 194
8.4.3 Conformance Test Suites 194

8.5 Standards for Registration Authorities 195
8.6 Assessment 196
9. DATA INTERCHANGE SERVICE STANDARDS 197
9.1 Document Exchange 197
9.1.1 Office Document Architecture (ODA) and Interchange Format (ODIF) 198
9.1.2 Standard Generalized Markup Language (SGML) 201
9.1.3 Distributed Office Applications Model (DOAM) 204
9.1.4 Electronic Data Interchange (EDI) 205
9.1.5 Document Transfer and Manipulation (DTAM) 206
9.1.6 Document File and Retrieval (DTR) 207
9.1.7 Referenced Data Transfer (RDT) 208
9.1.8 DoD Document Exchange Standards 208
9.2 Graphical Data Exchange 210
9.2.1 Graphical Information Product Exchange 210
9.2.2 Standards for Graphics Services 212
9.2.2.1 Computer Graphics Reference Model 212
9.2.2.2 Computer Graphics Metafile (CGM) 212
9.2.2.3 Computer Graphics Interface (CGI) 213
9.3 Geographical Data Exchange 214
9.3.1 Digital Geographic Information Exchange Standard (DIGEST) 216
9.3.2 Geographic Document Architectures 218
9.3.3 SIMNET Common Geographic Data Model 218
9.3.4 IHO Committee for the Exchange of Digital Data (CEDD) 219
9.3.5 NATO Geographic Conference 220
9.3.6 Digital Chart of the World (DCW) 220
9.3.7 Vector Product Standard (VPS) 220
9.3.8 Spatial Data Transfer Specification (SDTS) 220
9.3.9 British Standard Specification for Geographic Information 221
9.4 Data Compression 221
9.5 Video Data Exchange 223
9.6 Audio Exchange Standards 224
9.7 Assessment of Coverage by Standards 225
10. USER INTERFACE SERVICE STANDARDS 227
10.1 Requirements for User Interface Services 227
10.2 Standards for User Interface Services 227

10.2.1 HCI Standards Organizations 228
10.2.2 Visual Display Terminal (VDT) 229
10.2.3 Virtual Terminal (VT) 230
10.2.4 Terminal Management (TM) 232
10.2.5 Status of X-Windows 233
10.2.6 User Interface Reference Models 234
10.2.7 OSF/MOTIF 236
10.2.8 OPEN LOOK 236
10.2.9 Form Interface Management System (FIMS) 237
10.3 Assessment 237
11. GRAPHICS SERVICE STANDARDS 239
11.1 Reference Model for Computer Graphics 239
11.2 Graphical Kernel System (GKS) 239
11.3 Programmer's Hierarchical Interactive Graphics System (PHIGS) 240
11.4 Assessment of Coverage by Standards 241
12. PROGRAMMING SERVICE STANDARDS 243
12.1 Requirements 243
12.2 Programming Languages 244
12.2.1 Ada Programming Language 244
12.2.1.1 Ada Programming Support Environment (APSE) 244
12.2.1.2 Common APSE Interface Set (CAIS) 244
12.2.2 Pascal Programming Language 245
12.2.3 C Programming Language 246
12.2.4 COBOL Programming Language 247
12.2.5 FORTRAN Programming Language 247
12.2.6 LISP Programming Language 247
12.2.7 BASIC Programming Language 248
12.3 Standards for Software Environments 248
12.3.1 Bindings 248
12.3.2 Software Engineering Environments 250
12.3.3 Knowledge-Based Systems (KBSs) 253
12.3.4 Software Repositories and Reuse 254
12.3.5 Process Models and Development Methods 254
12.4 Assessment of Coverage by Standards 256

13. APPLICATIONS AND APPLICATIONS PORTABILITY INTERFACES 259
13.1 Applications Portability 259
13.1.1 Requirements for Applications Portability 259
13.1.2.1 ISO 259
13.1.2.2 National Institute of Standards and Technology (NIST) 261
13.1.2.3 X/Open 262
13.1.2.4 Open Software Foundation (OSF) 262
13.1.3 Standards for Applications Portability 262
13.1.3.1 Interfaces for Applications Portability (IAP) 263
13.1.3.2 Example Model for the Open Systems Environment 264
13.1.3.3 NIST Applications Portability Profile (APP) 264
13.1.3.4 X/Open Common Applications Environment (CAE) 270
13.1.3.5 Open Software Foundation (OSF) Profiles 274
13.1.3.6 Technical and Office Protocol (TOP) 274
13.1.3.7 Multivendor Integration Architecture (MIA) 276
13.1.3.8 EWOS Profiles for the Open System Environment (OSE) 277
13.1.3.9 Unix International's ATLAS 278
13.2 Assessment 279
14. INTERNATIONAL AND NATIONAL STANDARDIZED PROFILES 281
14.1 Profiles of OSI Standards 281
14.1.1 Regional Workshops Developing OSI Profiles 281
14.1.2 International Standardized Profiles (ISPs) 282
14.1.2.1 Interchange Format and Presentation Profiles 284
14.1.2.2 Application Profiles 285
14.1.2.3 Transport Profiles 286
14.1.2.4 Relay Profiles 287
14.1.3 UK, US, and CA GOSIP 288
14.1.4 European Procurement Handbook for Open Systems (EPHOS) 292
14.1.5 International Versions of GOSIP 293
14.1.6 NATO GOSIP and NATO Standardized Profiles (NSPs) 293
14.1.7 Industry/Government Open Systems Specification (IGOSS) 294
14.1.8 Other Profiles and Transition Strategies 294
14.2 OSI Environments 295
14.2.1 ISO Development Environment (ISODE) 295
14.2.2 COS/COSINE Recommendations 295
14.3 Assessment of Coverage by Standards 296

15. STATUS OF NATO OSI DATA COMMUNICATIONS STANDARDS 297

15.1 Introduction 297

15.2 Military Requirements for NATO OSI 297

15.3 Organizational Responsibilities--TSGCE Subgroup 9 300

15.3.1 NTIS Transition and NOSIP Strategy 304

15.3.1.1 NTIS Transition Strategy 304

15.3.1.2 NATO Open Systems Interconnection Profile (NOSIP) 304

15.3.2 Status of Activities and Plans for Developing Lower Layer OSI STANAGs 305

15.3.2.1 Lower Layer STANAGs 306

15.3.2.2 Functional Profiles 306

15.3.2.3 NATO Standardized Profiles 307

15.3.2.4 NOSIP 307

15.3.2.5 Use of OSI in NATO 307

15.3.2.6 Multipeer Data Transmission 308

15.3.2.7 Multihoming 309

15.3.2.8 Multiendpoint Connection 309

15.3.2.9 Mobile Hosts 309

15.3.2.10 Lower Layer Addressing 310

15.3.2.11 Precedence and Preemption 310

15.3.2.12 Real-Time Programs 310

15.3.2.13 Glossary of NATO Data Communication Terms 310

15.3.2.14 Liaison With Other Groups 310

15.3.2.15 Work Plan 311

15.3.3 Status of Activities and Plans for Developing Upper-Layer OSI STANAGs 311

15.3.3.1 Proposed SG/9 Restructuring 312

15.3.3.2 Naming and Addressing 312

15.3.3.3 MMHS STANAG 4406 312

15.3.3.4 FTAM 312

15.3.3.5 Registration 313

15.3.3.6 Impacts of NATO GOSIP 313

15.3.3.7 Upper Layer Security 313

15.3.3.8 ISDN 313

15.3.3.9 Program of Work 313

15.3.3.10 Quality of Service 315

15.3.3.11 Conformance Testing 315

15.3.4 Nunn Initiatives and Work Plan of WG3 316

15.3.4.1 WG3 on Communications System/Network Interoperability (CSNI) 316

15.3.4.2 Media-Independent Data Link Architecture (MIDLA) ... 318

15.3.5 Status of Activities and Plans for Developing Network Management Standards 319

15.3.6 AHWG on ISDN 322
15.3.7 AHWG on Security 327
15.3.7.1 Major Security References 327
15.3.7.2 Layer 3 and Layer 4 Security Protocols 327
15.3.7.3 Security Activities 327
15.3.7.4 Security Support for CNSI 328
15.3.7.5 Work Plan for AHWG on Security 329
15.3.8 Status of Activities and Plans for Developing the Military Message Handling System (MMHS) for NATO 329
15.3.9 Status of Activities and Plans for Developing Data Link Standards for NATO 331
15.3.10 TSGCE SG9 Project Group on MIDS LVT 333
15.4 Status of NATO OSI STANAGs 333
15.4.1 Physical Layer STANAGs 335
15.4.2 Data Link Layer STANAGs 336
15.4.3 Network Layer STANAGs 337
15.4.4 Transport Layer STANAGs 341
15.4.5 Session Layer STANAGs 343
15.4.6 Presentation Layer STANAGs 344
15.4.7 Application Layer STANAGs 345
15.5 Development of Other Technical STANAGs 347
15.5.1 Network Independent Interface (NIIF) 347
15.5.2 Lightweight Protocols 348
15.5.3 EUROCOM and US/EUROCOM 349
15.5.4 Other Efforts 350
15.6 Assessment 350
16. NEAR-TERM INITIATIVES AND SYSTEMS FOR ACHIEVING INTEROPERABILITY IN NATO 353
16.1 TSGCE Work on Communications and Information Systems 354
16.1.1 Work of TSGCE SG11 on Communications 354
16.1.1.1 Organization of SG11 354
16.1.1.2 Activities of the Working Groups 355
16.1.1.3 Work of PG6 on Post-2000 Tactical Communications 355
16.1.2 Work of TSGCE SG12 on Information Systems 357
16.1.2.1 WG2 on Data Processing and Management 357
16.1.2.2 AHWG on ATCCIS 359
16.2 ACE ACCIS 360
16.3 Air Command and Control System (ACCS) 362
16.4 Battlefield Information Collection and Exploitation Systems (BICES) 365

16.5 NATO Maritime Operational Intelligence Support (NMOS) 365
16.6 Quadrilateral Interoperability Programme 366
16.7 Standard Automated Message Interface for NATO's ACCISs (STAMINA) 367
16.7.1 STAMINA Application Profile 369
16.7.2 STAMINA Transport Profiles 370
16.7.3 STAMINA Development Activities 371
17. NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS 373
17.1 Overview of National Initiatives to Implement OSI Standards in Military and Related Systems 373
17.1.1 France 373
17.1.2 Germany 377
17.1.3 The Netherlands 378
17.1.4 Netherlands, Norway, France, United Kingdom 379
17.1.5 United Kingdom 379
17.1.6 United States 382
17.2 Identification of Efforts to Evaluate the Performance of Civil Standards for Military Use 400
17.2.1 Sources of Reports on Performance Evaluations 400
18. CONCLUSIONS AND RECOMMENDATIONS 403
18.1 OSI Technical Standards 404
18.2 Other Technical Standards 405
18.3 Recommendations 405
Appendix A The Use of Interoperability Parameters to Ensure Standards Coverage A-1
Appendix B Functional Profiles Identified in the NTIS Transition Strategy B-1
Appendix C National Initiatives for Military Use of OSI Standards C-1
Appendix D International Civil Standards Relevant to CCISs D-1
Appendix E Numerical Listing of ISO Standards and CCITT Recommendations Relevant to CCISs E-1
Appendix F Organizations for Standardization F-1
Appendix G Status of Open Systems Standards Development in ISO/IEC G-1

Appendix H International Military and Other Standards Based on OSI Standards or Used in Profiles Open Systems H-1

Appendix I Background, Objective, and Statement of Work I-1

Appendix J Distribution List J-1

References References-1

Acronyms Acronyms-1

Index Index-1

(This page intentionally left blank.)

LIST OF FIGURES

Figure 1. Overview of the Methodology 3
Figure 2. Organization of Working Paper 25 7
Figure 3. Facilities of the Architecture 21
Figure 4. Classes of Standards and Their Relation to Groups of Standards 32
Figure 5. Flowchart of the ISO Standardization Process 36
Figure 6. Classes of Standards and Their Relation to Groups of Standards 41
Figure 7. The Seven-Layer Model for Open Systems Interconnection 43
Figure 8. Composition of an OSI System 44
Figure 9. The Role of a Relay 44
Figure 10. Post-2000 Tactical Communications Architecture-Extended LAS 53
Figure 11. The US DoD CIM Technical Reference Model 55
Figure 12. Services and Interface Connectivity 59
Figure 13. Stacks of Standards for Application and Transport Options 110
Figure 14. OSI Management Standards 171
Figure 15. A Model for the Open Systems Environment 266
Figure 16. An Example View of the Architecture for the Applications Portability Profile 267
Figure 17. Taxonomy for International Standard Transport Profiles 287
Figure 18. Stacks of Standards Recommended for UK GOSIP 290
Figure 19. Stacks of Standards Recommended for US GOSIP (Version 2.0) 291
Figure 20. RNLA Command Post Communication Network 378
Figure 21 RNLA C3 System Architecture 379
Figure 22. US Army Tactical Command and Control System (ATCCS) 389
Figure 23. US Army ATCCS Layered Software Reference Model 390
Figure 24. US Marine Tactical Command and Control System (MTACCS) 392
Figure 25. DoD Protocol Suite 397
Figure 26. US GOSIP Protocol Suite, Version 2 399
Figure 27. Proposed Mixed Protocol Suite 400

(This page intentionally left blank.)

LIST OF TABLES

Table 1. Listing of ATCCIS Papers 10

Table 2. Standards in the Eight Service Areas and Their Relation to ATCCIS 33

Table 3a. Definitions of Terms for Standardization and CCIS Architectures 40

Table 3b. Application, Transport, and Relay Options Offered by OSI Standards 45

Table 4. Proposed NATO Post-2000 Network Management Protocols 54

Table 5. Objectives and Principles for the CIM Technical Reference Model 56

Table 6a. WAM Target Profile 60

Table 6b. US DoD Common Operating Environment 62

Table 7. Status Overview of Key Data Management Standards 65

Table 8. New Work Items Proposed in ISO for TP 87

Table 9. Excerpts from the 1991 Working Paper by the NACISC on the Requirement for a NATO Data Management Policy 93

Table 10. Data Management Requirements Identified in ISO Relating to Data Structures and Data Models 97

Table 11. Status Overview of Key Network Service Standards 101

Table 12. Base Standards for Message Management 112

Table 13. Status Overview of Key Operating System Interface Standards 145

Table 14. POSIX Standards Being Developed by IEEE for Submission to ISO 146

Table 15. OSI Security Framework 157

Table 16. Security Protocols Developed in SDNS 166

Table 17. Definitions of OSI Management Functions From DIS 10164 180

Table 18. Status Overview of Key Data Interchange Standards 197

Table 19. Future Work on Office Document Architecture (ODA, ISO 8613) 199

Table 20. Status Overview of Key User Interface Standards 227

Table 21. Status Overview of Key Graphics Service Standards 239

Table 22. Status Overview of Key Programming Service Standards 243

Table 23. Standards for the Applications Portability Profile 267

Table 24. Applications Portability Standards 270

Table 25. Applications Portability Standards Being Developed by IEEE for Submission to ISO Through ANSI 271

Table 26. Standards for TOP Version 1.0 275

Table 27. Standards for TOP Version 3.0 275

Table 28. EWOS Profiles for the Open System Environment 278
Table 29. Overview of Taxonomy for International Standardized Profiles 285
Table 30. Standards for COSINE Profiles 296
Table 31. Eight Military Features for Enhancing OSI in NATO 298
Table 32. Impact of Military Features on Layers of OSI Reference Model 299
Table 33. Proposed Revised Military Features 300
Table 34. Proposed Revised Special Tasking Instructions for TSGCE SG9 303
Table 35. Work Plan and Activities on Lower Layer STANAGs by WG1 311
Table 36. Work Plan and Activities on Upper-Layer STANAGs by WG2 314
Table 37. Proposed Work Areas for CSNI in WG3 318
Table 38. Initial Approach to Military Features for ISDN 323
Table 39. Military Features for ISDN 324
Table 40. Initial Activities on ISDN 326
Table 41. Work Plan for the AHWG on ISDN 326
Table 42. Planned Activities for AHWG on Security 329
Table 43. Work Plan and Activities on MMHS 332
Table 44. SG9 Tasking Instructions for WG4 on Data Links 332
Table 45. NATO OSI Standards 334
Table 46. Areas of Deficiencies and Enhancements for STANAG 4253 337
Table 47. Military Enhancements Identified for Annex C of STANAG 4263 339
Table 48. Deficiencies and Enhancements Identified for STANAG 4254 342
Table 49. Deficiencies and Enhancements Identified for Annex C of STANAG 4264. 342
Table 50. Status of X.400(MHS)-1988 Relative to the Eight Military Features 346
Table 51. Proposed Tasking Instructions for SG12/WG2 on Data Processing and Management 360
Table 52. Standards for Quadrilateral Interoperability Programme 368
Table 53. Military Features Added to the STAMINA Specification 369
Table 54. Standards for STAMINA Transport Profiles 371
Table 55. French Army Standardized MHS Gateway 374
Table 56. US DoD (CIM) Assessment of Standards Availability 384
Table 57. US Navy Copernicus Architecture--Pillars, IERs, and Functions 393
Table 58. US Navy Copernicus Architecture--Functional Architecture 394
Table 59. US Air Force Software Architecture 395
Table 60. Summary of Standards in the Eight Service Areas and Their Relation to ATCCIS 403

ATCCIS Working Paper 25

TECHNICAL STANDARDS FOR CCISs

1. INTRODUCTION

1.1 Derivation

This paper derives from Working Paper (WP) 24 [Ref. ATCCIS 1988], which defines the basic concepts, logical elements (called facilities), and attributes of the architecture for the Army Tactical Command and Control Information System (ATCCIS), a common army command and control system concept for the year 2000 and beyond. The objectives of the ATCCIS architecture are to achieve interoperability through common standards and maintain the potential to reduce costs of future command, control, and information systems (CCISs), without unnecessarily restricting national options for implementation.

1.2 Purpose

The purpose of this working paper is to identify the technical standards that will be required to support implementations of the ATCCIS architecture. In this working paper, existing and planned standards appropriate to the ATCCIS facilities (and, more generally, the eight service areas common to many types of CCISs) are surveyed to the level of detail necessary to confirm a reasonable basis for the future support of the CCIS requirements. Relevant standards are identified, but no recommendations for selecting standards are considered. Gaps in current and planned standards coverage, which may require some developmental effort, are identified and are being passed to the appropriate standards defining body within NATO. WP 25 also offers guidance in ensuring adequate coverage by the set of standards employed at the time of implementation.

The ATCCIS architecture is one of the early attempts to completely define a CCIS architecture through the use of standards. It is not yet known to what degree international commercial standards can be made to satisfy CCIS requirements, but it is assumed that the extraordinary investments in open system standards during the 1980s and 1990s could have a major impact on the next generation of CCISs. As the Nations explore the use of these standards in their military and non-military systems, many of the practical issues not addressed in this paper will be resolved.

1.3 Scope

This working paper presents information and analyses that are intended to support implementation of the ATCCIS architecture, especially that minimum part of ATCCIS functionality called *Basic Interoperability*--the capability to allow two systems to exchange data and to preserve the meaning and relationships of the data exchanged.

WP 25 provides a broad overview of the existing and developing technical standards applicable to CCISs, specifically to automated CCISs. Very little of the work is specific to tactical CCISs. Further, many of the standards are applicable to many types of information systems and have been the attention of many national and international efforts to reduce acquisition costs of government- and industry-procured systems. An attempt has been made to discuss the standards in groups that are not specific to ATCCIS but that would apply to many types of CCISs.

The scope of the analysis of standards, which is the focal point of this paper, is broad, extending to international and national, commercial and military standards. However, the emphasis is on international commercial standards with military enhancements where required.

1.4 Information Sources

This assessment is based primarily on a review of standards for open systems developed by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telegraph and Telephone Consultative Committee (CCITT). Since ISO/IEC has decided to use the profiles of standards being developed by regional standards workshops, the primary sources for profiles are those workshops. Use of open systems standards in NATO is the responsibility of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 (SG9) on Data Distribution; thus, TSGCE SG9 draft STANAGs, *NATO Technical Interoperability Standards (NTIS) Transition Strategy* [Ref. NATO 1991], and working documents form the basis of the assessment of military use of open systems standards. Technical work on ATCCIS is being coordinated through the Ad Hoc Working Group (AHWG) on ATCCIS of TSGCE's SG12 on Information Systems.

The cut off date for information contained in Edition 3 of WP 25 is December 1991. The primary impact of the cut off date is that the progression of some standards to committee draft (CD), draft international standard (DIS), and international standard (IS or ISO) status may not be fully reflected herein.[1] Some aspects of the planned reorganization

---

[1] Significant contributions have been received from representatives to TSGCE, the British Standards Institute (BSI), the American National Standards Institute (ANSI), the US National Institute of Standards and Technology (NIST), OMNICON, and Technology Appraisals.

of TSGCE (e.g., approval of terms of reference for subgroups) will not be finalized until the January 1992 TSGCE plenary.

1.5 Methodology

This section describes the methodology employed to identify the group of existing and planned standards required to support ATCCIS functionality and to assess the completeness of standards coverage. The methodology is illustrated in Figure 1.

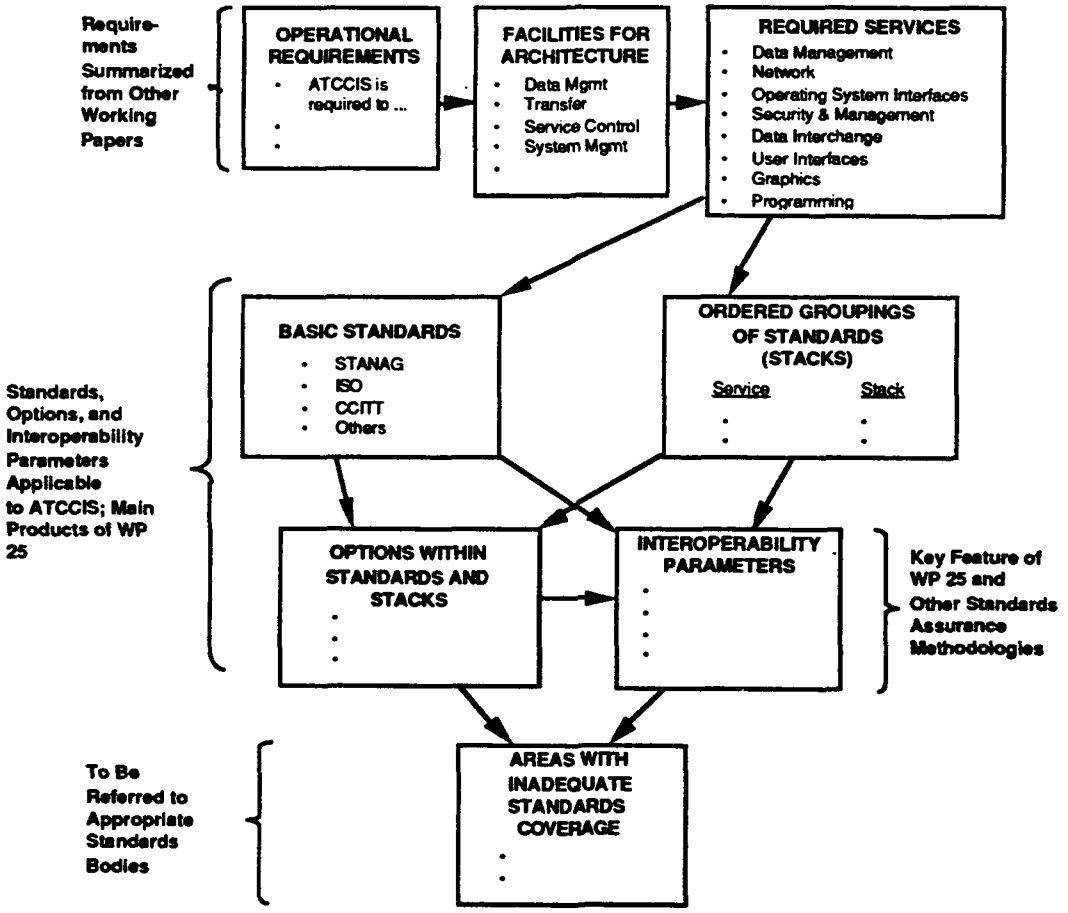


Figure 1. Overview of the Methodology

1.5.1 Identifying Standard Services Required for Basic and Enhanced Interoperability

The four ATCCIS facilities essential to basic interoperability identified for the ATCCIS architecture (see Chapter 2) are the Data Management Facility (DMF), the Transfer Facility (TF), the Service Control Facility (SCF), and the System Management Facility (SMF). These four "Basic Facilities" provide the three mechanisms necessary for basic interoperability: providing end-to-end transfer of data; managing the storage,

retrieval, and interpretation of data; and managing these mechanisms as the minimum capability to support basic interoperability.

The standards for CCISs addressed in this document are not limited to the Basic Facilities required for basic interoperability. Capabilities, such as portability of applications software, that support a more general concept of interoperability constitute *enhanced interoperability*. These are addressed in the ATCCIS architecture in such facilities as the Input/Output Facilities (IOFs) that provide interfaces to systems not conforming to the ATCCIS architecture; the Man-Machine Interface (MMI) Support Facility (MSF) that provides standard user interfaces, and Application-Level Facilities (ALFs) that provide common automated support for various command and control functions. (An overview of the features of the ATCCIS architecture is given in Chapter 2.)

Eight areas of services have been identified. Four of these groups are essential to basic interoperability and thus to the four basic facilities of the ATCCIS architecture: data management (ATCCIS DMF), network services for OSI (ATCCIS TF), operating system interfaces (ATCCIS SCF); and security and management (ATCCIS SMF and other facilities). Four others will provide for enhanced interoperability: data interchange formats (applicable to the DMF), user interfaces (applicable to the MSF), graphics (applicable to the MSF and ALFs), and programming services (applicable to ALFs). (Architectures and reference models relevant to the service areas are discussed in Chapter 4, standards for the eight service areas in Chapters 5-12, and interfaces for applications portability in Chapter 13.)

The ATCCIS architecture will be defined by adopting existing or emerging standards wherever and whenever possible. Further, when such a standard cannot be found ATCCIS will identify the requirement for a standard to be developed and will pass such a requirement to the appropriate standards defining body within NATO. Each facility in the ATCCIS architecture is a logical entity that provides a set of related services; implementation of a facility is not defined by the architecture and is a national responsibility for each system. This paper identifies standards (and options within standards) that are applicable to each facility, but the paper does not recommend any specific standard or groups of standards. Selection of appropriate standards, as well as the basic design choices implicit in the standards and options within standards, will be made by agreement prior to implementation decisions.

1.5.2 Identifying Base Standards

Following a review of the required services, the next step is to identify the base standards appropriate for each group of services. These standards may come from international, NATO, national military, or national non-military standards bodies, and they may be existing or planned. High-level options within standards applicable to CCISs are

identified. (Sources and the development process for international standards are discussed in Chapter 3.)

For many functions, there are several interrelated standards that must be used together to provide the required services. In most cases there is an order or hierarchy among these standards in which the lower levels are closer to physical means, and higher levels are associated with applications that are independent of the physical means. An ordered grouping of standards is called a stack. A profile is a stack of standards for which the interoperability parameters are partially or fully specified (profiles usually represent agreements among implementors). Where applicable to services required by CCISs, stacks will be constructed and illustrated in tables or figures.

1.5.3 Assuring Coverage by Standards

Assurance of adequate standards coverage is addressed in three ways. First, WP 25 checks for the existence of standards that generally support each specific ATCCIS function. Requirements for which no existing or planned standard seems to exist, or for which existing standards do not seem to be adequate, are identified so that these needs may be referred to the appropriate NATO standards defining body.

On a more specific level, a methodology for assuring adequate standards coverage through detailed analysis has been developed. An interoperability parameter approach is defined that begins with the identification of the system design parameters whose control is required to achieve interoperability. The assembled parameters act as a checklist for interoperability since each interoperability parameter must be controlled by a suitable standard. The purpose of an analysis using interoperability parameters is to recognize and examine all relevant quantities and characteristics in a direct manner, instead of assuming that existing or draft standards will provide adequate coverage of the quantities. Appendix A discusses this approach in more detail. NATO's TSGCE Subgroup 9 (SG9) and ISO/IEC have developed a format, called a standardized profile, for specifying stacks and interoperability parameters. Standardized profiles are discussed in Chapter 14, and examples are provided in Appendix B. The status of NATO work to address military deficiencies in open system standards (primarily for network services) is given in Chapter 15.

In the third step of the coverage analysis, the array of standards identified that could support ATCCIS is compared with plans for near-term efforts to check for completeness. Near-term efforts include: developing NATO C2 systems, such as the Air Command and Control System (ACCS), and conducting multilateral interoperability demonstrations, such as the Quadrilateral Interoperability Programme--these are discussed in Chapter 16. National initiatives for military use of OSI standards are reviewed in Chapter 17, and detailed examples are given in Appendix C. In addition to providing a check on completeness of ATCCIS applicable standards, some of these near-term efforts are of

interest because they represent transition strategies for moving to open environments for information processing and exchange.

1.6 Structure of the Paper

Chapter 2 provides background on the ATCCIS architecture. Chapter 3 provides an overview of the standardization process in relation to CCISs. Chapter 4 describes the major reference models and architectures essential to CCISs, including the reference model for open systems interconnection (OSI) that is the basis for most of the current international commercial data communications standards activities. Chapter 3 is essential to understanding the assessment, but the remaining chapters are generally independent and can be read in any order.

Figure 2 identifies the roles of each of the chapters. Chapters 5-8 address basic interoperability. Chapters 9-12 address enhanced interoperability. Chapter 13 describes the interfaces essential to ensuring that applications entities are, to the extent possible, independent of hardware. Chapter 14 summarizes international and national activities to develop profiles of standards in order to ensure common sets of interoperability parameters are selected for acquisition. The work in NATO and national military organizations to adopt, modify, and implement open systems standards are reviewed in Chapters 15-17. The conclusions and recommendations are provided in Chapter 18.

Several appendixes, some lengthy, are provided as reference material. Appendix A expands the discussion of the interoperability parameter methodology and applies the approach to some commonly used standards (RS-232, RS-423, STANAG 4202, and CCITT X.25). Appendix B summarizes the application, transport, and relay functional profiles identified for use in NATO. Appendix C provides examples of profiles of national initiatives to address the military use of OSI standards. A compilation of technical standards being developed by ISO and CCITT is given in Appendixes D and E, the former listed by layer of the OSI Reference Model and the latter listed numerically. Appendix F identifies the role and (in some cases) the standards responsibility of international and national, both civil and military, standards bodies. Appendix G provides some detailed information on the work plans for one of the major subcommittees (SC21) of the Joint Technical Committee Number 1 (JTC1) of ISO and IEC. Finally, Appendix H identifies STANAGs and other military and commercial standards being developed for use in open systems. An index is provided to assist the reader in locating information on specific topics and standards.

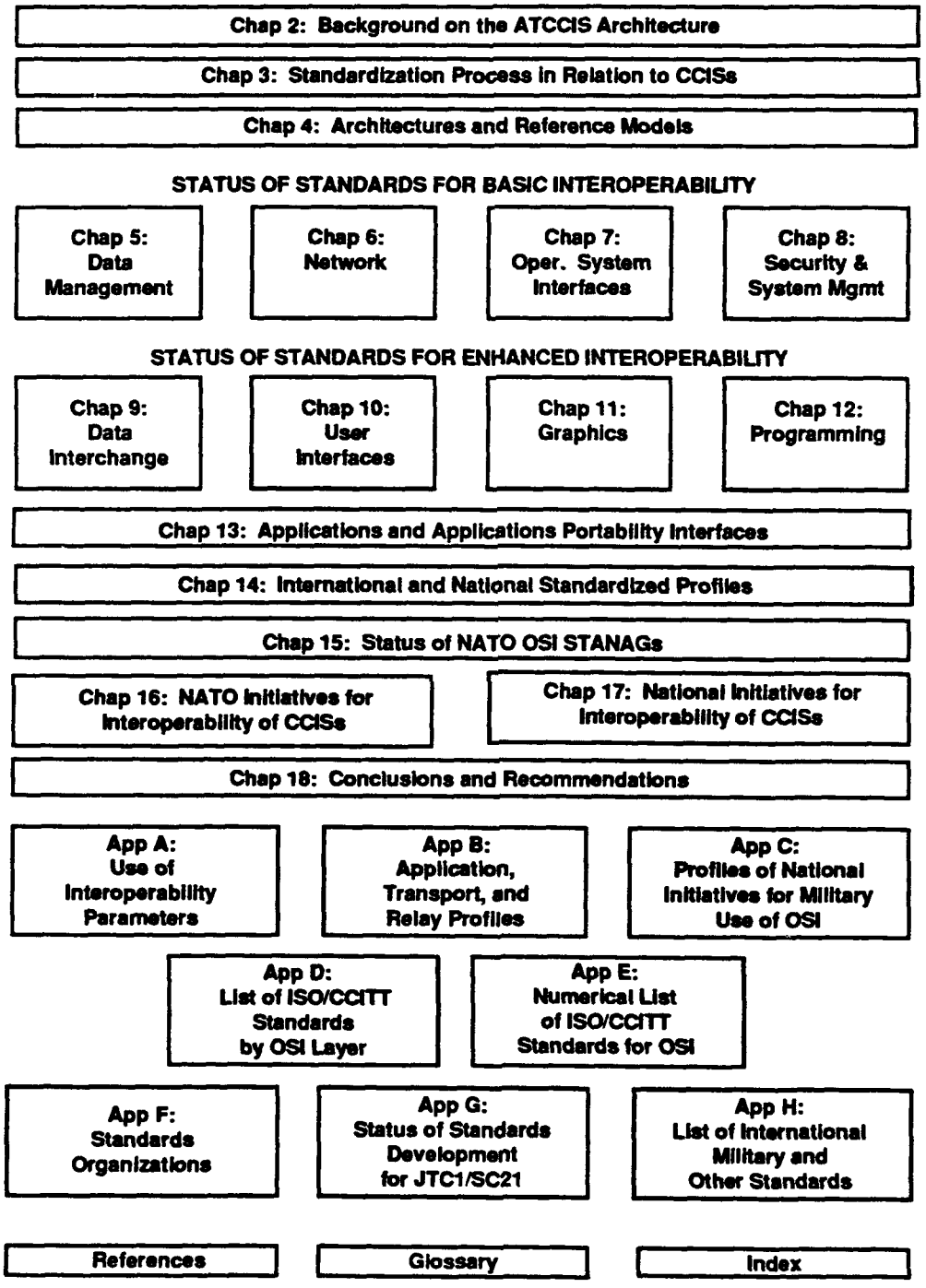


Figure 2. Organization of Working Paper 25

(This page intentionally left blank.)

2. BACKGROUND ON THE ATCCIS ARCHITECTURE

The purpose of this chapter is to provide a technical overview of the ATCCIS architecture. However, this information is not required to understand the review of standards that follows. For more information on ATCCIS, the reader should first consult the ATCCIS *Phase II Final Report* (October 1990), the *Phase III Work Plan* (December 1991), and the *Phase III Project Brief* (December 1991), from which this overview is taken [Refs. ATCCIS 1990, ATCCIS 1991]. Table 1 identifies the ATCCIS documents that have been circulated to the Nations by SHAPE.

Quick Reference	
Topic	Page
Application Level Fac	26
ATCCIS Architecture	17
ATCCIS Phase I & II	9
ATCCIS Objectives	9
ATCCIS Findings	11
Concepts for Arch	14
Data Mgmt Facility	23
Ensembles	20
Facilities	18
Input-Output Facilities	26
MMI Service Facility	26
Service Control Facility	25
System Mgmt Facility	26
Transfer Facility	25

2.1 Background for ATCCIS

2.1.1 ATCCIS Phase I and Phase II (1984-1990)

The primary purpose of the ATCCIS program is to achieve interoperability between national automated CCISs for use in the Central Region (CR) at Corps and below in the years 2000 and beyond. Two implicit objectives are to ensure that (1) ATCCIS-conformant systems deployed by the Nations are also interoperable with the systems being developed under the Allied Command Europe (ACE) automated CCIS programme and (2) such systems are affordable.

The ATCCIS Permanent Working Group (PWG) was tasked by Supreme Headquarters Allied Powers Europe (SHAPE) to develop an operational and technical concept for an interoperable tactical ACCIS that is based on stated operational requirements and evolving military concepts. The PWG is comprised of army officers and civilian scientists from four Nations (France, Germany, United Kingdom, and United States), SHAPE, and Allied Forces Central Europe (AFCENT) working cooperatively in accordance with guidance from SHAPE.

2.1.2 ATCCIS Objectives

To satisfy the primary purpose of attaining interoperability, the ATCCIS development programme must satisfy four principal objectives:

a. To formulate common requirements for the use of battlefield information

b. To ensure that all international and multinational users of critical battlefield information can exchange that information on a basis that is mutually agreeable

c. To exchange information so that it conveys the same meaning and understanding to source and recipient alike

d. To define a technical architecture capable of accomplishing the necessary exchanges and transactions.

Table 1. Listing of ATCCIS Papers Distributed by SHAPE As of 31 December 1991

No.	Class	Title	Edition	Date
-	NU	Phase II Work Plan	2.0	Sep-86
1	NS	Threat	1.0	Mar-86
2	NR	Mission Needs & Objectives	1.0	Sep-85
3	NC	Concept for Survivable C2	1.0	Dec-87
4/5	NC	Key Tasks	1.0	Oct-85
6	NC	Echelons & Staff Organizations	1.0	Jul-86
7B	NU	Degrees of Data Interoperability	1.0	Mar-86
7F	NU	Databases	1.0	Aug-89
7L	NU	Data Management & Standardization	1.0	Jun-89
7M	NU	Methodology for Identifying C2 Operational Requirements	1.0	Sep-89
7N	NU	Standardization of Data for Interoperability	1.0	Sep-90
8	NC	Operational & Functional Concepts	2.0	May-88
10	NC	Information Flow Requirements & Products for Each Key Task	2.0	Sep-90
11	NU	Requirements from Key Tasks	2.0	Jan-90
12	NR	General Requirements	1.0	Sep-88
12A	NR	Security Requirements	1.0	Sep-88
13	NU	IERs Among Elements of Each HQ	1.0	Feb-88
14	NC	IERs Between HQs	2.0	Sep-90
17	NC	Interfaces to Non-ATCCIS	1.0	Apr-88
18	NR	Operational Standards for ATCCIS IERs	1.0	Sep-88
18A	NU	Modernization of Land Force Operational Standards	1.0	Sep-89
22	NU	Architectural Concepts	3.0	Sep-87
23	NU	Requirements Analysis	1.0	Sep-87
24	NU	Architecture Definition	3.0	Oct-90
24B	NU	Properties of TF and SCF	1.0	Dec-87
25	NU	Technical Standards for ATCCIS Architecture	2.0	Aug-90
30	NU	Applicability of the Architecture	1.0	Jan-90
34	NU	ATCCIS Communications	1.0	Jan-90
34A	NU	Background to ATCCIS Comms	1.0	Oct-88
39	NR	Phase II - Final Report	1.0	Oct-90
-	NU	Phase III Work Plan	1.0	Dec-91
-	NU	Phase III Project Brief	1.0	Dec-91

2.1.3 ATCCIS Phase II Findings

There were eight principal findings of the Phase II study.

1. There is more than 80% commonality in the key command and control (C2) tasks performed at corps level and below, despite the fact that the organization and structure of command posts (CPs) utilized by the four Nations differ significantly.

a. The PWG developed and harmonized a detailed listing of the Key Tasks performed at tactical echelons by the ground forces of each of the four Nations. The PWG also documented the specific information needed by a particular command or staff element/cell in order to accomplish a given Key Task. These analyses demonstrate that the Nations have common requirements for the use of battlefield information.

b. CR Nations do not have a common way of expressing their operational requirements when participating in multinational cooperative C2 efforts. Therefore, the PWG adopted an ACE methodology, Command and Control Requirements Analysis (C2RA), and successfully modified it for use at the tactical level. It appears that this method is suitable for adoption by other Nations faced with a similar requirement. Indeed, the ABCA (Australia, Britain, Canada, and America) Nations have adopted the ATCCIS methodology as their way ahead for progressing C2-related projects.

2. The four Nations can directly correlate those specific C2 processes performed in, and the information exchange requirements (IERs) pertaining to, their respective corps, division, and brigade CPs with a harmonized set of ATCCIS C2 processes and sets of ATCCIS IERs.

a. The forces of all Nations must have a common understanding of how C2 processes are performed in order to operate effectively together and ensure that orders and directives are not misinterpreted. Notwithstanding national variations in organization and doctrine, the detailed analyses revealed that the C2 processes carried out by all four Nations are essentially common. The study represents the first comprehensive investigation of the essential and necessary interactions between the national formations and NATO Principal Subordinate Commands (PSCs).

b. The study effort identified the producers and users of nearly 3,000 C2 Products such as operations orders or situation reports. Using these results, the IERs were then defined for those national forces that might be required to operate in coalition with the forces of other Nations or under the operational control of a NATO Headquarters (HQ). Requirements have been reconciled with the emerging results of the ACE ACCIS system design and integration effort.

3. Current C2-related operational standards prescribed for use by NATO and the Nations are often conflicting, inadequately defined, and ill-suited for international exchange of information in either a manual or an Automatic Data Processing (ADP)-supported CCIS environment.

a. NATO C2-related operational standards have been compared with corresponding national instructions, doctrine, and directives. It was found that many of the standards are out-of-date or imprecisely written. In other instances, individual Nations and formations have opted to implement modifications that no longer resemble the base standard. This is an unsatisfactory basis for progressing either manual or ADP-supported CCIS programmes.

b. To remedy this problem, the PWG proposed a strategy for modernizing NATO C2-related operational standards. SHAPE endorsed the PWG proposal and forwarded it to the NATO Military Agency for Standardization (MAS). More work is urgently required before this problem can be rectified.

4. A NATO-wide data management policy is required.

a. The need for such a policy is well established in NATO, but none has yet been promulgated.

b. Commonly agreed and unambiguous definitions of data are required for use in ACCISs. Lack of such definitions severely inhibits the attainment of international as well as multinational interoperability. Current operational and technical procedures cannot ensure that the source and the recipient of information that is exchanged between and among cooperating formations will each share the same meaning and intent of that information.

5. A technical architecture for an ATCCIS can be defined by using international commercial (nonproprietary) standards supplemented, where necessary, with military enhancements or standards.

a. Given the existing significant differences in national philosophy, organizations, funding, and procurement schedules, it was determined that development of common hardware for ATCCIS would not be practical.

b. The PWG determined that the most feasible way for the technical work to proceed would be to focus on the establishment of an architecture that would provide a common basis acceptable to all Nations.

6. The analysis has concluded that an ATCCIS-conformant system must be a transaction processing system with a partitioned, partially replicated database.

a. The essential nature of military C2 is the interaction of commanders and their staff with superior and subordinate formations, by the manipulation of military information through various forms of transactions.

b. ATCCIS-conformant systems must be capable of supporting applications and maintaining the capability for consistent interpretation of data across national and multinational formation boundaries.

c. The interactions that users of tactical ADP systems make are in the nature of transactions that are, for example, in the form of updates to a database, requests for information, or orders to be issued where appropriate. Future demands on transaction processing systems will probably take the form of decision support.

d. The architectural concept is defined in terms of a number of logical facilities that provide technical services essential for the interoperability of ADP systems that support the C2 function. The key attribute of ATCCIS-conformant systems is Basic Interoperability, i.e., the exchange of information that preserves the meaning and relationships of the information exchanged. It is achievable through the implementation of four facilities; the facilities themselves are defined in terms of standards, protocols, and functionality. However, it is still too early to select specific interoperability parameters, individual standards, or stacks of standards.

e. The sole requirement placed on tactical communications by the architecture is to provide a standard network service.

7. The concept for the ATCCIS architecture is consistent with that for the NATO Consultation, Command and Control (C3) Architecture.

a. The current NATO C3 Architecture draws heavily on ATCCIS technical proposals.

b. The ATCCIS technical concept is also compatible with the draft guidelines for technical standards being established within NATO.

8. Operational and technical standards necessary for national implementation are still immature; a programme definition phase is required.

2.1.4 ATCCIS Method of Work for Technical Analyses

The technical analyses in ATCCIS have been limited to those aspects of the architecture that appeared to be essential to achieving basic interoperability--the exchange of information that preserves meanings and relationships--and the potential for cost savings without unnecessarily limiting national implementation options. Provision has been made in the proposed architecture for supporting a wide range of approaches for developing and implementing applications to support operational requirements, but there was no attempt to delimit or specify those approaches. Technical and procedural standards were reviewed for their applicability for specifying the architecture, but no selection of such standards has yet been attempted. The review has identified standards employed in NATO and--where such standards could be widely used--in the Nations for ensuring interoperability and providing the potential for cost savings. Preliminary analysis has been performed on the applicability of the architecture to a wide range of operational configurations, but this analysis was descriptive rather than complete in so far as covering all possible operational requirements or in fully validating the technical aspects of the architecture. Technical analyses have also addressed the impact of the architecture on communications and of communications on the architecture, but it is too early to be definitive about what communications will be in place by A.D. 2000.

Key features of the technical approach can be summarized as follows:

- *The architecture was specifically limited to defining only those aspects required for interoperability.* The architecture is not intended to be a complete architecture satisfactory for implementation. Specifically, the architecture does not define any application-level facilities, nor does it define any user interfaces or user interaction with the database.
- ATCCIS conformancy limits implementations only to the extent that they must provide the services and logical facilities of the architecture. Thus, the architecture intentionally does not have the detail required to guide the choice of computer architecture, workstations, operating system, database management system, or other commercial off-the-shelf (COTS) products. These aspects, together with the definition of application-level facilities and user interfaces, would be national options and would have to be addressed in national systems.
- The architecture is, by design, driven primarily by the requirement for interoperability. National CCIS architectures are expected to differ depending on the additional driving requirements imposed to meet national needs, which include the use of COTS software, support common software development among several Nations, or use a wide mix of products from different vendors.
- NATO has defined six "Degrees of Interoperability," reflecting the procedures by which the transfer of data associated with interoperability is to be achieved. It has been generally accepted that degree 5 interoperability--automated data exchange with user-imposed access restrictions--is the mechanism required by the Nations and has been adopted by the study as the basis for providing interoperability. Many of the concepts underlying the architecture are governed by the requirement to implement degree 5 interoperability.

2.2 Fundamental Concepts of the ATCCIS Architecture

This section describes seven concepts that are fundamental to the architecture.

2.2.1 Information Exchange

Information Exchange Based on Information Items. Information items are the essential ingredients for the performance of a military Key Task (both input and output). Information exchange today is conducted on the basis of formatted messages in the form of C2 Products, which ideally are composed of agreed groups of information items. However, in the future, information exchange between conformant systems will be conducted on the basis of information items themselves, and the required information aggregates can be constructed from these information items. Information products in their entirety constitute a highly inefficient basis for information exchange. Note that:

a. Preparation of information aggregates from groups of information items in performance of Key Tasks is the prerogative of national implementation and may not necessarily be standardized.

b. The definition of information items that support the performance of Key Tasks is seen as relatively stable, whereas the procedures for performing the Key

Tasks and the form of the associated C2 Products can be expected to change more often.

c. Agreement on the exchange of information items that preserves meaning and relationships is essential for interoperability, but agreement on formats for presenting these data is not required for interoperability.

d. A C2 Product may be propagated by creating a new set of its constituent data items. However, a C2 Product may also be propagated more efficiently by an update to some of its constituent items.

Information Exchange Based on Other Data Types. Information will need to be exchanged for other types of information objects--an object contains information in some agreed context--than objects based only on information items for structured data. Examples of such information objects are assessments, briefings, documents such as operations orders, video imagery, graphical displays such as map overlays, and terrain representations. Document exchange can be achieved by agreements on document structure and format without restricting national options for implementing word or text processing capabilities or national preferences for how documents are presented to users.

2.2.2 Information Models

The architecture will need to support several types of data models, including a relational model for a database for structured data. Since structured data is expected to be present in all ACCISs, the relational model will be common to all conformant systems.

Relational Model. For many army ACCISs, data are distributed and selected parts of the total data are replicated in a limited number of locations; this is a concept technically referred to as a partitioned, partially replicated database. Since data are maintained in a number of locations because the data originate and are used in different locations, the connectivity of those locations cannot always be guaranteed. Unexpected temporary or permanent loss of nodes and links is a feature of the military environment. Furthermore, communications limitations may demand local caching (storage) for performance reasons. Hence, *in order to ensure that the required data is available at a specific location at the time it is needed, the database is organized and maintained as a partitioned, partially replicated database.*

Other Data Models. *The architecture will need to support information models other than the relational model described above.* These could include object-oriented models for such data types as documents, imagery, and terrain representations. Further, the architecture will need to provide for the integration of different types of data (e.g., data items or documents) for the various models. Each data model will lead to a different type of database in an implemented system.

2.2.3 Information Transfer

Three criteria have to be satisfied in order that Basic Interoperability can be achieved:

- Transfer of Data. There must be a means whereby data can be physically moved from the originating HQ to another HQ that needs that data.
- Interpretation of Data. There must be some means of identifying the data so that the two (or more) HQs using the data can be certain they will all interpret it in a consistent manner.
- Management of the Basic Interoperability Functions. There must be mechanisms for managing the processes involved in these operations, including (but not restricted to) the needs for security and keeping abreast of a changing tactical disposition of HQs.

The minimum capabilities required to support these criteria are (1) a mechanism that provides end-to-end transfer of data, (2) a mechanism to manage the storage, retrieval, and interpretation of data, and (3) a mechanism that manages these two mechanisms.

Several types of transfer mechanisms may be required for the various data types. Database-to-database transactions could support transfer of structured data (defined, for example, by a relational information model). Other transfer mechanisms may be required for exchange of such data types as documents; candidates are file exchange, military message handling, or electronic mail.

2.2.4 Transaction Processing

The interactions between users and an ACCIS are in the nature of transactions (e.g., in the form of updates to a database, requests for information, or orders to be issued). This transactional characteristic of ACCISs will continue to apply in the future with the expectation that there will be additional demands on such systems, for example, in the form of decision aids and other forms of automation to support the decision process. Therefore, *the principal characteristic of systems that support tactical C2 is transaction processing*.

2.2.5 Support for Applications

Requirements have been identified for providing military services to users, which in turn require the provision of decision support and other functions to support the performance of Key Tasks. The provision of these functions will be fulfilled by a set of applications executed on the ADP systems supporting the staff in the performance of their Key Tasks.

It is therefore necessary for conformant systems to be able to support the execution of such applications. Furthermore, the allocation of applications to particular systems or parts of systems should not be fixed, but should have sufficient flexibility to allow for

changing operational situations. The manner in which such applications are incorporated into a system is specified by the architecture, but the detailed specification of the functionality of any particular application is outside the scope of the architecture and may be a matter for individual Nations to determine for themselves, or may be the subject of separate multinational agreements. Within the architecture, any application, irrespective of its functionality, must conform to certain rules and interface standards.

2.2.6 Support for Human-Computer Interfaces (HCIs)

The technical capabilities of a system, and the information held within such systems, are of no practical use unless the staff users can gain access to those capabilities and information. It is therefore essential for systems to provide an adequate human-computer interface. Agreement on a common human-computer interface is not essential for interoperability and is therefore not addressed as part of the requirements for Basic Interoperability. However, there are many benefits to be obtained by adopting a common approach to human-computer interface, including, for example, a common presentation to users and the potential for common development of software for applications. The architecture therefore has identified in outline a Man-Machine Interface (MMI) Service Facility (MSF) to provide a common set of services. Such a facility allows the adoption of a User Interface Management System (UIMS), providing such capabilities as window managers and user dialogue managers to allow flexibility for applications while at the same time removing from those applications the need to account for the particularities of any one set of equipment for user interaction.

2.2.7 Information Exchange With Nonconformant Systems

Interoperation with nonconformant systems will be an important capability of conformant systems during the transition phase. In addition, it is expected that there will always be some nonconformant systems fielded by the Nations; information exchange with those systems is expected to be in accordance with current NATO procedures that use message text formats (i.e., STANAG 5500). Such systems may be manual or ADP-supported, and the degree of interoperability achievable and the services required may cover a wide range. An additional set of facilities has been identified to provide for such interoperation, although no detailed effort has been allocated to refining their specifications. *In order to achieve interoperability with nonconformant systems, there must be an agreement on data standardization.*

2.3 Overview of the Architecture

The fundamental concepts on which the architecture is based are identified in Section 2.4 and describe a transaction processing system with a partitioned, partially replicated database, capable of supporting applications and maintaining the capability for

consistent interpretation of the data across organizational boundaries. This description of the nature of an ATCCIS-conformant system is basic to the structure of the architecture.

The architecture is defined in terms of a number of facilities (defined below) essential for the interoperability of ADP systems, which support the command and control function and provide opportunities for cost savings. The facilities are themselves defined in terms of functionality, protocols, and standards.

2.4 ATCCIS Facilities

A facility is a logical entity that provides at its external interface a set of related services, which includes all of the functionality necessary to provide those services, together with any additional functionality required to relate one service to another or to maintain the status and internal logical properties of the facility. The architecture defines the logical structure of, and interrelationships among, the facilities. The facilities necessary to provide Basic Interoperability are referred to as the Basic Facilities, whose functionality must be standardized for all conformant systems.

2.4.1 Basic and Application-Level Facilities

There are four Basic Facilities in the ATCCIS architecture:

(1) Data Management Facility (DMF). The DMF provides functionality to ensure the proper management of data, and to ensure that there is a consistent representation of data and data relationships across all conformant systems.

(2) Transfer Facility (TF). The TF provides functionality to allow different parts of a system, or two conformant systems, to invoke services one from another. TF includes data transfer protocols, services of the communications infrastructure, and services to manage data transfer and communications.

(3) System Management Facility (SMF). The SMF provides functionality supplementary to the management services of the TF and DMF for control of part or all of a system.

(4) Service Control Facility (SCF). The SCF provides functionality to control interactions among all other facilities.

The Basic Facilities provide the three mechanisms identified in Section 2.2.3 (viz., providing end-to-end transfer of data; managing the storage, retrieval, and interpretation of data; and managing these mechanisms) as the minimum capability to support Basic Interoperability.

Application-Level Facilities (ALFs) provide the functionality associated with performing the automated parts of Key Tasks in a subfunctional area (SFA). Within the architectural model, there may be some ALFs providing general application-level services common to a number of subfunctional areas or Key Tasks, and other ALFs providing particular functionality in support of one SFA or a single Key Task. The extent to which Key Tasks in an SFA are supported by automation is a national prerogative. ALFs could

be national-unique, standardized among some nations, or standardized among all the nations.

2.4.2 Other Facilities

Two additional facilities have been identified for the architecture, other than the ALFs and the four Basic Facilities. These are the Man-Machine Interface (MMI) Service Facility (MSF) and a family of Input/Output Facilities (IOFs). The MSF provides the functionality for a generalized interface between ALFs and users, irrespective of the particular devices used to interact with users and the human-computer interface they implement. Each IOF provides an interface between a conformant system and a particular class of nonconformant systems. There are as yet no formal operational requirements for the MSF or IOFs, but agreements to standardize these facilities could lead to opportunities for cost savings.

2.4.3 Facilities and Operational Activities

Four classes of activities have been identified in the operational analysis of Key Tasks (WP 11) that need to be supported by ADP functionality. These classes and their relationship to the facilities are as follows:

- Access. This class includes all activities and actions involved with the access by the user to information, or recording information provided by the user. It includes any subsidiary activities and actions to enable the user to specify and carry out his access requirements satisfactorily. In this context for an ADP system, the term "user" should also be interpreted as including any item of software operating on the user's behalf. The access class will be provided primarily by the DMF, supported by human-computer interfaces (e.g., MSF), and ALFs.
- Processing. This class includes all activities and actions involved in the manipulation of information to produce new, or revised versions of existing, information. The processing class will correspond to the functionality associated with performing the automated parts, if any, of Key Tasks in an SFA. Within the architectural model, there may be facilities providing general application-level services and facilities providing particular functionality in support of one SFA or a single Key Task. This functionality will be provided through ALFs. There may be a significant number of processing activities and actions performed manually.
- Transfer. This class is specifically concerned with the transfer of information from one command post or group of users to another. It is not concerned with any processing of the information, nor with the presentation of the information to the user, nor recording updated information that the user might provide. Again, in this context for an ADP system, the term "user" should also be interpreted as including any item of software operating on the user's behalf. The transfer class will be primarily provided by the TF and DMF.

- Control. This class includes all activities and actions concerned with the management of the C2 process, rather than performing specific actions within the process. The control will be supported by the management services of TF and DMF, the SMF, and ALFs with specific system management functionality. Interactions among the other facilities will be controlled by the SCF. There is expected to be a significant number of control activities and actions performed manually.

2.4.4 Interaction Between Facilities

Each facility will provide a defined set of services. These services are available to all other facilities within the same ensemble (see below). A facility that calls on the services of another facility must do so by means of a predetermined service call with a predetermined set of parameters. The service requested may provide an acknowledgement, a return of data, or both, or an exception condition. The action of the called facility will be predetermined.

2.5 Ensembles and Components

2.5.1 Basic Ensemble

An ensemble is a set of facilities that includes, as a minimum, the four Basic Facilities. The smallest ensemble is one that contains only the Basic Facilities and is referred to as the Basic Ensemble. A set of facilities that does not include the four basic facilities (i.e., does not include the Basic Ensemble as a subset) is not an ensemble; it is merely a grouping of facilities that has no significance.

Systems may be represented logically as configurations of ensembles. Two ensembles participating in a peer interaction may be part of the same or different systems. The TF provides, by virtue of its functionality, the linking mechanism between all ensembles.

A simplified picture of the architecture is depicted in Figure 3. It shows the relationship between the TF and the other facilities in two ensembles. The Basic Ensembles are highlighted with bold lines. SMF, SCF, and DMF each appear in all the ensembles, whereas the TF is considered common to all the ensembles. Ensembles A and B can be thought of as the facilities at two physical locations. The TF includes the services for open systems interconnection and the bearer circuits (i.e., communications media).

2.5.2 Interaction Between Ensembles

The TF links one ensemble to another. A facility in any ensemble has access to the TF. Facilities may call on the services of other facilities that form part of the same ensemble for assistance. A facility will be aware of the other facilities within its own ensemble, but will not, in general, be aware of the existence of other ensembles. However, a facility can be made aware of other instances of the same facility that exist in

other ensembles, known as peer facilities, and can interact with those peer facilities through the functionality of TF to assist in providing its services. For example, data replication and remote access to data both require peer interactions between data management facilities. A facility will not normally be aware of the existence of the same facility in every other ensemble; indeed, restriction on the awareness of other ensembles will be one of the mechanisms employed to control access and "need to know."

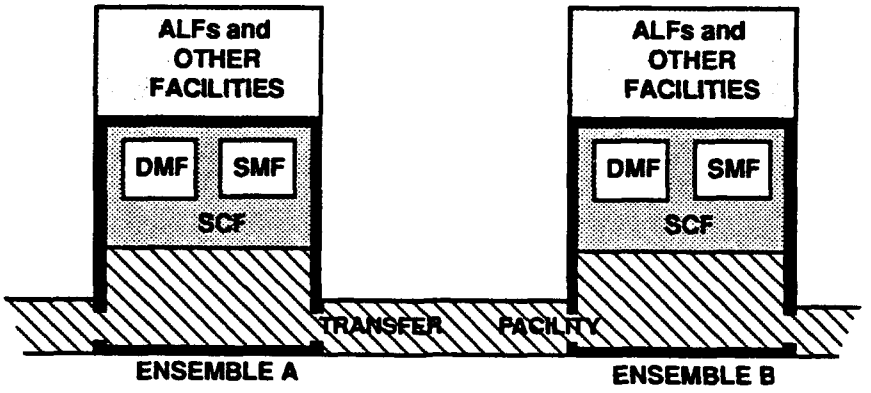


Figure 3. Facilities of the Architecture

A facility requiring services from another ensemble may call only on the services of a peer facility. If the services of a different type of facility are required, the calling facility must call on the local instance of the called facility; in the absence of such a local instance, the services of that facility are not available.

2.5.3 Components and Their Relationship to Ensembles

A Component is a collection of hardware and software that implements, as a minimum, the Basic Facilities in order to interoperate with other Components at least at the level defined by Basic Interoperability. It must provide the services of those facilities, either by implementing all of those services itself or by providing access to their implementation on other Components.

There is a one-to-one relationship between Components and ensembles. Specifically, the implementation of an ensemble is a Component, and a Component implements only one ensemble. The subsets of an ensemble, even if they include the Basic Ensemble, are not thought of as separate ensembles in relation to the Component on which they are implemented. Thus, consolidating the facilities from two Components onto one Component, as may be required if one of them becomes inoperative, is considered as combining the two ensembles into one ensemble, not implementing two ensembles on one Component.

A collection of Components is known informally as a system, usually with a qualifier that indicates the basis for the collection, such as a headquarters system or a national system. There is a wide range of possible configuration options for a headquarters system, from a single Component serving all users through terminals to a large number of individual workstations, each a Component, interacting to provide the total requirements of the HQ.

It should be noted that a set of workstations connected on a LAN may be a single Component or each workstation may be a separate Component, depending on whether the four basic facilities have been implemented once for the collection or once in each workstation. The choice is entirely a national option. In the case where each workstation is a separate Component, it is likely that the measure of interoperability among such a grouping of ensembles will be significantly higher than the measure of interoperability specified overall. This is also a national choice. Thus, system specifiers are free to determine their requirements independently for local interoperability.

Automated support of subfunctional areas will be implemented on a set of Components. Data elements owned by those subfunctional areas will be managed by DMF services implemented on those Components. Those DMF services must ensure that these data elements are available to the other subfunctional areas that require them. An SFA may not create, delete, or amend data elements owned by other subfunctional areas.

2.5.4 ATCCIS-Conformant Systems

If a number of Components are interconnected according to the architectural rules, then the resulting system itself becomes conformant. A conformant system will, in general, comprise a number of distinct interconnected Components, each of which must conform to the architecture and interoperate with other Components of the system, and with Components of other systems, according to the standards defined by the architecture. Thus, the conformance of a system can be demonstrated by proving all its Components and interconnections to be conformant. A conformant system will remain conformant if additional conformant Components are connected according to the rules and standards defined by the architecture. From a technical point of view, when two systems are interconnected they can be considered as a single system. However, management considerations will normally differentiate between the two systems.

An HQ will be configured from one or more Components. A Component may host part or all of one or more subfunctional areas. Implementing agencies would have great freedom in how the software and hardware of a system might be designed to achieve conformancy.

2.5.5 System Management

Services must be provided to allow conformant systems to be configured and managed so that users' ADP needs are satisfied in the most effective manner. System managers will call on system management ALFs to assist them in managing the system in the same way that other users will call on their specific ALFs to perform their day-to-day roles.

Several aspects of a conformant system will require data to relate its own operations to other parts of that system or to other conformant systems. Some Key Tasks are concerned with system management and will manipulate sets of information containing system management parameters. System management information exchange requirements (IERs) define the exchange of system management parameters. Tables of system management parameters will be managed by the DMF with access rights specific to the system management functions. Users, other than system managers, will be able to read but not modify these tables.

An example of a system management table is the logical-to-physical translation table that will be used by the TF.

Other aspects of system management will be performed by the system managers calling on management services of the DMF and TF. Most of the system management functions, which will be offered to the system managers as high-level services by the appropriate ALFs, will be effected either by these local system management services in TF and DMF or by the maintenance and distribution of local tables.

2.6 The Four Basic Facilities

This section provides technical details regarding the four basic facilities: DMF, TF, SCF, and SMF.

2.6.1 Data Management Facility (DMF)

The purpose of data management is to (1) represent the meaning and relationships of the information items required to perform key tasks, (2) ensure meanings and relationships are preserved when information is exchanged with another conformant system, and (3) ensure changes to data items are applied consistently wherever these items are stored. The DMF needs to support a number of data models, including a relational model for structured data. These data models should be derived from a common conceptual schema to ensure compatibility of the data objects and data elements.

Requirements. The DMF is required to provide data from the ATCCIS database to a facility in the same ensemble performing a service on behalf of the user. Further, the DMF supports updates to the database, replicates a partition between ensembles, and copies a partition for local use.

Concepts. A replication domain (RD) is a partition of the data owned by an SFA. The RD is the smallest unit of the database that can be replicated in full. An RD contains data from a single data model.

A replication pattern is a specification of which ensembles are permitted to hold a copy of an RD other than the ensemble owning the RD. The replication pattern is one of the mechanisms for providing access control in the architecture.

An access control domain (ACD) is a subset of an RD with a common set of authorized users. A set of data elements, in the case of structured data with a relational model, comprises an ACD.

Services. There are three primary services provided by the DMF: update transactions, access, and replication transactions.

- Update transactions are performed on RDs in a single ensemble. (As a national option, within the same HQ one update transaction may update RDs in multiple ensembles.)
- Access is the retrieval of a set of values for specified data elements (or other data objects). Access may be performed by:
  (1) Query, from an RD in the same ensemble as the requesting facility
  (2) Remote query, from an RD in another ensemble to which access has been previously agreed.
- Replication transactions copy all the data that has been updated within the RD to another ensemble. The services provided by a replication transaction may depend on the type of data in the RD.

By definition, the physical manifestation of a source RD for a replication transaction is in a single Component and the physical manifestation of the target RD is also in a different single Component. Thus, since the physical manifestation of an RD would be entirely contained in the database (or other appropriate data structure implementing the data model) at a single Component, the protocols for a replication transaction are simpler than if the replication involved sources or targets with multiple databases spanning several physical Components. A complete list of DMF services is provided in Annex A of WP 24.

Support for DMF Services. A special RD (called a system management RD) will be defined to describe the RDs accessible to each DMF and to identify the logical addresses of the physical manifestation of those RDs.

DMF Services are Transparent to the User. All data to which the user has access are in the ACDs of RDs known to the DMF. Some of that data will reside locally (in the same ensemble as the DMF) and some remotely (in an ensemble of another Component). Speed of access performance may depend on whether the DMF needs to invoke a query or remote query to satisfy an access request.

The DMF can be invoked by the SMF, ALFs, MSF, or IOFs in the same ensemble, or by a DMF in another ensemble through a peer-to-peer protocol via the TF.

Implementation Considerations. The implementation of a DMF will require a data manipulation language (such as Database Language SQL for data defined by a relational model). Database management systems may provide all the services required of a DMF.

2.6.2 Transfer Facility (TF)

The Transfer Facility (TF) is the logical entity that interconnects all ensembles. Whereas the other facilities are considered to have a separate manifestation in each ensemble, the TF is considered to be a facility that has one manifestation only, but one that extends across every ensemble. Notwithstanding, that manifestation of the TF in every ensemble has a corresponding implementation in every Component. The logical interconnectivity between two ensembles is thus provided as a result of the functionality of the TF that interconnects the two ensembles. The implementation of the TF in the corresponding Components will result in functionality in each Component together with communications interfaces and one or more communications media between those interfaces.

Network management includes management functions for all layers of open systems interconnection (OSI), naming and addressing, and registration authorities for controlling assignment of names and addresses. Network management will be addressed in part by work being conducted in ISO and CCITT (e.g., ISO 7498-3, *Naming and Addressing*, and ISO 7498-4, *Management Framework*). Those aspects required to ensure interoperability will be addressed by the standards to be adopted for the architecture. These include configuration management and fault management as well as common management information services and protocols.

2.6.3 Service Control Facility (SCF)

The Service Control Facility (SCF) is the logical entity that binds together all the facilities in an ensemble. The services of the SCF are expected to be provided by the underlying operating system of the implementation. There is no concept of peer interactions between SCFs.

A facility will be explicitly aware of the services that it requires of another facility and will invoke a request for such a service via the SCF. The only standard identified to date that applies to the SCF is the Portable Operating System Interface for Computer Environments (POSIX) (IEEE P1003).

2.6.4 System Management Facility (SMF)

The SMF is a logical entity intended to provide functionality supplementary to the management services of the DMF and TF for control of parts or all of a system. However, to date, no specific functionality has been identified for SMF that is not provided by DMF and TF. No standards, therefore, have been identified for the SMF. Thus, the system management aspects of Basic Interoperability appear to be satisfied by exchanging system management data and using management services of DMF and TF.

2.7 Application-Level Facilities

An application-level facility (ALF) is a logical entity that provides services to support the functionality of part or all of one or more Key Tasks. An ALF may be very general purpose, such as a word processor, or may be unique to a single Key Task, such as a battle management decision aid. The entities with which a user interacts, whether directly or indirectly, are ALFs. Some ALFs are therefore likely to contain particular procedures and doctrinal aspects embedded within them that will be specific to an individual nation. These may therefore be more difficult to agree to on a multinational basis and hence will tend, at least initially, to be Nation-specific.

2.8 Other Facilities

This section describes two facilities that provide additional capabilities over those provided by the four Basic Facilities and the ALFs. They have been specifically identified because they act as interfaces between the architecture on the one hand and users or nonconformant systems on the other hand. Neither of these facilities are required for conformancy, but their use would provide the potential for cost savings.

2.8.1 MMI Service Facility (MSF)

Users require means to interact with an ADP system. Within the architecture, the MSF has been identified as providing a standard set of user services as the interface between a user and the other facilities within the ensemble. This could be provided separately for every ALF, but providing a unique interface for each ALF would limit flexibility and the potential for cost savings. MSF will provide services both to users, so that they can call on the services of appropriate facilities, and also to those facilities so they can display information to users and solicit responses or input.

2.8.2 Non-ATCCIS Input/Output Facilities (IOFs)

An IOF is a logical entity for providing the services for interface between conformant systems and nonconformant systems. Because there will be several different nonconformant systems for which interfaces will be required, there will be a family of IOF types rather than a single one. Within an ensemble there can be one of each type of IOF.

One part of the interface between a conformant system and a nonconformant system is not designed in accordance with standards of the architecture. This interface will be an IOF providing the necessary services to pass data out to nonconformant systems and to receive data from those systems.

Standards for IOFs will be defined as required for each type of nonconformant system and will include both data management and data transfer standards. Examples are STANAG 5500 messages.

(This page intentionally left blank.)

3. STANDARDIZATION PROCESS IN RELATION TO CCISs

3.1 Role of Interoperability in Future C2 Processes

Quick Reference	
Topic	Page
Interoperability	29
Limitations of Standards	32
Services for CCISs	29
Standardized Profiles	40
Stds Development	33
Stds Organizations	35

The primary focuses for future C2 interoperability are on joint operations and combined operations. Command elements must monitor, assess, plan, decide, and execute functions with close coordination and integration of the capabilities of the military components. In combined operations there is expected to be an increased reliance on coalition forces with multinational headquarters. Ensuring effective coalition operations requires pre-planning of C2 capabilities and high confidence of supporting the anticipated (and possibly unanticipated) information exchange requirements with automated, interoperable systems.

3.2 Services Requiring Standardization for CCISs

The standards needed for joint and combined interoperability cover a wide range of required services and definitions: data communications protocols [e.g., for open systems interconnection (OSI)], network application services and interfaces (for applications portability, maintainability, and evolvability), COMSEC and COMPUSEC equipment and procedures, data elements, data models (e.g., for multi-media documents, in additional to the commonly used relational model), information and communications resource dictionaries (e.g., for databases and communications resources), naming conventions (for data elements and information exchange requirement statements), and glossaries (for the terms used to define the other aspects subject to standardization).

Eight groups of services common to many types of CCISs have been identified. They are:

(1) Data Management Services. Provide for data processing functionality and support of data objects. Data management services address data dictionary, directory, query, and reporting. These services support the storage, control, distribution, management, and allocation of simple data such as text and numeric information and complex items such as complete documents, maps, charts, images, and multimedia objects.

(2) Network Services. Include the transmission and interface standards and protocols that support logical and physical communication. They describe and constrain how the hardware and software of the nodes cooperate in node-to-node interaction.

(3) Operating System Interface Services. Operating systems manage hardware and software resources and all software interfaces, including local and distributed execution of application programs. Standards in this domain include those that cover program-to-program communication and synchronization as well as management of memory and interfaces to network and data management services.

(4) Security and System Management Services. Security services protect the components, mechanisms, and information of the CCIS. Basic security functions include authentication, access control, confidentiality, integrity, and nonrepudiation. This area includes services pertaining to systems management, conformance testing, and registration authorities.

(5) Data Interchange Standards. Provide the ability to transfer data that represents abstract objects such as military orders, reports, research documents, graphical items (e.g., maps, overlays, symbolic graphical data that might be produced by a simulation), and raw video (e.g., television images). Data exchange services also address product descriptions. Data exchange services permit the exchange of data among applications and between systems so that the meaning and relationships in that data are preserved.

(6) User Interface Services. Support visual and functional interaction with the user, providing access to hardware and software and graphical user interface (GUI). They control the presentation of data and mode of interaction.

(7) Graphics. Support the creation and manipulation of pictures elements, to include display element definition and management and graphical object attribute definition and management. These services are used for describing multi-dimensional graphic objects in a form that is independent of output devices and for managing hierarchical database structures containing graphics data.

(8) Programming Services. Support the development, checkout, installation, maintenance and testing of application and system software, including computer-aided software engineering environments, specification languages, and program development and, maintenance tools. Programming services also include the language-specific and inter-language interfaces or bindings that support the client-server interaction.

The eight service areas are derived from the Application Portability Profile (APP) services proposed by the US National Institute for Standards and Technology (NIST) and the US DoD Corporate Information Management (CIM) Reference Model. The NIST APP has just seven service areas--it does not include security as a service area. The CIM Reference Model identifies all eight service areas. The generic CCIS architecture for the Worldwide Military Command and Control Information System (WWMCCS) Automated Data Processing (ADP) Modernization (WAM) program has seven service areas--it includes Graphics in the user interface service.

3.3 Using Standards and Profiles to Specify Open Aspects of CCISs

One of the underlying principles for any CCIS is that specifying standards is essential to achieving interoperability. However, specifying standards will not alone guarantee interoperability. Indeed, every standard has a number of system and design parameters or interoperability parameters whose values may need to be fixed in the design phase of implementation. To ensure interoperability, each of these interoperability parameters must also be specified and controlled. Some interoperability parameters are very general and may be used to specify a class of options or mode of operation. Other interoperability parameters may be very detailed, such as restrictions on timing, format size, or bandwidth.

Because each standard is a reflection of the degree to which agreement can be reached in a service area, many important attributes (i.e., interoperability parameters) are often left unspecified or unaddressed. As agreements are reached over time, the standards will improve by addressing more functionality and harmonizing conflicting approaches. In cases where standards identify extensions and other types of options, great care must be taken in standards specification and interoperability parameter control to ensure that whenever an extension or option is permitted, every implementation of the related service also supports this extension or option. This principle is especially important in achieving not only interoperability but also portability of applications from one environment or implementation to another, such as is needed when operating systems, data management systems, interface packages, and hardware are upgraded.

An open system has been defined in IEEE P1003.0 as follows:

> Open System. A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (1) to be ported across a wide range of systems (with minimal change), (2) to interoperate with other applications on local and remote systems, and (3) to interact with users in a style which facilitates user portability.

There are three major classes of standards applicable to open systems:

- Standards for higher level applications and data representation
- Standards and profiles for OSI
- Standards for bearer circuits and other elements of the external environment.

The classes are shown in Figure 4. Interoperability parameters need to be drawn from all three classes of standards, both from the minimum requirements and from the options within the standards. As will be shown in subsequent chapters, the network services require standards in the lower two classes, whereas the other groups of services (i.e., data management, operating system interfaces, security and system management, data interchange, user interfaces, graphics, and programming) are addressed primarily by standards for higher level applications and data representation. The application or highest

layer of the OSI standards has standards not only for the communication services but also for other groups of services.

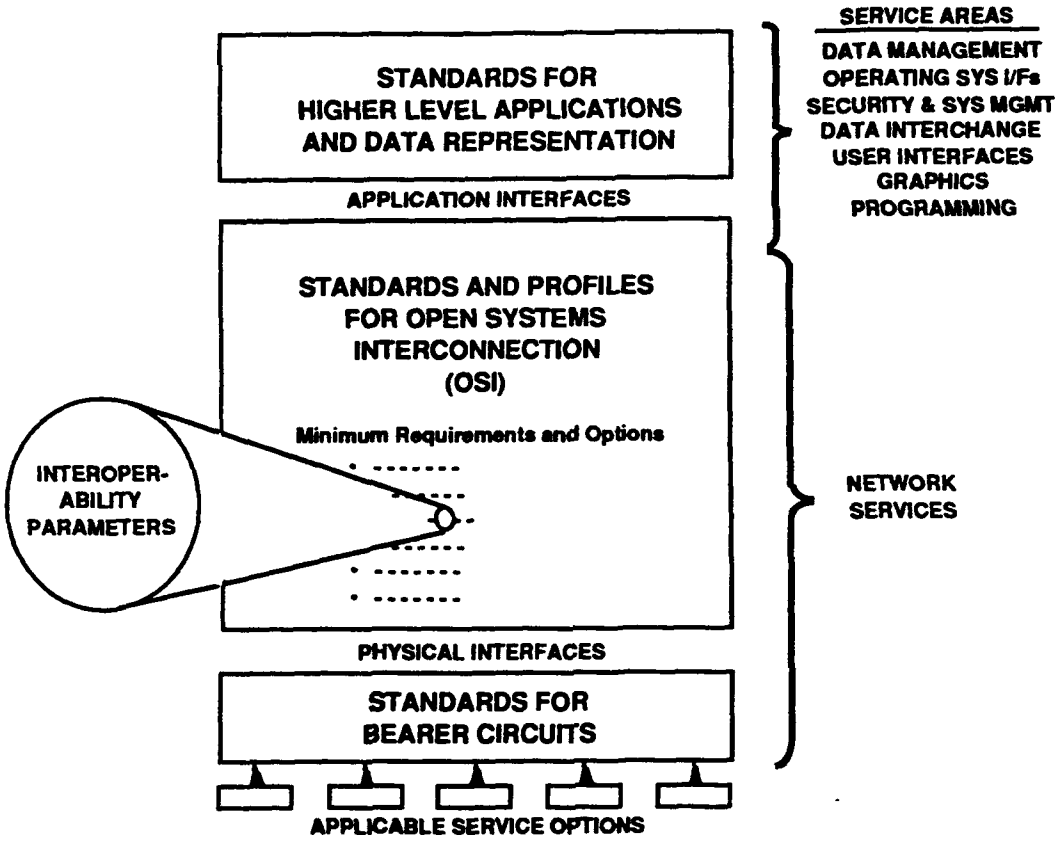


Figure 4. Classes of Standards and Their Relation to Groups of Standards

3.4 Overview of the Standards in the Eight Service Areas

Table 2 identifies standards potentially applicable to CCISs in the eight service areas: data management, network, operating system interfaces, security and system management, data interchange, user interfaces, graphics, and programming. The status of these standards is discussed in Chapters 4-10. Open systems profiles for CCISs for the 1990s are expected to be developed from this set of standards.

3.5 Limitations on the Role of Standards

Use of standards, together with the appropriate control of interoperability parameters within the standards, has the potential to achieve the required interoperability and portability of CCIS applications at a substantially reduced cost when compared with the use of military-unique specifications. Many aspects of the target architecture may be eventually expressed through selection of standards. However, the groups of standards applicable to CCISs have changed rapidly over the last five years and are likely to continue

to change for several reasons. The changes may be due to wider acceptance of one technical approach over other competing approaches, leading to international standardization of that approach. The changes may also occur as a natural process of stabilization and maturization of new models and understanding of the required services. In addition, and perhaps most important, changes may occur as a result of the introduction of new functions and new technology, such as high data rate local area networks. Finally, some standards will fall out of use as they are replaced by others that give better performance for CCISs. To adapt to the changing nature of CCIS standards, CCIS architectures must be flexible and not constrained to the standards mature and available at a specific time.

Table 2. Overview of Standards in the Eight Service Areas and Their Relation to ATCCIS Basic and Other Facilities

Data Management	Network	Operating System Interface	Security & OSI System Management	Data Interchange	User Interface	Graphics	Programming
ATCCIS DMF	ATCCIS TF & IOFs	ATCCIS SCF	ATCCIS SMF & Others	ATCCIS DMF	ATCCIS MSF	ATCCIS DMF & MSF	ATCCIS ALFs
Chapter 5	Chapter 6	Chapter 7	Chapter 8	Chapter 9	Chapter 10	Chapter 11	Chapter 12
SQL SQL2 SQL3 IRDS RDA ISAM TP ODP Data Elements	OSI RM X.400 MHS FTAM X.500 Dir. JTM ACSE CCR ROSE RTSE RPC ASN.1 BER PROFILES GOSIP EPHOS	POSIX OSCRL	NOSA SANISI ISO 7498-2 Security Frameworks Sec. Protocols P1003.6 SDNS BLACKER Systems Mgmt. Mgd. Objects CMIS CMIP Conf. Testing Estelle SDL LOTOS Reg. Authorities	ODA ODIF SGML EDI DTAM DFR RDT	HCI X-Windows Drivability UIMS Toolkit VDT TM MOTIF VT	GKS PHIGS	Ada Pascal C COBOL BASIC FORTRAN LISP Bindings CASE Tools CAIS PCTE PCIS IEEE Software Engin. Stds

3.6 Overview of the Standards Development Process

This section provides a summary of standards. It describes the role of standards, standards organizations, and the process by which standards are developed. It also gives information on ordering standards and updating their status. More information can be found in the following references: [Refs. NATO 1989; Stallings 1985; Stallings 1987; SC21 N 4911 1990; Rose 1990; INI 1987; Army 1989; and SPAG 1987].

3.6.1 Role of Standards

Standards convey information; their implementation can assure compatibility, reduce variety, and establish minimum levels of quality and reliability. Moreover, they can be categorized by type: interface, process, or product. Interface standards are the least restrictive and merely define certain characteristics. Process standards, while somewhat more restrictive, define the manner in which a process is performed, but do not determine the actual output. Product standards, since they define a particular output or outcome, tend to be the most restrictive. These categories also indicate the likely effects of a particular standard (or function of a standard) in terms of whether certain groups may resist the standard and how well the standard will be integrated into the technology life cycle. For example, a product standard promulgated too early in the technology life cycle may be resisted and not implemented by industry because it does not allow enough flexibility in adapting to anticipated changes in the technology. Conversely, simple interface standards may be insufficient for users or maintainers of a product who require accurate or detailed information about a particular product and how it functions [Ref. Putnam 1982].

In the case of CCISs, standards are used to achieve interoperability and increase portability so that the variety of commercial off-the-shelf (COTS) products can be increased. Therefore, most of the standards described in this document are interface standards. However, merely specifying standards will not necessarily yield interoperability. The standards must be accepted and to be accepted they must be correct and reflective of the state of practice. Moreover, many standards have options. To be interoperable, two systems using the same standard must have selected the same options and other types of interoperability parameters from a predefined standards profile. For example, the UK, US, and Canadian GOSIPs recommend certain standards and options for government implementations of OSI.

The NIST APP is one national approach to identifying standards that could be used to achieve an open environment that would ensure a high degree of applications portability. In addition to the operating system, this environment includes data management, data interchange, network services, user interface, graphics services, and programming services. Security and System Management Services underlie the seven basic services since they are integral to them all. Efforts are still required to specify the appropriate standards and "bindings" for the open environment. The complete APP proposed by NIST, together with the status of relevant standards other than POSIX, is discussed in Section 7.4.3.3.

Reference models are developed to provide a common framework for different standards and protocols. For example, the OSI comprises many standards, but the OSI Reference Model divides the scope of OSI standards into seven layers, showing what function each performs and how they interact. The reference model also indicates the model's relationship to other models and addresses issues that cut across several models.

A communications architecture is similar to a reference model, but is at a higher level. An architecture determines which services are required to perform the overall goals of an information system. The standards, protocols, and reference models work in harmony to perform these services.

3.6.2 Standards Organizations

This section discusses the organizations that produce standards. Chapter 14 discusses organizations that produce standardized profiles for open systems.

Standards come from various national and international sources including industry, implementor's workshops, governments, and international organizations. Of particular interest are those organizations developing standards within the context of the OSI Reference Model. A few of the important national, international, and military standards organizations are included in this section to acquaint the reader with the scope of their standards-making activities. Appendix F is a more complete listing.

Several international organizations are involved in the promulgation of standards. Two that are particularly relevant to computers and information technology are the ISO and the IEC. The ISO/IEC JTC1 is charged with international standardization of information technology systems [Ref. Cargill 1989, 126]. In addition, the CCITT and NATO issue recommendations and standardization agreements, respectively.

International Organization for Standardization (ISO). The development of an ISO standard, from first proposal to actual publication of the standard, is an arduous and time-consuming process, which ensures that the final result is acceptable to as many countries as possible. Figure 5 is a flowchart of the process.

If the CD obtains substantial support, it is then circulated as a draft international standard (DIS) for a six-month balloting period. If the DIS receives a majority approval by the TC members and 75 percent approval from all voting members, it is advanced to the Central Secretariat. If the balloting of the DIS is negative, the DIS text is revised by an editing committee and resubmitted as a second DIS for balloting or demoted to CD status for work to continue on building consensus. The Central Secretariat submits an approved DIS to the ISO Council, the board of directors of ISO. The council accepts the DIS as an international standard (IS),[2] and finally, ISO publishes the international standard.

A standard that has achieved DIS status is considered to be stable. Only minor changes are made to DIS text draft prior to becoming an international standard. If it is necessary to modify a standard, there is an addendum process whose steps are: working draft addendum (WDAD), proposed draft addendum (PDAD), draft addendum (DAD) with DIS status, and addendum (AD) with international standard status. A similar process

---

[2] ISO is used in this document to denote an international standard adopted by ISO or jointly by ISO/IEC.

[working draft amendment (WDAM), draft amendment (DAM), and amendment (AM)] is used for amendments. In addition, technical corrigenda may be approved to correct technical errors that do not affect the intended standardization.

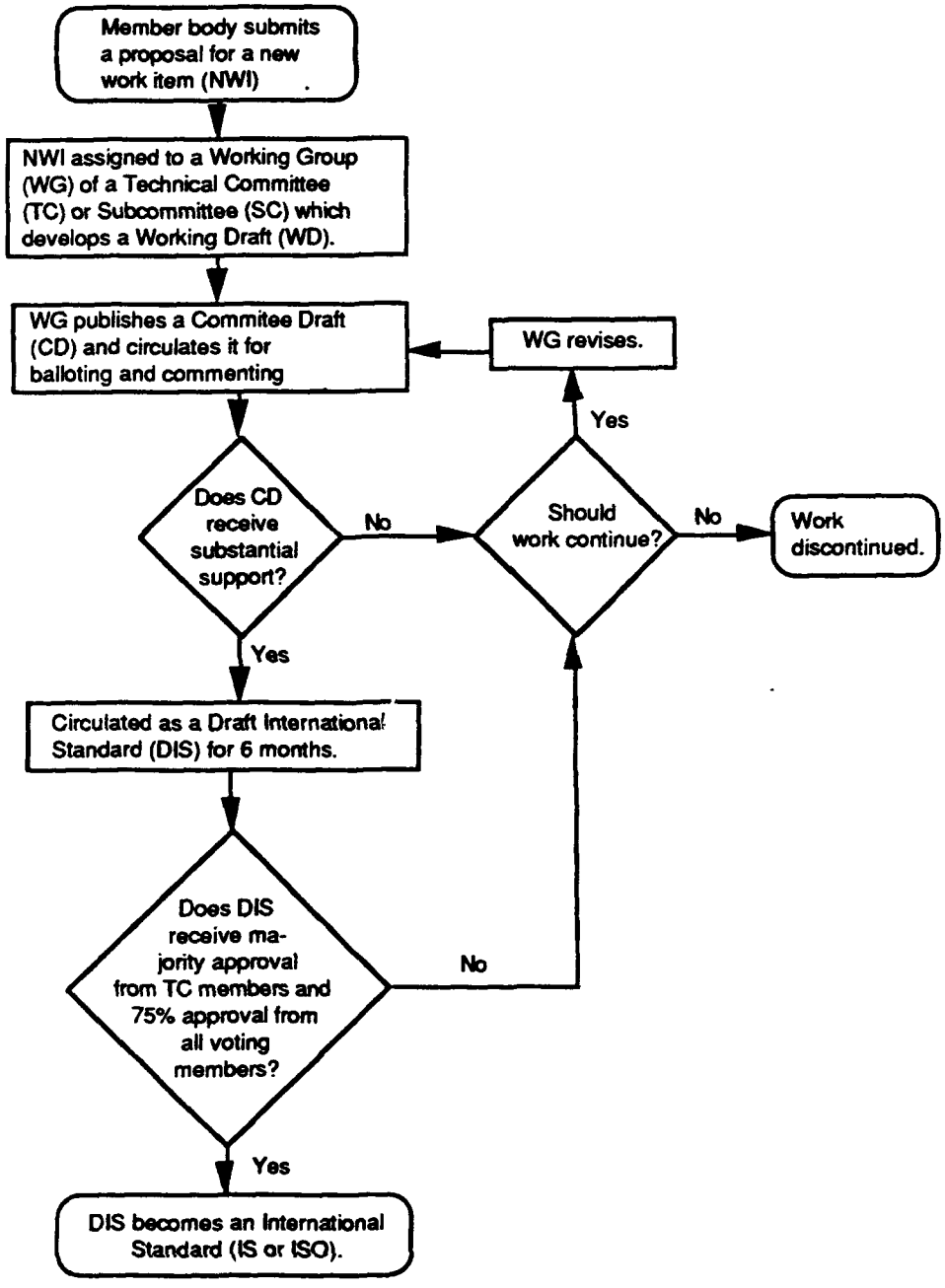


Figure 5. Flowchart of the ISO Standardization Process

The ISO/IEC JTC1 Special Group on Functional Standardization (SGFS) is developing standards for International Standardized Profiles (ISPs). As such, they bear an

ISP prefix in lieu of the traditional ISO prefix although their numbers follow the ISO numerical sequence. Designations for drafts being refined for ISP status are pDISP for proposed draft ISP and DISP for draft ISP.

ISO/IEC. ISO/IEC is a voluntary, nontreaty organization that develops standards in many areas. Founded in 1946, this organization promotes the development of standardization and related activities that facilitate the international exchange of goods and services.

The members of ISO/IEC are organizations chosen by the participating nations and nonvoting, observer organizations. Most ISO/IEC members are governmental standards institutions or organizations incorporated by public law.[3]

ISO/IEC is organized, under the administrative arm of the Central Secretariat, as a group of technical committees chartered to produce standards in various areas. The committee most relevant to this work is the Joint Technical Committee one (JTC1) of ISO/IEC (formerly, TC97 on Information Processing Systems). JTC1 is organized into subcommittees and working groups that actually produce the standards. The work related to OSI is carried on by subcommittees SC6 (lower layers) and SC21 (upper layers). More specifically, the working groups of prime interest are:

- SC6--Telecommunications and Information Exchange Between Systems
  - WG1--Data Link Layer
  - WG2--Network Layer
  - WG3--Physical Interface Characteristics
  - WG4--Transport Layer
  - WG5--Architecture and Coordination of Layers 1-4.
- SC21--Information Retrieval, Transfer, and Management for OSI
  - WG1--OSI Architecture
  - WG3--Database
  - WG4--OSI Management
  - WG5--Specific Application Services and Protocols
  - WG6--Session, Presentation, Common Application Service Elements, and Upper Layer Architecture.
  - WG7--Open Distributed Processing.

Now that the fundamental lower layer standards are in place, SC21 is the more active of the two subcommittees; a summary of the ongoing projects and expected completion dates of standards now in development is given in Appendix G. SC6 is active

---

[3] The member bodies from the FR, GE, UK, and US are the Association Francaise de Normalisation (AFNOR), Deutsches Institute fur Normung (DIN), British Standards Institute (BSI), and American National Standards Institute (ANSI). Other member bodies are identified in Appendix F.

in security and management for the lower layers, as well as continuing work in standardization of new subnetwork technologies and interworking of subnetworks. SC27 on Security Techniques is of interest to the security services discussed in Chapter 8.[4]

International Telephone and Telegraph Consultative Committee (CCITT). CCITT is a committee of the International Telecommunications Union (ITU), a United Nations treaty organization. CCITT is chartered to study and issue recommendations on technical, operating, and tariff questions relating to telegraphy and telephony. The primary objective of the organization is to standardize techniques and operations in telecommunications to achieve end-to-end compatibility of international telecommunication connections.

The members of CCITT, because it is a committee of a treaty organization, are governments. Normally, the members of the CCITT are the national Post, Telephone, and Telegraph administrations.[5] CCITT is organized into 15 study groups (SGs). There are three areas of activity concerned with OSI matters: data communications, telematic services, and integrated services digital networks (ISDNs). Work in CCITT is focused on specific formal questions posed at the beginning of the study period. In the three areas concerned with OSI matters, the work directly involves six SGs:

- SG I on the operational aspects of telematic services
- SG VII on interfaces to public data networks, including X.25 and related standards
- SG VIII on terminal equipment recommendations for the telematic services
- SG XI on switching and control signaling for telephony
- SG XVII on data transmission over the telephone network
- SG XVIII on digital networks in general and ISDN in particular.

Documents produced by CCITT are called recommendations, not standards; the term recommendation is used because CCITT does not have the authority of a standards body nor of its representative governments to prescribe implementation. Every four years the CCITT holds a Plenary Assembly that establishes the work program for the next four years. This work program is composed of questions submitted by the SGs based on requests made by the various member organizations. At the end of the 4-year period, each study group prepares draft recommendations in answer to these questions and submits them to the new Plenary Assembly. If the assembly approves these recommendations, the

---

4 The *ISO Technical Programme*, published in January and July, lists CDs, DISs, draft technical reports (DTRs), DADs, and DAMs in technical committee order. Each entry includes the target date, edition, title, and stage number. This same information for OSI (and related) standards is summarized twice a year by OSI layer in the Association for Computing Machinery Special Interest Group on Data Communication (ACM SIGCOMM) Journal *Computer Communication Review* (January and July issues).

5 The representation for the United States is from the Department of State.

drafts are published as CCITT Recommendations. In urgent situations, the drafts can proceed through a special balloting procedure to become a CCITT Recommendation before the normal 4-year period has expired. The new series of recommendations, when published, supersedes the recommendations from all previous study periods. All recommendations produced in the same study period are bound in books of the same color. For example, the 1984 recommendations are known as the "red books," the 1988 recommendations are known as the "blue books," and the 1992 recommendations will be known as the "yellow books."[6] Wherever possible these are adopted as ISO standards.[7]

Tri-Service Group on Communications and Electronics (TSGCE). TSGCE develops and maintains technical standardization agreements (STANAGs) for NATO. TSGCE has a number of subgroups and project groups working on standards. For example, TSGCE SG9 has responsibility for the NATO OSI Reference Model and for developing OSI STANAGs and profiles. Appendix F lists the various subgroups and project groups, and includes an organizational chart for NATO bodies in the fields of communication and information systems.[8]

3.6.3 Organizations Producing Standardized Profiles

Three international regional workshops of government and industry groups interested in implementation have been established to promote OSI and develop profiles. A Regional Workshop Coordinating Committee (RWCC) promotes dialog and harmonization among these workshops. The goal of the workshops is to define standards profiles that will ensure the interoperability of products from different vendors. The European Workshop for Open Systems (EWOS) promulgates harmonized technical proposals for functional profiles of OSI standards and corresponding conformance test specifications. The Asia-Oceania Workshop (AOW) also prepares technical proposals for standardized profiles. The most active AOW participant is Japan. The North American OSI Implementor's Workshop (NAOIW) provides North American input to the standardization of profiles (since the workshop is hosted by NIST, it is sometimes called the NIST OIW). The recommendations of this workshop form the basis for U.S. GOSIP. They also form the basis for a common OSI specification, called Industry/Government Open Systems Specification (IGOSS) being developed in the United States (see Section 14.4.7).

---

6 CCITT is currently evaluating electronic distribution of its recommendations. If it is successful, CCITT will be discontinuing their printed series.

7 CCITT recommendations are available in the United States from Omnicom, Inc., 115 Park St. SE, Vienna, VA 22180-4607, 1-800-OMNICOM.

8 NATO STANAGs are listed in *NATO Standardization Agreements and Allied Publications*, AAP-4(1990), which is available (as are the STANAGs) from the NATO Subregistry at national MODs.

3.7 Proposed Definitions for Terms Used in Standardization and CCIS Architectures

Table 3a provides the definitions of a number of technical terms used in this document and elsewhere in discussing standardization and CCIS architectures. These definitions were derived from many sources and proposed by the US CIM Standards Office. [Ref. Keane 1991]

Table 3a. Definitions of Terms for Standardization and CCIS Architectures

Application Software Interoperability: The ability to have application software operating on heterogeneous hardware/software platforms cooperate in performing some user function. (Source: NIST with modification)
Basic Interoperability: The exchange of information that preserves the meaning and relationship of the information exchanged. (Source: ATCCIS)
Buffer/gateway: Software or hardware used to compensate for a difference in rate of flow of data or time of occurrence of events or differences in protocol or in data representation when transferring data, from one system to another. (Preliminary. Source: NATO Interoperability Management Plan (NIMP), Edition 2)
Compatibility: The capability of two or more items or components of equipment or materiel to exist or function in the same system or environment without mutual interference. (JCS PUB 1)
Information system interoperability: The ability of systems to exchange data, in a timely manner, in support of a user-defined business decision process, and to preserve the meaning and relationships of the data exchanged. The degree of interoperability/information exchange, e.g., manual, limited automated, fully automated, is to be determined by the system users and developers.
Interoperability: The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (JCS PUB 1)
Open Specifications: Public specifications that are maintained by an open, public consensus process to accommodate new technologies over time and that are consistent with international standards. (Source: IEEEPOSIX1003.0)
Open System: A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: to be ported with minimal change across a wide range of systems; to interoperate with other applications on local and remote systems; and to interact with users in a style that facilitates user portability. (Source: IEEE POSIX 1003.0)
Open System Environment (OSE): The comprehensive set of interfaces, services, and supporting formats, plus user aspects, for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. (Source: ISO)
Portability: The ability to use application software and data on heterogeneous hardware/software platforms. (Source: NIST)
Scalability: The ability to use the same application software on many different classes of hardware/software platforms, form personal computers to supercomputers. (Source: NIST)
Taxonomy: A scheme for describing the orderly classification of objects according to their presumed natural relationship. The classification scheme is a system of signs and symbols (the vocabulary) that includes rules for the formation and transformation of admissible expressions (the grammar).
Technical Architecture: A set of standards such that information systems built to the standards are inherently interoperable. The degree of interoperability is to be specified by the functional user as part of the requirements definition process. (Preliminary. Source: Suggested by DMR and the ATCCIS)

Source: *CIM Terminology*, Private communication from Mr. John Keane, US DoD CIM Standards Office, CIM/XI, 16 July 1991, UNCLASSIFIED.

3.8 Assessments of Standards

Where possible, the following chapters provide assessments of the status of the standards in the eight service areas. The main assessments appear at the ends of the

chapters. Summary assessments, derived from the NIST Applications Portability Profile (APP), are provided at the beginning of the chapter in the form shown in Figue 6.

	LOC	PAV	CMP	MAT	STB	DFU	PRL
Standard 1	○		○	●	○		
Standard 2	●	○	●	●	●	●	●
Standard 3			○		○		

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

Figure 6. Classes of Standards and Their Relation to Groups of Standards

The notations of Figure 6 are defined as follows:

- Level of consensus -- A low evaluation is given to specifications that are proprietary or are used by a very limited or specialized group of users; a high evaluation is given for a specification that has already become an international standard; average evaluations are assigned for pubic domain specifications that are not standard, or that may be in the process of becoming a standard (i.e., standards committee work-in-progress), or that are widely available across various hardware/software platforms.
- Product Availability -- A low evaluation is given to specifications for which only a very few proprietary products are available; high evaluations are given to specifications for which there is a wide variety of products available from various vendors across different application platforms; average evaluations are assigned to specifications that may be proprietary but have many products available from a variety of vendors, or that are public domain specifications with products readily available.
- Completeness -- A specification is evaluated on the degree to which it defined and covers key features necessary in supporting a specific functional area or service.
- Maturity -- According to the underlying technology of a specification, a high evaluation indicates that it is well-understood (e.g., a reference model is well-defined, appropriate concepts of the technology are in widespread use, the technology may have been in use for many years, a formal mathematical model is defined, etc.). A low evaluation indicates that it may be based on technology that has not been well-defined and may be relatively new.
- Stability -- A high evaluation means that the specification is very stable, that no changes are expected within the next 2 years. A low evaluation indicates that significant or many changes are expected within a relatively short time, or that incompatibilities exist between current and expected releases of the specification. An average evaluation is given to those specifications that may have changes forthcoming to replace or deprecate features in the existing specifications.

- De facto usage -- This evaluation criterion estimates the likelihood that a vendor will independently propose products that conform to this specification whether or not a reference specification is stated in the procurement documents. A high evaluation indicates that most proposed products will conform to the specification. A low evaluation indicates that it is unlikely that the vendor will propose products based on the specifications. An average evaluation indicates that vendors are just as likely to propose products based on the specifications as not (i.e., no clear determination exists). In the cases of low or average evaluations, it is imperative that users include a specification in procurement documentation. A low evaluation does not necessarily mean that products implemented on the specification do not exist. It can also mean that some vendors would rather provide products that are not based on the recommended specifications.
- Problems/limitations -- Lower evaluations are assigned to specifications with severe restrictions on use or capabilities (e.g., licensing restrictions), or known problems tend to be too difficult or too numerous to overcome (e.g., new releases of the specification are not compatible with previous releases, or not enough is covered in the standard to be useful). An average evaluation is given to those specifications that require some minor additional facility in order to be fully effective in their intended environment.

4. ARCHITECTURES AND REFERENCE MODELS

This chapter describes the OSI Reference Model and several other reference models used in the standardization process. It also describes a number of CCIS architectures emerging in NATO and the nations that may, in part at least, be standards-based in the 1990s. The ATCCIS architecture is treated separately (Chapter 2). Specific CCISs are discussed in Chapters 16 (NATO) and 17 (national).

Quick Reference	
Topic	Page
Basic OSI Options	42
CIM Reference Model	52
Military Requirements	47
NATO C3 Architecture	47
NATO C3 Master Plan	47
OSI Reference Model	41
Tac Comms Post-2000	50
Tac CCIS Architectures	54

4.1 OSI Reference Model

The first step of the analysis of standards is the classification of the group of CCIS services in terms of the OSI Reference Model developed by ISO. In this model, the functions required for interoperation between data processing systems are divided into seven layers (Figure 7). Layers 1-4 are called the lower layers and are primarily concerned with control of the data transmitted between data processing systems. The Physical Layer (Layer 1) controls data transmission over physical media (e.g., wire). The Data Link Layer (Layer 2) augments the Physical Layer function by providing transmission error control along segments of the transmission network. The Network Layer (Layer 3) controls the data transmission route. The Transport Layer (Layer 4) provides protocols for moving data between end systems on the network.

Layers 5-7 are called the upper layers and are concerned with the interface between end systems. The Session Layer (Layer 5) establishes a logical connection between communicating end systems. The Presentation Layer (Layer 6) ensures that data from the network are presented to the user in an intelligible form. The Application Layer (Layer 7) provides services to the application programs that may request support from other systems on the network in order to complete their user-dictated tasks.[9]

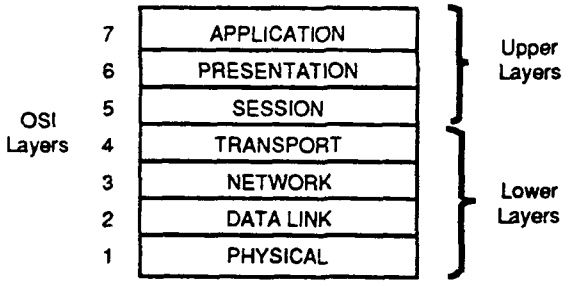


Figure 7. The Seven-Layer Model for Open Systems Interconnection

9 Architectural issues for OSI are treated in Chapter 6 on network service standards.

4.1.1 Basic Options in OSI Standards

Options for international standards that support the OSI model are often designated by grouping the OSI layers into two classes: application options and transport options (Figure 8). Using the definitions of [Ref. NATO 1989], the combined Layers 5-7 offer application options, while Layers 1-4 offer transport options. A separate category of relay options that provides interfaces between subnetworks will also be considered. Relay options normally are provided by Layers 1-3 (Figure 9). Examples of these options are illustrated in Appendix B.

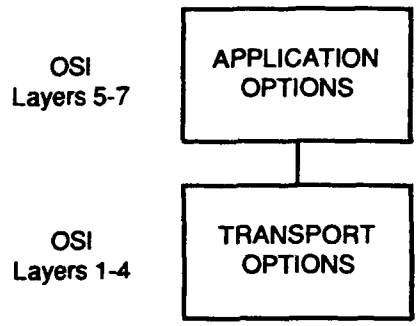


Figure 8. Composition of an OSI System

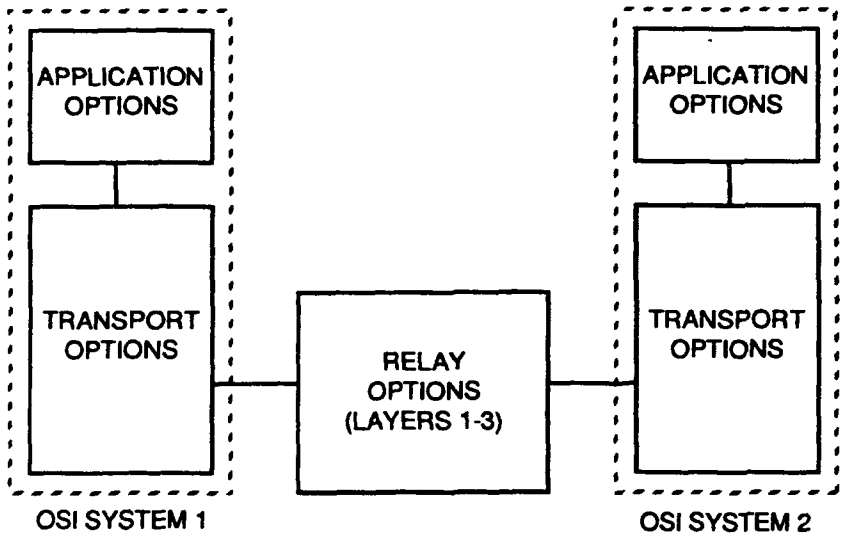


Figure 9. The Role of a Relay

The major application, transport, and relay options in OSI being developed by ISO, IEC, and CCITT are listed in Table 3b. The transport and relay options are addressed in Chapter 6 on the network services.

Table 3b. Application, Transport, and Relay Options Offered by OSI Standards

BASIC APPLICATION OPTIONS

- Primary Services:
  - Message Handling:
    - Message Handling Service (MHS) [CCITT]
    - Message-Oriented Text Interchange System (MOTIS) [ISO]
  - File Transfer Access and Management (FTAM)
  - Telematic Services (Teletex, Telefax, Textfax)
  - Virtual Terminal (VT)
  - Job Transfer and Manipulation (JTM)
- Other Services:
  - Directory
  - Distributed Transaction Processing (TP)
  - Open Distributed Processing (ODP)
  - Remote Data Access (RDA)
  - OSI Management
  - Application Service Elements (ACSE, RTSE, ROSE, CCR)
  - Information Resource Dictionary System (IRDS)
  - Office Document Architecture (ODA)
  - Computer Graphics Metafile (CGM) and Interface (CGI)
- Transmission Mode:
  - Connection Oriented (CO)
  - Connectionless (CL)

BASIC TRANSPORT OPTIONS

- Subnetwork Types:
  - Circuit Switched Data Network (CSDN)
  - Packet Switched Data Network (PSDN)
  - Dedicated Line (Point-to-Point Subnetwork)
  - Switched Telephone Network (STN)
  - Integrated Services Digital Network (ISDN)
  - Local Area Network (LAN)
- Transmission Modes:
  - Connection Oriented (CO)
  - Connectionless (CL)
- Transmission Media Interfaces:
  - Wire
  - Radio
  - Fiber Optic Cable
  - Microwave
  - Infrared

BASIC RELAY OPTIONS

- LAN to LAN
- LAN to Wide Area Network (WAN)
- WAN to WAN
- LAN to WAN to LAN

4.1.2 Connection-Oriented and Connectionless-Oriented Transmission Modes

One of the important issues that must be considered when reviewing OSI standards is the choice between connection-oriented (CO) services (also called "virtual circuit" services) and connectionless-oriented (CL) services (also called "datagram" services). Each of the seven OSI layers, except the Physical Layer, may be CO or CL. (The Physical Layer has no connection orientation.) The OSI Reference Model recommends that the upper four layers be either all CO or all CL. The following paragraphs, based on [Refs. Purton 1987; Stallings 1985; Stallings 1987a; and NATO 1987], address some prominent distinctions between these two classes of services.

The basic difference between CO and CL service is that CO service requires that an explicit relationship be established between the interacting peer entities before any further activity can take place, while in CL service no such explicit relationship occurs. A connection preserves the state of peer-to-peer communications from one data transfer to the next, storing and distributing information regarding the connection within the service provider, while the CL transmission does not. In CO service the relationship may be real—such as a dedicated circuit—or virtual, such as a particular path from node to node between peer entities in a CO packet-switched service. In the latter case the path would be agreed upon before data transfer begins and would remain unchanged during the transfer. A heuristic example of CO service is any national public telephone service; the regular delivery postal service is a heuristic example of a CL service.

CO service has three phases: connection establishment (set up), data transfer, and connection release (call termination). The route of each data packet is determined by the state of the network during the call set up and remains static for the duration of the connection. Since the state information is maintained for each established connection and the route of data packets is static, the data units are freed from the requirement to carry the full address of the required destination. The CO explicit relationship is established during the negotiation portion of the set-up phase and before the transfer phase. CO service provides for negotiation of the form of transmitted data and may maintain sequence and flow control. Error handling may also be supported. The overhead invested in setting up and maintaining a CO connection pays off when the data transfer phase is relatively long. The CCITT Recommendation X.25 for interfacing to a packet switching wide area network (WAN) is an example of a CO protocol.

In contrast, CL service has only one phase—namely, data transfer. The form of the data transferred must be pre-arranged between peer entities. Sequencing, flow control, and error handling are not supported by the CL service, but are instead the responsibility of the interacting peer entities. Sometimes referred to as a "datagram" service, CL service

requires each data unit to be self-contained; there is no relationship between individual data unit transfers.

While the service mode at each of the six highest OSI layers may be CO or CL, crossover between the two types of service usually occurs only at the Network Layer (Layer 3). In these cases, the connection orientation of the Application Layer (Layer 7) agrees with the connection orientation of Layers 4, 5, and 6; further, the connection orientation of Layers 2 and 3 also agrees, but this orientation may differ from that of the higher layers. The rationale for maintaining the service mode (CL or CO) throughout Layers 4-7 is based on the recommendation of the ISO Reference Model for simplifying system and protocol complexity, specifically that the features at one layer should not be negated by the unavailability of similar services at another layer. The goal of the OSI Reference Model is to limit the amount of *a priori* information exchanged between end systems regarding services used to communicate, which is best met by limiting the mixing of service modes. The following ISO/IEC standards for the four cases of connection orientation of the transport and network services are:

- ISO 8602 for CL transport and CL network
- ISO 8602 for CL transport and CO network
- ISO 8073 for CO transport and CO network
- ISO 8073 DAD 2 for CO transport and CL network.

The many resulting combinations of service are useful in different circumstances. CL service may be appropriate for military applications that require robust networks capable of continuing data transfer even as some nodes are taken out of service, especially for the lower layers (network and data link). [Refs. Purton 1987 and Stallings 1987a] give some additional examples of cases for which CL service is appropriate, even for the upper layers. Included are inward data collection from the sampling of data sources, broadcast messages, some distributed transactions, some real-time transmission applications, and cases in which one or more communicating peers are mobile. In general, CO service is beneficial when long-lived connections with extensive data transfer are anticipated. FTAM is an example of an application that would likely benefit from a CO connection.

The cases in which Layers 2 through 7 are all either CO or CL are more straightforward than cases with upper and lower layers of different orientation. If CL upper layers operate over CO lower layers, the full functionality of the lower layers is not employed; the application in this case does not enjoy the amenities of CO service.

The OSI standards supporting CO service were the first to be developed and are nearly complete. Until recently, standards supporting the lower layer CL service were more advanced than those supporting upper layer CL services. CL protocols for the Transport Layer (ISO 8602), Session Layer (ISO 9548), and Presentation Layer (ISO 9576) are complete.

Choice of connection orientation affects the structure of the Network Layer and to some degree the performance of services in the Network and Transport Layers. The Network Layer is divided into three sublayers (ISO 8648, *Internal Organization of the Network Layer*). From top to bottom they are the Subnetwork Independent Convergence Protocol (SICP), the Subnetwork Dependent Convergence Protocol (SDCP), and the Subnetwork Access Protocol (SAP). This structure is preferred by many European countries. In a CL network, the Network Layer is divided into two sublayers: Internetwork Protocol (IP) and Subnetwork Specific Protocol (SSP), where the IP focuses on unreliable internetwork transfer of information while the SSP focuses on the reliable transfer of individual data units across the supporting networks. The CL approach is favored by the United States [compare the OSI profiles recommended by the United Kingdom and the United States given in Section 6.4.3, noting that ISO Class 4 Transport Protocol (TP4, discussed below) provides services for CL networks]. In the CL model, end-to-end responsibilities are placed in the network sublayers, whereas in the CO approach the end-to-end requirements are placed in the Transport Layer. One drawback of using TP4 over a CO network is the size and complexity of the implementing code. For this and other reasons, many implementors of CO stacks do not support TP4. Section 6 of [Ref. NATO 1987] provides an analysis of the impact of the choice of CL or CO mode on the interconnection of heterogeneous military networks.

As in the Network Layer, there are significant differences in the protocols for the Transport Layer in connectionless and connection-oriented modes. The CL transport protocol (TP) makes use of only a subset of the CO network services, while the CO TP makes use of all the CO network services. The CL transport service is not expected to provide ordered delivery, flow control, or error control. Hence, the CL TP is very simple and requires only a single type of transport protocol data unit (TPDU). Ten types of TPDUs are used to provide CO transport services. There are five classes of the CO TP, of which only Class 4 can make use of a CL network service [Ref. Stallings 1987]:

- Class 0. Simple class, oriented for Teletex (upgrade to CCITT T.70). Connection flow control is based on network flow control, and connection release is based on release of the network connection
- Class 1. Basic error recovery class, designed to run on a CCITT X.25 network and provide minimal error recovery for network-signalled errors. TPDUs are numbered so that they can be resequenced
- Class 2. Multiplexing class, an enhancement of Class 0 that still assumes a highly reliable network service. Has the ability to multiplex multiple transport connections onto a single network connection
- Class 3. Error recovery and multiplexing class. Provides the union of the capabilities of Class 1 and Class 2
- Class 4. Error detection and recovery class. Assumes that the underlying network service is unreliable, in particular that the TPDUs may be lost or arrive

out of sequence. Provides for TPDU retransmission, duplicate detection, flow control, connection establishment and termination, and crash recovery.

4.2 Military Requirements for OSI

During the past 8 years, NATO and the Nations have been addressing a number of deficiencies in the emerging OSI standards that need to be addressed to military needs. The eight deficiencies being addressed in TSGCE SG9 are (see Chapter 15 for definitions):

- Multihomed, mobile host systems
- Multi-endpoint connection
- Internetworking
- Network/system management functions
- Security
- Robustness and quality of service
- Precedence and preemption
- Real-time and tactical communications.

With respect to the eighth military feature, "Real-time and Tactical Communication," MITRE developed a proof-of-concept prototype system to test the applicability of GOSIP protocols in the tactical environment and concluded that the full OSI protocol stack could be used for tactical messages if the use of OSI Congestion Avoidance is required and the number of Message Transfer Agents (MTAs) that must be traversed is minimized. In addition, the architectures of the implementations must focus on efficient queue handling and connection handling [Ref. Messing et al. 1990].

Other efforts underway to evaluate potential OSI performance for tactical systems include a MITRE traffic study [Ref. Galitzer 1991] using loads of the US Maneuver Control System (MCS, see Section 17.1.5) traffic found in the MCS Segment Specification. Experiments were conducted that evaluated traffic between command posts and internal command post traffic between maneuver control and other battlefield functional areas (e.g., fire support). All of the experiment's messages were sent with normal priority and, at 600 bps delivery rates, all messages arrived in 15 minutes. Separate work done by McArthur and Bryant [Ref. McArthur 1991] in 1991 found that overhead generated by X.400 could seriously affect real-time and near-real-time tactical applications on low-bandwidth networks. For an example message with 7 recipients, 3,532 octects (28,256 bits) of overhead were required. They note that overhead may be reduced by more efficient encoding or more selective used of X.400 parameters and conclude that "on the surface, however, it appears that X.400 is not well suited for most tactical applications which require real-time or near-real-time responses."

4.3 NATO C3 Architecture

4.3.1 Relation to NATO C3 Master Plan

The *NATO Consultation, Command and Control (C3) Master Plan* distributed in draft form in July 1989 for comment by the nations has four parts, one of which--the NATO C3 Architecture--has five volumes:

- *NATO Consultation, Command and Control (C3) Master Plan,* Edition 1
- *Tri-Major NATO Commanders' Command and Control (TRI-MNC C2) Plan,* Edition 4
- *Political Consultation and NATO Civil Emergency Planning (PCNCEP) CIS Plan,* Edition 1
- NATO C3 Architecture: NACISA/APD/C3AB (89) 101 NACISA, 31 May 1989:
  (1) Volume 1, *Consolidated Architecture*
  (2) Volume 2, *HQs and Facilities Subsystem*
  (3) Volume 3, *Information System Subsystem*
  (4) Volume 4, *Communications Subsystem*
  (5) Volume 5, *Sensor and Warning Installations Subsystem.*

All but the TRI-MNC C2 Plan were prepared by the Information Systems Working Group (ISWG) and Communications Systems Working Group (CSWG) of the NATO Communications and Information Systems Committee (NACISC). The TRI-MNC C2 Plan was prepared by the three Major NATO Commands (MNCs).

The NATO C3 Master Plan specifies NATO C3 priorities across the key mission components and all civil functions. The Mission Oriented Approach (MOA) methodology was used to integrate, harmonize, and order the requirements and proposed solutions of the three interrelated contributory components: the TRI-MNC C2 Plan, the PCNCEP CIS Plan, and the NATO C3 Architecture.

4.3.2 Background to the NATO C3 Architecture

The NATO C3 Architecture is based mainly on the 1980-1982 Architecture Design Study (ADS), the ADS follow-on studies (STC Projects 85-3 and 86-1), and ATCCIS Working Papers (WP 11, WP 24, and WP 25). The Architecture applies to the NATO Command, Control and Information System (NCCIS), which is comprised of ACCISs.

4.3.3 Attributes of the NATO C3 Architecture

The NCCIS Architecture describes an automated CCIS in precisely the same terms used to describe ATCCIS: "a transaction processing system with a partitioned, partially replicated database, capable of supporting applications, and maintaining a consistent interpretation of the data across organizational boundaries." Systems conforming to the

Architecture are identified as "NCCIS-conformant." As in ATCCIS, NCCIS-conformant systems have three minimum required capabilities:

(1) A mechanism that provides the required end-to-end transfer of data

(2) A mechanism to manage the storage, retrieval, and interpretation of data

(3) A mechanism that manages these two mechanisms.

As in ATCCIS, the NCCIS architecture employs the concept of basic interoperability to address two needs: the need to communicate so as to permit the exchange of data, and the need to have a common interpretation of the data thus exchanged. The NCCIS Architecture identifies the following as required to achieve basic interoperability: international OSI information exchange standards, data dictionary, data model (defining logical structure of data), and database conceptual schema (logical database design).

The NCCIS Architecture uses the concept of enhanced interoperability to describe interoperability aspects that go beyond basic interoperability. In NCCIS, these apply only to NATO-owned systems for "higher degrees of interoperability to support other operational requirements, flexibility, and cost saving." Examples of areas where higher degrees of interoperability can be achieved in NCCIS are common and generic application programs and human-machine interface:

- Common application programs refer to those application programs that are not defined for a specific application (automation of a key task) and are suitable to support a wide range of applications and users
- Generic application programs where the whole or part of a Key Task may be subject to agreement by commands regarding a common procedure for the performance of that Key Task.
- Human-machine interface standards may bring interoperability of CCISs to what is called "common look." This means that commanders will have access to functions and data using uniform access and presentation methods.

Information requirements for NCCIS, as in ATCCIS, are analyzed in terms of C2 Products and the information items that can be used to construct the C2 Products. NCCIS supports the requirements that each user be associated with a functional area and that the user be able to access and manipulate items in the information set owned by that functional area. It explicitly supports three major classes of functionality: (1) automation of key tasks, leading to support of decisions and execution of other functions; (2) automated support for the exchange of information items, including preservation of meanings and relationships; and (3) allowing users to access and manipulate information items. As in ATCCIS, NCCIS provides for three mechanisms for information exchange: data management services, application programs to support exchange of formal messages, and electronic mail for *ad hoc* information exchange.

NCCIS identifies five major classes of services: information exchange, data management, system control, application support, and human-machine interface management. In NCCIS these services are discussed as functions. The standards identified for supporting the architectures are identical for NCCIS and ATCCIS. Differences between NCCIS functions and ATCCIS facilities for these required classes of services include:

a. NCCIS is a complete architecture for an automated CCIS, whereas ATCCIS focuses on four Basic Facilities required as a minimum to support basic interoperability.

b. ATCCIS provides the SMF to include any system management services not provided by the other Basic Facilities, whereas in NCCIS, system management is seen as being provided exclusively by the classes of service. (To date, no additional SMF-unique services have been identified; therefore, the NCCIS and ATCCIS architectures are consistent.)

c. Security services are described in detail for NCCIS and are expected to be supported by each class of service in NCCIS.

d. Detailed descriptions of the NCCIS functions differ, in part, from those of the corresponding ATCCIS facilities. However, the Annexes of the NATO C3 Architecture that specify the data management, system management, and system control functions are nearly identical with the descriptions of the DMF, SMF, and SCF in the ATCCIS architecture.

4.4 NATO Tactical Communications Architecture Post-2000

TSGCE SG11 has a project group (PG6) that is developing a tactical communications architecture for the same timeframe as ATCCIS (post-2000). Its major components are a Local Access Subsystem (LAS), a Wide Area Subsystem (WAS), and a Mobile Subsystem (MS). Figure 9 depicts an extended LAS component with three interconnected LASs.

PG6 has also developed a conceptual Post-2000 NATO Reference Model for use with the future tactical communications architecture with seven layers (not identical with the OSI and current NATO Reference Model): Media Layer 1, Access Layer 2, Routing Layer 3, End-to-End Layer 4, Session Layer 5, Presentation Layer 6, and Application Layer 7. The upper layers and the protocol stacks envisioned for network management protocols for the Post-2000 Tactical Communications Architecture are shown in Table 4.

The LAS provides the means for user access to the WAS and for local communications services in the local area. Additionally, it provides interfaces to the civilian commercial network. The LAS is composed of distributed access LANs and centralized access PABXs connected by dual fiber optic rings (see Figure 10). The access LANs provide service access for a distributed community of interest to the dual ring LAN, while the PABXs represent the interconnection of existing switching equipment to the new network. The PABX will be phased out and replaced by LAN technology as the

architecture evolves into the future. The dual ring LAN has a wide-band Asynchronous Transfer Mode (ATM) switch that provides access to other LAS rings via a LAS radio or to the WAS nodes via WAS radio links. The LAS radio is also used, as well as fiber optic cable, to extend the dual ring in the event of a geographical obstacle. User access to the LAS is via a single channel providing integrated (voice, data, and video) services either separately or simultaneously. User terminals are envisioned to function similarly to commercial ISDN terminals, using ISDN-type signalling and message sets modified for tactical use to control and request access to integrated user services.

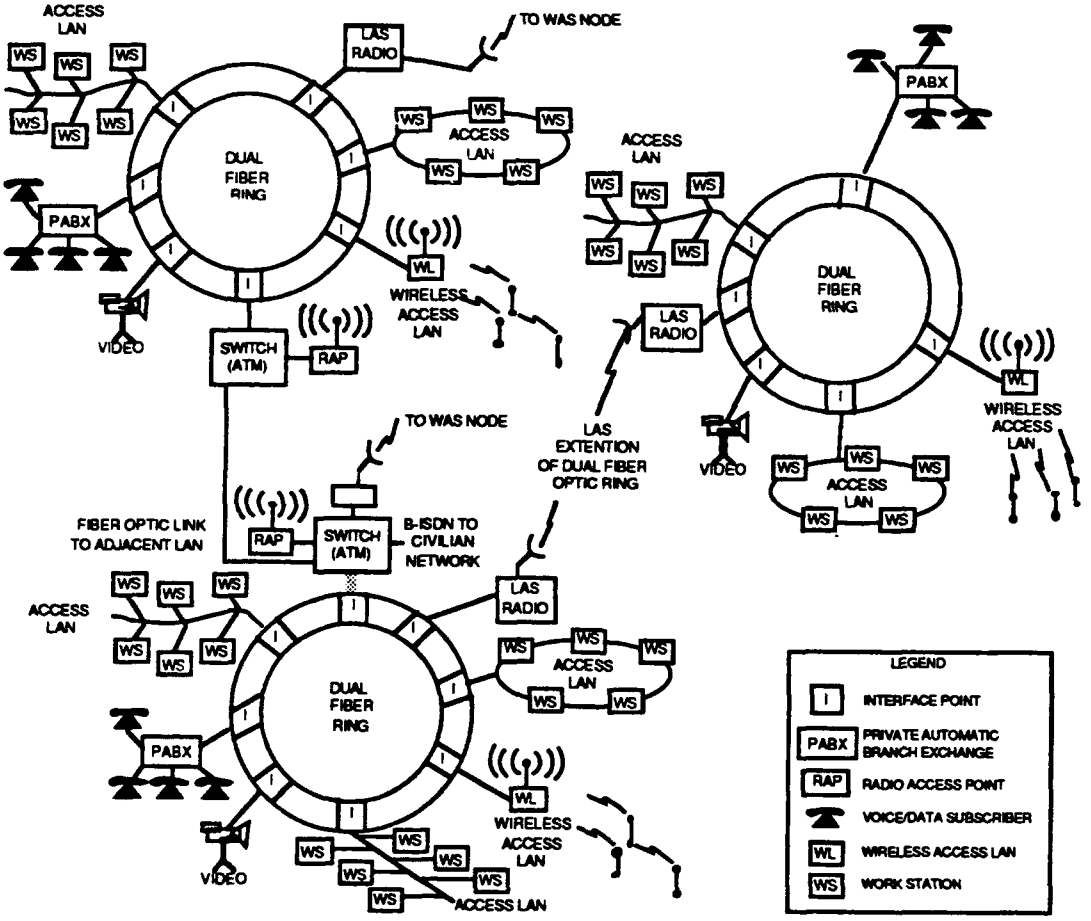
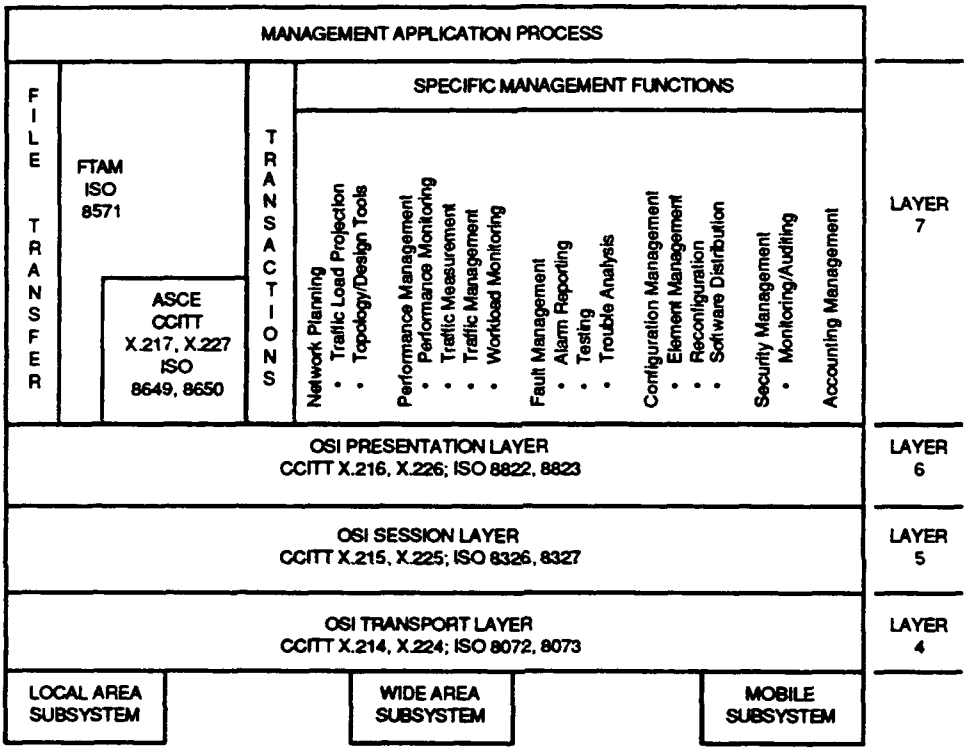


Figure 10. Post-2000 Tactical Communications Architecture-Extended LAS

The WAS provides long-haul transport and switching of user services through the tactical network as well as local access to users in the vicinity of a WAS node. WAS nodes are really extensions (explosions) of the LAS architecture with longer-range transmission and greater variety and number of transmission resources. ATM technology is used to replace fixed-bit-rate circuits with flexible virtual circuits in which capacity is negotiated on an as-needed basis. The ATM capability of the WAS architecture will replace current-generation circuit, packet, and message switches with fast "asynchronous" packet

switches. These switches will be linked by wideband trunks in which the full capacity of the radio link will be available to the switch as a single wideband circuit rather than multiplexed narrow-band time-division-multiplexed circuits. The ATM switch will statistically multiplex the instantaneous demand for virtual circuit service from diverse end users on this single wideband channel.

Table 4. Proposed NATO Post-2000 Network Management Protocols

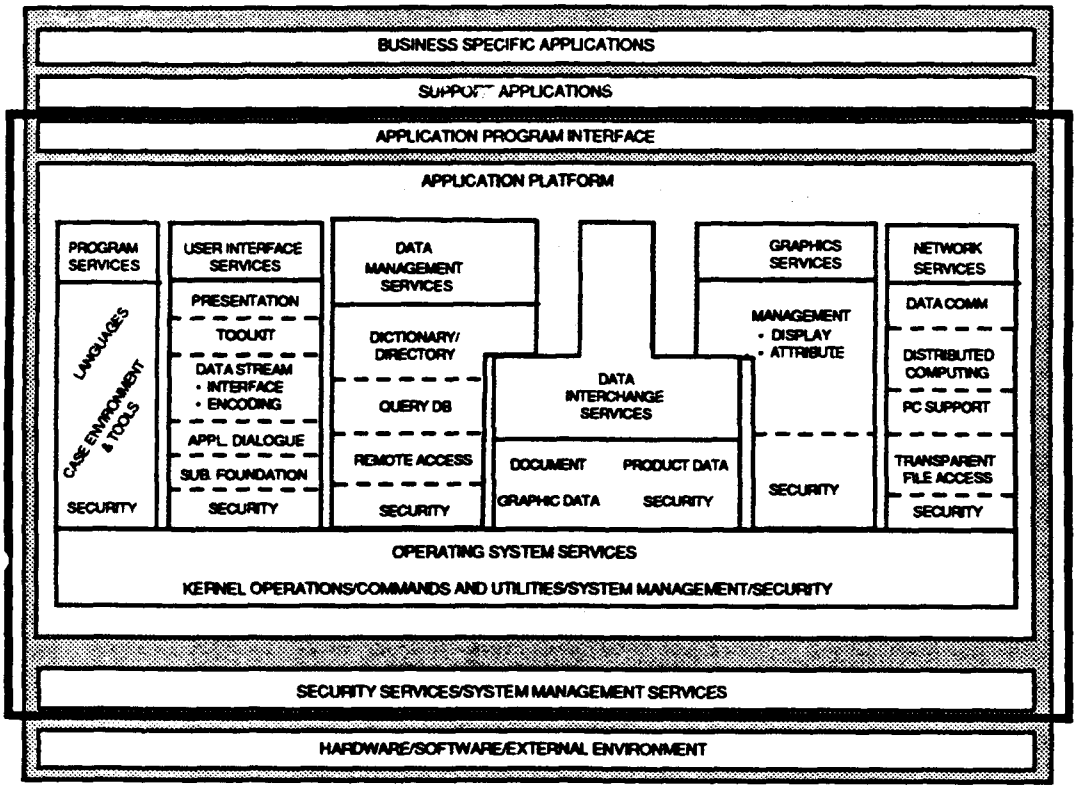


Source: *Subjective Evaluation of Candidate Architectures for the Tactical Communications Systems Land Combat Zone Post 200*, Draft, Prepared by the United States for TSGCE PG6, 10 May 1991, NATO UNCLASSIFIED.

4.5 US DoD CIM Reference Model

The US DoD has been developing a standards-based approach to corporate information management (CIM), which includes not only CCISs but also the business and supporting base information systems for the military. A key strategy for implementing CIM in the US DoD is the transition of DoD's present information systems and associated information technology resources to a communications and computing infrastructure based on the principles of opens systems architecture and systems transparency. DoD has developed a CIM Technical Reference Model to provide technical guidance for the acquisition, development, and support of DoD information systems and associated infrastructure systems. The CIM Technical Reference Model, shown in Figure 11, provides the high-level relationships of the CIM domain and shows the major service areas

and their relationships. When populated with specific standards, the model defines a profile of recommended technical standards for DoD information systems. The model, while not an architecture, defines standards and guidelines that can be tailored and applied to meet the needs of specific business units (i.e., mission areas or functional areas). The goals of the model are to: improve user productivity, development efficiency, portability, scalability, and interoperability; promote vendor independence; and reduce life cycle costs. These goals are to be achieve by following the principles identified in Table 5. [Ref. CIM 1991]



Key: Heavy solid lines identify those areas addressed in WP 25.

Figure 11. The US DoD CIM Technical Reference Model

Table 5. Objectives and Principles for the CIM Technical Reference Model

OBJECTIVE	PRINCIPLES
Improve User Productivity	• Consistent user interface. A consistent user interface will ensure that all CIM capabilities will appear and behave in a similar, predictable fashion regardless of application or site. This has the benefits of simplifying training, facilitating the development of future applications, and improving ease of use across applications. • Integrated applications. Applications available to the user will be consistent. Support applications, such as office automation and electronic mail, will be integrated with business unit specific applications • Data sharing. Databases will be shared across DoD in the context of security and operational considerations. • Consistent security interface. Security features will have similar characteristics across business unit applications. Users will see the same security labels in a common format and manage them in the same way. User login will be consistent across applications.
Improve Development Efficiency	• Common development. Applications that are common to multiple business units will be centrally developed or acquired. • Common Open System Environment. A standards-based common operating environment that accommodates the injection of new standards, technologies, and applications on a DoD-wide basis will be established. This standards-based environment will provide the basis for development of common applications and facilitate software reuse. • Use of commercial products. To the extent possible, hardware-independent commercial off-the-shelf products should be used to satisfy requirements in order to reduce the dependence on custom developments and to reduce development and maintenance. • Software reuse. For those applications that must be custom developed, incorporating software reuse into the development methodology will reduce the amount of software to be developed and add to the inventory of software suitable for reuse by other systems. • Resource sharing. Data processing resources (i.e., hardware, software, and data) will be shared by all users and applications requiring those services and having the proper authorization.
Improve Portability and Scalability	• Portability. Applications that conform to the model will be portable, allowing for movement across heterogeneous computing platforms with minimal modifications. In addition, implementing activities will be able to upgrade their hardware base, as technological improvements occur, with minimal impact on operations. • Scalability. Applications that conform to the model will be configurable, allowing operation on platforms ranging from microcomputers to mainframes depending on user requirements.
Improve Interoperability	• Common infrastructure. The DoD will develop and implement a communications and computing infrastructure based on open systems and systems transparency, including but not limited to operating systems, database management, data interchange, network services, and user interfaces. • Standardization. By implementing standards from the CIM Technical Reference Model, applications will be provided a common set of services that improve the opportunities for interoperability.
Promote Vendor Independence	• Interchangeable components. Hardware and software will be acquired or implemented so that the insertion of new products will result in minimal disruption to the user's environment. • Non-proprietary specifications. Capabilities will be defined in terms of non-proprietary specifications that are available to any vendor for use in developing commercial products and that support full and open competition.
Promote Vendor Independence	• Interchangeable components. Hardware and software will be acquired or implemented so that the insertion of new products will result in minimal disruption to the user's environment. • Non-proprietary specifications. Capabilities will be defined in terms of non-proprietary specifications that are available to any vendor for use in developing commercial products and that support full and open competition.

Table 5. (Continued)

OBJECTIVE	PRINCIPLES
Reduce Life Cycle Costs	• Reduce duplication. Elimination of "stovepipe" systems and "islands of automation" in favor of interconnected open systems that can share data and other resources will dramatically reduce overlapping functionality and unneeded redundancy. • Reduced software maintenance costs. If the principles described above are implemented, reductions in software maintenance will be realized because there will be less software to maintain. In addition, if the use of COTS products is increased, support costs will be reduced further since COTS vendors distribute their product maintenance costs across a much larger user base. • Reduced training costs. A reduction in training costs will be realized as users rotating to new organizations will already be familiar with the common systems and consistent interfaces.

Source: *Technical Reference Model for Corporate Information Management,* Versions 1.0, Center for Information Management, US Defense Information Systems Agency, 4 November 1991, UNCLASSIFIED.

4.6 Example Defense-Wide CCIS Architectures

The military Services of the US DoD have been developing a number of architectures of future (near- to mid-range) CCISs that support cross-functional information exchange and provide for intra-Service and (in most cases) inter-Service interoperability. Some examples of DoD-wide CCIS architectures and models are discussed in this section; Service-unique architectures are discussed in Section 17.3.

Architecture and Target Profile for Worldwide Command and Control System (WWMCCS). An architecture, which provides the structure of a system, and a target profile, lists standards used in building a system that conforms to the architecture, has been developed for the next generation (post-1995) WWMCCS ADP Modernization (WAM). The architecture is designed to be generic for all CCISs. The CCIS generic architecture and WAM target profile promote the following principles:

a. Systems will be open. People and computer programs will be able to exchange data and services among different parts of the system without regard to differences in suppliers of hardware and software.

b. Systems will be distributed. Computers and storage devices will be located in different command centers. Command centers may be made up of dispersed cells; key users will carry their computing resources wherever they go. Application programs and data will reside on computers at thousands of locations.

c. Distributed components will cooperate according to standard protocols that implement, among other things, a client-server model. That is, application programs make use of other programs, possibly on other computers, to perform such services as data management and communications.

d. Software designs will be layered to encapsulate design details that are expected to change. Three special cases of layered design are the OSI model, separation of data management from applications, and standardization of interfaces to operating systems.

The target profile includes standards for an information system whose interface specifications comply with open system standards defined by the National Institute of Standards and Technology (NIST) and by other standardization groups. The definition is not constrained by the limitations of the present WWMCCS, but contains the best technology expected to be available in the latter half of the present decade. It enables a move toward the goal of an open system while satisfying WAM requirements.

The architecture provides support for evolvability and interoperability. The architecture recognizes that: user needs cannot be predicted with complete accuracy; requirements change; technology becomes obsolete; the market continually provides better products; and systems evolve, not in distinct generations, but in a steady flow of changes and improvements. The architecture is based on an open system environment, which supports evolution by separating functions into a layered architecture whose boundaries adhere to accepted standards defined through open consensus.

In the generic CCIS architecture, a CCIS is treated as a distributed information system of nodes connected by networks. Within a node, functions now served by a central computer and terminals are expected be provided by a local network of servers and workstations, and each node would be connected to others through a wide area network. The CCIS of the future is envisioned to be a group of interconnected wide area networks. Thus, the generic architecture is a network of networks that connect nodes, each of which may itself contain a network. To describe this complex structure, seven areas are defined to group relevant protocols and interface standards:

a. Data Management supports the storage, control, distribution, management, and allocation of simple data such as text and numeric information and complex items such as complete documents, maps, charts, images, and multimedia objects. Information about the network and nodes themselves (e.g., configuration data) will be also handled through data management services.

b. Network Services are the transmission and interface standards and protocols that support logical and physical communication. They describe and constrain how the hardware and software of the nodes cooperate in node-to-node interaction.

c. User Interface Services support visual and functional interaction with the user, providing access to hardware and software and graphical user interface. They control the presentation format of data and mode of interaction.

d. Operating Systems manage hardware and software resources and program interfaces, including local and distributed execution of application programs. Standards in this domain include those that cover program-to-program communication and synchronization as well as management of memory and interfaces to network and data management services.

e. Security provides for the privacy, protection, and integrity of the programs and data that make up the CCIS. Security pervades the model, applying at every interface and point of data transfer.

f. Programming Services control CCIS application development and the execution of applications.

g. Data Exchange Standards permit the exchange of data among applications, transfer of data between systems, and display of data to the user in a way that preserves the meaning and relationships in that data.

The functional parts of the architecture and the service areas fit together as shown in Figure 12. The architecture has data management, networks, operating systems, user interfaces, and application functions. These equivalent services jointly support the execution of applications. Data Exchange is not associated with a particular part of the structure; rather, it is a set of standards that mediate data interchange among applications and between the support functions as well. Security is similarly not associated with a particular part of the structure but can be considered analogous to a "substrate" that underlies the entire structure.

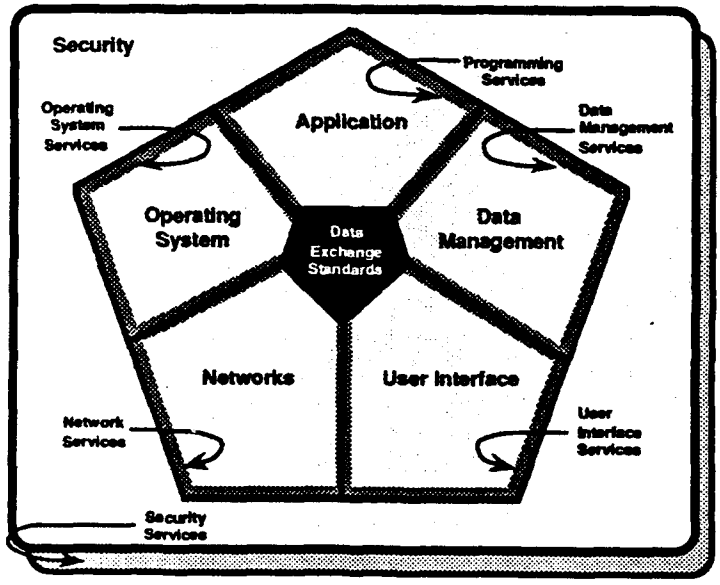


Figure 12. Services and Interface Connectivity

The WAM target profile is a listing of standards intended to provide guidance to those who will design a CCIS in the 1995-97 time period. It reflects standards expected to be current during that period and identifies areas where standards may be insufficient. Table 6a summarizes the specific areas covered by the profile. Although multilevel security is part of the given CCIS requirement, it is not anticipated that standards for validated, trusted multilevel security will be in place in time for a 1995-97 development. Pending the report of the DISSP (see below), no recommendations for security beyond system-high mechanisms are made in the current draft WAM target profile.

Table 6a. WAM Target Profile

Data Exchange
X.12, EDIF---Formatted documents
ISO 8613, 8839, 10179---Unformatted
ISO 8632---Computer graphics files
ISO 10303---Product model data
STDS, VPS, DIGEST---Maps and geographic information
Multimedia
ISO 19018, 11172, JBIG, X.56---Data compression
ASCII

Data Management
Data management reference model
SQL
Information resources directory system
Remote data access
Distributed transaction processing

Networks
ISO-OSI reference model
GOSIP
- Upper layer standards
- Lower layer standards
- Intermediate layer standards
- Application layer standards
  - Directory services
  - FTAM
  - Message handling
  - Remote data access
  - Remote procedure call
  - Transaction processing
  - Telematic standards
  - Virtual terminal

Operating Systems
POSIX
- Basic services
- Ada bindings
- Real-time extensions
- Security extensions
- Shells and utilities
- System management
- Distributed system services

Programming Services
Ada
C and C++
Other languages
CAIS-A
PCTE+

Security Services
"Rainbow books"
Trusted database management
Secure data network system
Standard for interoperable LAN security

User Interface
User interface architecture (based on APP)
- Window management
- Toolkit and user interface management
- Terminal management

Graphics
- Graphics subroutine library
- Device independent and dependent stds.
- Color standards
- Rendering standards

Human factors standards

Note: The NIST Applications Portability Profile is basic to the Target Profile and appears explicitly or implicitly in most of the service areas.

DoD Integrated Communications Architecture. The Defense Information Systems Agency (DISA) and the military Departments are formulating information and security architectures for an Integrated Communications Architecture (ICA), concerned with platform, base-level, and long-haul communications. These architectures are expected to be founded on local ISDN switches and high-speed LANs; the long-haul networks will also provide ISDN service. In security, new technology for end-to-end and multi-level security devices is being exploited. [Ref. COPERNICUS 1991]

DoD Common Operating Environment. The US Army, Navy, Marine Corps, and Air Force have agreed on a Common Operating Environment (COE) based, in

part, on US GOSIP and the NIST APP/OSE.[10] The goal of the COE is to reach consensus among the Services as a means of promoting interoperability, portability of applications, and the sharing of ideas, software, and data products. The COE addresses, in part, the growing interdependence among federal organizations; critical need for common architectures, communications networks, and databases; excessive dependence on single vendors; and underdeveloped interoperability of products and portability of people, data, and applications. Anticipated benefits are improved efficiency of Service systems in supporting deployed commanders, reduce costs by cutting development and fielding time, reduce porting effort, improved interoperability between systems, reduced training time, reduced duplication of effort between Services, improved system capabilities, and reduced maintenance efforts.

The COE is a suite of standards agreed to by a consensus of participants. The standards will be commercial standards where possible to further reduce the cost of developing software. The elements of the environment to be addressed, eventually, by the COE standards include the following:

- Open system hardware architecture
- Data architecture
- Software documentation
- LAN/BUS interfaces
- Programming language
- Operating system
- Human-machine interface
- Graphics interface
- Map and overlay display
- Real-time track database management services
- Encyclopedic database management services
- Security services.

The COE Working Group has agreed to commonality in the following areas: POSIX compliance (FIPS-151); Ada; Ada-to-C bindings for a relational database management system (DBMS), X-Windows, and UNIX; X-Windows 11.2 migrating to PEX; MOTIF as the graphic user interface (GUI); SQL and its evolutions; and TCP/IP evolving to GOSIP for network services. The Services are now actively seeking a description of common requirements for system architectures and system specifications. They are seeking agreements on recommendations for a common style guide, standard interprocess communications, standard map data, standard graphic user interface, standard

---

[10] The Air Force, Coast Guard, Defense Intelligence Agency, Defense Mapping Agency, Joint Tactical C3 Agency, and the Joint Staff are all represented in COE discussions.

relational DBMS-to-SQL interface, and a standard map display. Table 6b identifies the services for the COE and (in the second column) example standards (the latter are taken from the Navy's implementation). [Ref. COE 1991]

Table 6b. US DoD Common Operating Environment

Services	Example Standards
System Support	
Operating Systems	UNIX--POSIX compliant
Communications Interface & Protocols	GOSIP, TCP/IP, SAFENET, CSS
Windowing (human-machine interface)	X-Windows II (Release 4)
Systems administration	Diagnostics
System management	CMIS, CMIP, SNMP
System security	COMPUSEC Orange Book, SDNS
BUS architecture	VME, FUTUREBUS+
C2 Support	
Display Toolkit	MOTIF
Database manager	SQL, Relational DBMS
Internal interface	BTR
System services	Ada, C, Ada bindings
Display	Chart+
C2 Communications Applications	
External communications	GLOBIXSs, TADIXSs, Physical nets
Message Processing	US Message Text Formats, OTH-G, TADILs A & B, Bit-oriented messages
Correlation	Attributes, ELINT, Probabilistic, Acoustic
Database	Track, C&P/008

Source: *Fleet Communications in the Copernicus Architecture*, Final Draft, 20 June 1991, UNCLASSIFIED.

The top-level architecture model will be the CIM Reference Model (see Section 4.5 above), and a combination of the style guides for the DoD Intelligence Information Systems (DODIIS) will be considered as the DoD human computer interface style guide. The SQL-Ada Module Description Language (SAMeDL) has been recommended for DBMS-SQL interface (and is now being used for US Marine Corps Common Application Support Software inter-module communication).

SPACECOM Assured Mission Support Space Architecture (AMSSA). Space Command (SPACECOM) has developed the AMSSA to consolidate several architectures and expand them to all elements of air-land-sea forces. The goal is to integrate the use of space-based satellites with the communications requirements of the operational forces. The AMSSA seeks to apply "architectural-level" interoperability standards across communications; navigation; environmental monitoring; intelligence; surveillance; mapping, charting, and geodesy (MCG); launch; C2; satellite control; and logistics functional areas in support of the tactical user. The architecture seeks standards in the following six service areas with the associated functions and characteristics:

- Communications: switching, frequency, data rate, wave form
- Navigation: geolocation, timing, velocity
- Launch: mix-and-match flexibility and intercompatibility

- Integrated satellite control services (ISCS): satellite control, mission data processing, protected links
- Integrated logistics support (ILS): supportable, maintainable, operable
- Command and control: unity of command, survivable.

Standards are to be open, modular, and backward compatible without dictating particular engineering solutions. [Ref. SPACECOM 1991]

Defense-Wide Common Security Architecture. One of the tasks in the Defense-Wide Information Systems Security Program (DISSP), which is being conducted by DISA and the National Security Agency, is the development of a Defense-Wide Common Security Architecture. This architecture will include information systems security standards and protocols, uniform security accreditation procedures, security technology, and a transition plan. The architecture's scope includes: guidelines for system design, applicability to many information systems, addressing systems in detail at the service level, identifying relevant technology, describing relevant technologies and important issues, ensuring interoperability, and focusing on cost effectiveness. It is intended to support the increased use of multi-level security in DoD systems. [Ref. DISSP 1991]

C2 Architecture for SDIO Segments. The Strategic Defense Initiative Office (SDIO) has issued a Fixed/Mobile Segment (FMS) Standard to be used in the design of all fixed and mobile ground segments for the Strategic Defense System (SDS). Such segments include the Ballistic Missile Defense Command Center, the Service Component Command Center, the Regional Operations Centers, the Element Operations Centers, and the Ground Entry Points. This document covers open hardware and software architecture and software and user environments. Standards prescribed in the FMS document include [Ref. SDIO 1991]:

- Electrical interfaces: RS-232, RS-422/423, RS-449, IEEE 488.1/.2, MIL-STD-1881-114 or MIL-STD-188, ISO 8802.3 or ANSI X3T9.5 (Fiber Distributed Data Interface), and MIL-STD-1553 (data bus).
- Backplanes: Versa Module Europe bus (VMEbus) (IEEE P1014) or VME Extension for Instrumentation (VXIbus, IEEE P1155). The selection of VMEbus is to provide future growth to FUTURbus (IEEE 896.1). This may require a VMEbus-to-FUTURbus bridge compliant with IEEE P1014.2.
- Protocols: TCP/IP (MIL-STD-1788 and MIL STD-1777) or as available GOSIP (FIPS-146)-compliant protocols.
- Human-computer interface (HCI): X-Window System implementation (FIPS-158) of OSF/MOTIF featuring the direct manipulation of windows, icons, data, menus, and objects within the windows (primarily a "point-and-click" system of direct manipulation that minimizes typing. HCI complies with MIL-STD-1472 except where there are conflicts with OSF/MOTIF, MOTIF Style Guide, and multiprocessor requirements.
- Software: Includes the NIST Application Portability Profile (FIPS-151), GOSIP protocols and services in all software for SDS C2 ground segments,

Ada for all software development (with some C programming permitted), POSIX-compliant operating systems, database-defined constants (parameters), database management system supporting an SQL interface.

- Information processing system security: level of multi-level security protection is TBD. Underlying operating system in the applications processors meets DoD 5200.28-STD for controlled access protection (class C2).

5. DATA MANAGEMENT SERVICE STANDARDS

5.1 Requirements

Quick Reference	
Topic	Page
Assessment	97
Data Element Stds	91
Data Modelling Facility	81
IRDS	75
NDL	69
ODP	88
PPRDB	66
Ref Model Data Mgmt	68
Schema	66
SQL	70
TP	85

Data management standards support the storage, control, distribution, management, and allocation of simple data (text and numeric information) as well as complex data (complete documents, maps, charts, images, and multimedia objects). Data exchange standards (Chapter 4) permit the exchange of both simple and complex data among applications and between systems in a way that preserves the meanings and relationships in that data. An overview of the status of data management service standards is given in Table 7.

One or more standard query languages can be used as the basis of the peer-to-peer protocol for the exchange of data between CCISs. More than one data model (e.g., relational, hierarchical, image/map oriented) may be required. The information transfer services are primarily constrained by finite communications bandwidth and security.

Security is discussed in Section 9.2. Exchange mechanisms provided by the communications standards for network services are discussed in Chapter 6.

The data management services will provide mechanisms to accurately represent the meanings and relationships of the information items to be managed. These mechanisms include the database system, the conceptual schema, and CCIS domains. For each data model to be supported, these mechanisms will provide a standard way of representing the data, including support for common data definitions. (The definitions as well as the data would be standardized during the implementation phase of a specific CCIS.) An example of one type of support that could be provided is a data dictionary system, which could be used by CCISs to maintain common data definitions and representations.

Table 7. Status Overview of Key Data Management Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
IRDS	○		○	●	○		
SQL	●	○	●	●	●	●	●
RDA			○		○		

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

Another example is the data definition language (DDL) that may be provided with a database system or language. The data definition language (DDL) must be rich enough in its forms of expression to have attributes required of both commercial and military systems. For example, it needs to have the capability to recognize several types of hierarchy for data classification and compartmentalization and be trusted to permit access by users with varying levels of authorization for these classification levels and compartments.

5.1.1 Partitioned, Partially Replicated Database System

Data transfer services in future CCISs are expected to be provided by a partitioned, partially replicated database system. Partitioning means that the entire CCIS database is segmented into disjoint parts that are held at geographically separate locations. Some of the parts of the CCIS database are copied or replicated at other locations to ensure survivability or to provide more rapid local access. A partitioned, partially replicated database provides sufficient flexibility for efficient exchange of information in a manner that minimizes usage of communication by permitting either "push" access (for updates) or "pull" access (for queries).

5.1.2 Conceptual Schema

A common conceptual schema is needed to define all CCIS data related to information exchange.[11] The CCIS database will be segmented or partitioned into replication domains, each owned and managed by a specified subfunctional area. Each replication domain has one master copy and may have other copies referred to as slave copies. A single component would be able to access some, but not all of the master and replication domains.

5.1.3 Domains

Each domain comprises two parts. One part (domain details) provides the characteristics and control information for the domain. Examples of possible domain details are: name, owner, home CCIS component for the master domain, list of permitted users, component addresses for the replication domains, and security classification parameters. The other part of a domain (domain data) provides the values of each data item. The representations of some features of a domain, such as data item characteristics, data relationships, and data dictionaries, are implementation dependent and have therefore not been specified.

---

[11] The schema may not identify information managed uniquely by a headquarters or a national system.

5.1.4 Required Services

The following basic services appear to be required:

- Data definition--provides a common understanding between systems on the attributes and meaning of data.
- Local queries--queries that can be satisfied by a data item or a set of items as specified in parameters supplied in the query, subject to authentication of the requestor's identity before issuing the data, such that the data resides in either a master or slave copy at the location where the query is made.
- Remote queries--transfers, from a remote master or slave copy, a data item or a set of items as specified in parameters supplied in the query, subject to authentication of the requestor's identity before issuing the data, from a location other than the one where the query originated.
- Consistency control--ensures that any updates to values of data items in a slave copy ultimately become the same as the values in the master copies of the relevant domain; consistency control also ensures that update transactions are applied in the correct order.
- Local updating--provides for changing the values of a data item or set of data items for a domain, where the master copy is held at the same location as the one where the update originated.
- Local slave updating--provides for changing the values of a data item or set of data items for a slave domain, but without replication of the updates.
- Remote updating--provides for changing the values of a data item or set of data items for a domain, where the master copy is at a remote location; these operations are subsequently directed to all slave copies of the relevant domain.
- Integrity of replicas--ensures that each replica, together with deferred updates, can be used to replace the master domain in the event of a system failure.
- Management of distribution--supports the partitioning and partial replication of the databases.
- Recovery from failure--provides mechanisms to decide that there has been a failure, allows recovery from failure, and permit a slave copy to become a master copy.
- Change of command--supports change of location of command (COLOC) and succession of command (SUCOC) by permitting a slave to become the master and by permitting new slave copies to be designated dynamically.
- Database statistics--provides status and usage data for the system manager.
- Database initialization--provides for the creation and loading of initial values of a database and its replicas when the system is initialized.
- Standard knowledge base--document knowledge information.

In addition, the following management services appear to be required:

- Create domain--creates a new, empty domain, either as a master copy or for use as a replication copy of a domain.

- Delete domain--deletes a domain and erases all data in that domain. (When applied to a master copy it will delete all associated replication copies.)
- Transfer domain--causes, when proceeding to normal completion, the master of the domain to become a slave copy and the slave copy at a designated replication component to become the master.
- Assume domain--provides for change of ownership of a domain.
- Unassume domain--provides the capability to resolve the situation in which more than one CCIS component has exercised assumption of the same domain by designating another domain as the master.
- Amend domain--provides for changing the characteristics of a domain, such as the list of users or the replication list, by the owner or other authorized user.
- Details domain--provides for query of the details or characteristics of a domain by an authorized user.
- Copy domain--copies the entire contents of a domain, both characteristics and data, to a replication copy. (Space for the copy is first created by "create domain.")
- Restore domain--allows the owner of a domain to recreate the data in the master copy of the domain by copying it from a replication copy, in support of data recovery after failure.
- Advise domain--allows a CCIS component to be interrogated to see if it holds a copy of a domain. (This permits components who have lost and then reestablished communications to find out whether the replication list is correct.)

Some options for standardizing the appropriate features of domains are inherent in the discussions in the sections that follow. Some services being evaluated to provide database operations (not yet adopted) imply implementation of a relational database architecture. Examples of database operations are: select, update, delete, insert, project, product, union, intersect, difference, divide, join, and equijoin.

5.2 Standards for Database Services

This section primarily addresses the technical aspects of data management. The procedural aspects of data management are addressed in Section 5.3. The Reference Model for Data Management described below applies to both the technical and procedural aspects.

5.2.1 ISO Reference Model for Data Management

The *Reference Model for Data Management* is DIS 10032. Development began in 1988 and the DIS text was distributed in May 1991 (balloting ends in January 1992). Issues to be resolved for this reference model include distributed operation and export-import concepts and requirements. Coordination with ODP is required.

DIS 10032 includes in the scope of data management the description, creation, modification, use, and control of data in information systems. The model provides a framework for identifying interfaces; positioning interfaces relative to each other;

identifying facilities provided at each interface; identifying the process that supports each interface and, where appropriate, the specific data required for this support; positioning the use of the interfaces in terms of the information system's life cycle; and identifying the binding alternatives associated with each interface. The concepts defined in the model may be used to define the services provided by particular database management systems or data dictionary systems. The data management field of application concerns any user--human or applications program--who wants to request services for management and storage of information in a persistent manner.

SC21/WG3 is preparing a technical report, *Tutorial for Reference Model of Data Management,* that will address the following topics [Ref. IST 21 1534 1988]:

- Tutorial aspects for the Reference Model of Data Management
- Analysis of current database standards in terms of the Reference Model concepts
- Analysis of data management services using data flow diagrams
- Description of current database standards with respect to the requirements of the Reference Model.

PDTR text is expected in June 1993.

5.2.2 Data Definition and Manipulation Language Standards

There are now two data manipulation language standards approved by ISO, ANSI, and FIPS: NDL[12] and SQL.[13]

5.2.2.1 Database Language NDL

Database Language NDL (ISO 8907, ANSI X3.133-1986, FIPS 126) is an outgrowth of 1978 CODASYL specifications using a network model for a DDL and a data manipulation language (DML). NDL is characterized, in part, by extensive use of logical pointers. These pointers support such facilities as FIND NEXT (push down in a stack) and FIND OWNER (pop up in a stack). The specification work was conducted from 1981 to 1986 by the ANSI X3H2 Database Committee. No follow-on standards activities are being conducted by ISO or ANSI for NDL [Refs. Deutch 1987; Gallagher 1988]. Implementations supporting NDL are rare. The existing ANSI and ISO NDL standards will likely be withdrawn in 1992, or soon thereafter, unless some user or vendor establishes a requirement for its continued existence. [Ref. Gallagher 1991a]

---

12 NDL is not an acronym; historically, the term derived from the concept of a network data language.

13 SQL is also not an acronym; historically, the term derived from the concept of a structured query language, but today represents much more.

5.2.2.2 Database Language SQL

SQL (ISO 9075.2, ANSI X3.135-1986, FIPS 127) is based on a relational database model; the specification work was conducted from 1982 to 1986 by the ANSI X3H2 Database Committee. Future work in the standards for database management systems by ISO and ANSI X3H2 will be on distributed database processing (e.g., remote data access protocol) and extensions to SQL.

Both ISO and ANSI are working closely together and in parallel on SQL2 (DIS 9075.2), a follow-on standard. SQL2 was sent out for public review as X3.194-199x from November 2, 1990 through March 1, 1991. It is now being reviewed as X3.135-199x. An ISO editing meeting is scheduled for January 1992 to consider DIS ballot comments. This draft standard is an upward compatible enhancement of two existing SQL standards: *SQL with Integrity Enhancement* (ANSI X3.135-1989; ISO 9075:1989) and *Database Language - Embedded SQL for* COBOL, *FORTRAN, PL/1,* Ada, *and C* (ANSI X3.168-1989). The Integrity Enhancement Feature provides for check clauses, default clauses, and referential integrity constraints.

Since SQL2 has been stable for some time, it is anticipated that it will become an international and U.S. standard by 1992. In February 1990, FIPS 127 was revised (FIPS 127-1) to incorporate integrity enhancement and embedded SQL. FIPS 127-1 also documents guidelines and considerations for procuring SQL systems.

Work has already begun on SQL3 (WD 9075.4), which is planned to become a standard about 1995 or 1996. CD text is expected June 1993. SQL3 would incorporate the following features:

- Generalized triggers (similar to IF...THEN statements; based on a condition of data, not time)
- Generalized assertions (given a certain condition, to trigger integrity checks on the database; e.g., to do before and after validation on values in the database)
- Recursive expressions (these allow an open-ended subordinate assertion, such as, to completely search a tree--currently, only finite queries to specified levels are permitted)
- Escape from SQL to call external features
- Basic capability for user-defined data types (the only structure in SQL is a table; this allows the user to declare a domain separate from a table)
- Support for subtables, provided through inheritance and generalization features
- Appropriate support tools for object-oriented and knowledge-based systems.

A major new facility on user-defined abstract data types, with support for object identifiers and other object-oriented features was adopted at the DBL rapporteur group. In addition, the module facility was enhanced to make it a schema object completely maintained by the DBMS and a CALL statement was added to the SQL language to call procedures in the modules. Additional efforts were made to expand the notion of

updatability for table expressions using the definition of functional dependency. Working papers were discussed on how to enhance SQL to better address problems in GISs and in Full-Text manipulation [Ref. Gallagher 1991].

The ANSI standard X3.135-1986 SQL allows for two levels of compliance. Level 1 is a core standard that leaves many areas open to implementation definition. Level 2 contains many extensions over Level 1, but Level 2 still has a large number of options for implementation. Examples of facilities found in Level 2 but not in Level 1 are [Ref. Martin 1989]:

- Atomic transactions with respect to recovery
- Eighteen-character identifiers
- Table-name qualification by user-name
- Indicator variables
- Outer references
- Keyword ALL allowed in query-specifications, sub-queries, and set functions
- Updatable query-specification definitions
- Statements atomic with respect to database changes
- Not equal to comparisons (<>)
- Escape characters in the LIKE predicate
- REAL, DOUBLE PRECISION, and NUMERIC data types
- WITH CHECK OPTION on a view definition
- WITH GRANT OPTION on a privilege definition
- DISTINCT with AVG, MAX, MIN, and SUM.

NIST has established a test suite and formal testing service (April 1990) which provide a basic SQL conformance validation.

CD text for a new work item, *Data Management Export/Import for SQL* and *IRDS* [SC21 N 5137] is expected December 1992.

A CALS (see Section 9.1.4) Phase III requirement.calls for "intelligent" DBMSs. SQL3 intends to provide facilities for managing object-oriented data and for forming the basis of "intelligent" DBMSs. Of particular importance are many of the proposed SQL3 features to the STEP (see Section 9.2.1) because of that standard's unique data modeling and data access requirements. Existing and planned features in SQL3 may not satisfy all STEP requirements, but they should provide an appropriate base from which many requirements can be suitably addressed. [Ref. Gallagher 1990]

5.2.3 Remote Data Access (RDA)

RDA[14] is an ISO standard to facilitate access to databases from intelligent workstations and from other database systems. It is essentially a (standard) generalization of certain operations of database systems, file servers, and document servers. RDA will allow, with a minimum of technical agreement outside the interconnection standards, the interconnection of applications and database systems from different manufacturers, under different managements, of different levels of complexity, and exploiting different technologies. Since an application may itself be a database system, RDA can be used to support multi-database system interworking.

RDA service is designed to provide all possible valid data manipulation functions on any database. The functions needed (and available) depend on the structure and content of the database, so the definition of these functions must be accomplished at run time (not explicitly coded into software). Thus, RDA allows data management language operations to be defined and named (actually numbered) so they can be repeatedly invoked later in an application and association.

The ISO standard for RDA (DIS 9579) defines the format and meaning of messages that support this application. RDA uses common OSI services for the association control service element (ACSE)--ISO 8649 and ISO 8650, commitment concurrency and recovery (CCR) service elements--ISO 9804 and ISO 9805, and ROSE (ISO 9072) to provide the communications services. RDA can be viewed as a composition of ACSE and CCR with a specialization of the ROSE.[15] RDA needs no specific protocol of its own; it only requires additional sequencing rules and a method for handling violations of them. The Abstract Syntax Notation standards (ISO 8824 and 8825) are used in the Presentation Layer to define structures (data types) and rules for encoding structures so that the structures can be transmitted.

The ISO standard DIS 9579 is based on work of the ECMA Technical Committee on Databases, CCITT, and ISO SC18. ECMA TR30 (December 1985) was the starting point for RDA, and ECMA TR31 initially defined the concepts, notation, and connection-oriented mappings for remote operations. DIS 9579 has two parts:

- DIS 9579-1, *Generic Model, Service, and Protocol* [SC21 N 6375, 30 August 1991]
- DIS 9579-2, *SQL Specialization* [SC21 N 6376, 30 August 1991].

The remote operations philosophy is based on object modelling in which the functionality of an object is modelled as a set of operations available at its interface. Object modelling also includes the notion of object classes, subclasses, and property inheritance.

---

[14] Discussion taken from *Remote Database Access*, Tutorial, SC21 N 1927, ISO/TC97/SC21, 28 July 1987, UNCLASSIFIED; and DP 9579-1, 29 March 1990 [SC21 N 4282].

[15] Application Service Elements ACSE, CCR, RTSE, and ROSE are discussed in Section 4.3.6.

In RDA these concepts are used to define a generic RDA, which defines a class of remote database access applications, and specific RDAs, each of which defines a subclass of RDA applications. Those properties common to all RDA applications are defined in the generic RDA. Those that relate to subclasses are defined in RDA specializations.

The generic RDA can support any data management language. One of the specific RDAs is a specification for the Database Language SQL [Ref. SC21 N 2643 1988]. Other specific RDAs to be developed in the near future are also expected to be based on the relational approach. The relationship data management language was chosen because it supports complex selection functions and multi-record operations for updating and deletion. This enables the RDA to accomplish selection processing in the database server (the place where the data is stored). This reduces the amount of unneeded data that is transferred to the client (user) and thus minimizes use of communications [Ref. SC21 N 1927 1987].

The SQL specialization (DIS 9579-2) defines the service and protocol for access to databases and supports the data manipulation functions of SQL. This is done through specifying the transfer syntax for specific data manipulation functions, as provided for in ISO 9075 for SQL database systems. The elements of the SQL (or any other) specialization are definitions for [Ref. SC21 N 3342 1989]:

- Data resources available as a result of establishing a dialogue and any constraints on opening and closing further data resources
- Data structure of a class of data objects supported
- Permissible classes of operations upon the objects
- Representation of all operations in an abstract syntax
- Representation for data passed as parameters for these operations.

The SQL specialization for RDA (DIS 9579-2) augments the generic RDA (DIS 9579-1) so that the two parts together define the following:

- Capabilities of an SQL database server that supports dialogues with clients
- Model of dialogues between the SQL database server and remote users
- Model of a dialogue between an RDA client and an SQL server
- Abstract service interface for the RDA SQL ASE that models the communications facilities supporting interaction between the SQL client and the SQL server
- RDA SQL ASE protocol to support the RDA SQL service
- Characteristics of application contexts that include the RDA SQL ASE
- Application contexts that support remote database access using SQL, specifically the RDA Basic Application Context and the RDA TP Application Context.

The generic RDA (DIS 9579-1) and SQL specialization (DIS 9579-2) were progressed to DIS status in July 1991. A SQL2 specialization (DIS 9579-2 WDAM 1) is expected in June 1992 [Ref. Gallagher 1991]. PDAM text is expected in June 1993.

While there are no known RDA implementations, many SQL vendors are planning to have conforming client and server products available before RDA becomes a standard (before 1992). Vendor consortia, such as SQL-Access and X/Open, hope to have working prototypes operational in 1991 to demonstrate interoperability among different SQL users [Ref. APP 1991].

SC21/WG3 is considering standardizing some or all of the following properties of distributed database systems [Ref. SC21 N 5146 1990]--the new work would be done in conjunction with RDA:

- Single database image presented to the user
- Location transparency (includes automatic routing and transaction decomposition)
- Distributed transaction management
- Query optimization (to minimize communications flows)
- Data replication (optional)
- Local autonomy for database administration (i.e., no requirement for a single DBMS)
- Decentralized schema management
- Distributed deadlock detection/avoidance
- Extensibility (heterogeneous database)
- Concurrency management.

In October 1990, a new work item proposed creating an addendum to DIS 9579 entitled, *RDA Support for Stored DBL Statements* [ISO/IEC JTC1/SC21 N 5138]. In June 1991, WG3 recommended approval for this new work item. However, others recommended that a separate new project not be created, since the work could be accomplished as SQL enhancements instead [Ref. Gallagher 1991]. Services defined in DIS 9579-1 and DIS 9579-2 support the ability to define and repeatedly execute individual DBL statements at the Server. However, the defined DBL statement is considered part of the RDA Dialogue state, meaning that a defined DBL statement can only be used by the Client that created it and that any remaining defined DBL statements associated with an RDA Dialogue are removed before or when the RDA Dialogue is ended. An expanded "stored DBL statement" concept would:

- Allow a collection of SQL statements to be stored (and treated) at the Server as a single named object
- Permit the life of a stored collection of DBL statements to be longer than the life of an RDA Dialogue

- Allow any Client to use a stored collection of DBL statements [Ref. RDA 1990].

Work is continuing on this item with no target date available. SC21 has recommended that this new work item not be assigned a new project number but instead be considered to have two parts: (1) an SQL language part that is assigned to the already existing SQL3 project and (2) a supporting RDA service and protocol part that is assigned to the existing parent RDA project. [Ref. JTC1 N 1485 1991]

A CDTR, *Remote Database Access Tutorial,* [SC21 N 3343, January 1989] is planned for June 1992.

A June 1991 report, IST21 N 2880, *Interim Report on the Feasibility of Profiling Database Enquiry,* extends the scope of an earlier project on RDA to database enquiry (DBE) for all user-oriented database operations, which support and control the creation, modification, and retrieval of data in a database and the maintenance of the logical structure of the database. The report concludes that work should begin now on defining profiles for DBEs that would cover user access facilities and procedures, information presentation, communication, transaction management, and database management. The work would require additional base standards (e.g., RDA SQL2 specialization, user interface standards, and distributed database management standards) and extensions to the taxonomy of TR 10000-2.

5.2.4 Information Resource Dictionary System (IRDS) Standards[16]

Stable IRDS Standards. An IRDS is a system that provides facilities for creating, maintaining, and accessing an Information Resource Dictionary (IRD) and its IRD definition. There are two stable international standards for IRDS:

- ISO 10027:1990, IRDS *Framework,* June 1990
- DIS 10728, IRDS *Services Interface,* July 1991.

The IRDS *Framework* provides a common basis for developing information resource dictionaries (IRDs), which are sharable repositories for the definition of the information resources relevant to all or part of an enterprise. The IRDS *Services Interface* specifies a services interface that gives any program full access to all IRDS services, through whatever external call interface is provided by the language in which the program is written.

Information resources. Information resources governed by an IRD may include:

- Data needed by the enterprise

---

16 Portions of the discussion of IRDS are taken from ISO 10027, *IRDS Framework.*

- Computerized and possibly noncomputerized processes that are available for presenting and maintaining such data
- Available physical hardware environment on which such data can be represented
- Organization of human and physical resources that can make use of the information
- Human resources responsible for generating that information.

The IRDS standard does not provide a standard definition of all the above kinds of information. Rather, it provides a framework for defining such information in which the information can be represented and managed. The content of an IRD can be compared with the content of a typical application database--an application database contains data of relevance to the day-to-day operation of an enterprise. The difference is that the data is at a higher level (metadata or data about data) and may include such entities as data item types, data files, computer programs, and subsystems.

An IRDS is used to control and document an enterprise's information resources. ISO 10027, IRDS *Framework*, defines a number of concepts that are basic to data management. A *database* is a collection of interrelated data stored together with controlled redundancy according to a schema to serve one or more applications. *Database integrity* is the consistency of a collection of data in a database. *Export* is the function of extracting information from an IRDS and packaging it to an export/import file. *Import* is the function of receiving data from an export/import file into an IRDS. An *IRD* is a part of a repository managed by an IRDS in which the information resources of an enterprise may be recorded. A *value* is an abstraction with a single characteristic that can be compared with other values and that may be represented by an encoding of the value. A *data modelling facility* is a set of data structuring rules and an associated set of data manipulation rules. An *application schema* is a set of definitions that control what may exist at any time in an application.

IRDS framework, facilities, and interfaces. The IRDS Framework identifies the kinds of data, together with the major processors and their associated interfaces and the broad nature of the services provided at each interface. Aspects addressed by various IRDS standards include programming language dependence, interface style, data modelling facility used, and data interchange format. Examples of processor interface styles are programmatic (such as a procedure call interface, consisting of a sequenced set of parameters and associated binding rules for the CALL statement in a programming language); syntax for execution time interpretation; and service convention (a standard set of programming language independent conventions for specifying parameter lists and service primitives for use in an open systems environment). Examples of alternative styles for human interfaces are panels (abstract screen formats), concrete syntax (such as a command language), and graphics.

An abstract syntax is the specification of a service (such as for an interface style) by using notation rules that are independent of the encoding techniques used to represent them. An abstract syntax may be used to define a set of services without prescribing any linguistic form to be used when each service is initiated or invoked.

Examples of data modelling facilities are those based on standard database languages such as NDL or SQL, based on a non-standard database language, specific to a standard programming language (such as COBOLor PL/1), specific to a non-language standard (such as OSI Directory services), or which are non-standard data modelling facilities (such as entity-relationship modelling). Each data modelling facility is an intrinsically independent means of representing data and possibly the services that may be specified for such data.

Three types of support can be provided for a database using international standards. One is using standardized services at an interface, in which the contents of some part of the IRD are defined, together with the services by which those contents may be accessed and manipulated. The second type of support is by standardizing in precise terms the content of some part of an IRD according to some prescribed data modelling facility. The services that may be performed on that data may or may not be implicit in the general data manipulation services associated with that data modelling facility. The third type of support is the use of a standard data interchange format, designed to facilitate the interoperability of several real systems by standardizing the formats of the various kinds of messages sent from one real system to another. A data interchange format may be specific to an application.

IRDS provides for two types of user interfaces: a menu-driven (panel) interface and a command language interface. The panel interface provides for a structured path of screens (i.e., panels) by which an inexperienced user can execute IRDS functions. The command language may be used in either an interactive or batch mode. The work on a draft standard, *Command Language and Panel Interface* (DP 8800-1, March 1987), was suspended until August 1991, when the IRDS *Service Interface* (DIS 10728). The draft standard for the command language and panel interface is expected to be split into separate standards (possibly 8800-1 and 8800-2).

IRDS, including the command language and panel interfaces, is specified in terms of entities, relationships, and attributes. The entities represent or describe the concepts and data objects about which values are to be stored in the database. Relationships are binary associations between two entities (e.g., one contains the other). Attributes represent the properties of an entity or relationship. Each relationship and attribute is assigned a specific type. Entities can be compared if they have a common attribute with a common type. Ordered sets of attributes, called attribute groups, are also provided in IRDS. The IRDS schema that defines and controls what is permitted in a data dictionary is also defined using entities, relationships, attributes, and attribute groups. IRDS supports local and universal

naming conventions through three types of entity names: access names (used with the command language), descriptive names (e.g., from a NATO-wide data dictionary), and alternate names (e.g., aliases used for the convenience of one or more nations or one or more CCIS components). IRDS functions include adding, deleting, modifying, and copying entities and relationships, in addition to report writing.

IRDS Standardization in ISO and ANSI. The IRDS is a data dictionary standard being developed in parallel by both ISO (JTC1 SC21/WG3) and ANSI (ANSI X3H4). The standard is based on the entity-relationship model and would be applicable to Database Language NDL and Database Language SQL.

ISO and ANSI differ in their approach to IRDS standardization as well as in the technical details. The communities have diverged over the issue of whether relationships are permitted to have attributes (ANSI) or not (ISO). The rationale for the simpler model (no attributes) is that it would fit more easily with SQL tables. The rationale for the ANSI position is that a model permitting attributes, while more complex and more cumbersome, would provide greater flexibility. Further, a lot of existing products would be invalidated if no attributes were permitted for the relationships.

ANSI is developing two IRDS standards: (1) an IRDS with a human interface called a *Command Language and Panel Interface* (ANSI X3.138) and (2) a software interface to the IRDS called the IRDS *Software Interface* (ANSI X3.185).

ANSI X3.138 was adopted by the Federal Government as FIPS-156, effective October 1989. An 18-month transition period to allow industry to produce and provide IRDS products during which users could use non-conforming products ended in March 1991 [Ref. APP 1991]. While commercial products have been developed, their quality has not yet been determined because a Conformance Test Suite is not yet available. NIST projects that the Test Suite will be available for beta testing in late 1991 or early 1992 [Ref. Goldfine 1991]. An upgrade to FIPS-156 is not expected until 1995. Most likely the revision will be influenced strongly by object-oriented data models as well as emerging repository and Computer-Assisted Software Engineering (CASE) technologies [Ref. Price 1991].

ISO began a *Command Language and Panel Interface Standard* (DP 8800), but suspended the effort in 1987 when the ISO and ANSI efforts diverged. The IRDS *Service Interface* (DIS 10728) is comparable to ANSI IRDS *Software Interface* (X3.185) in that it allows software (as opposed to humans) to access the IRDS, however, the technical details differ.

DIS 10728, in combination with the *Framework* standard (ISO 10027) forms the basis for the first generation ISO IRDS standard (sometimes called IRDS1). Even though it has not reached IS status, work has already begun on the second generation IRDS (IRDS2). A NWI for IRDS *Extensions* (IRDS2) was introduced in October 1990 [SC21

N 5139]. Although the NP received the required number of approval votes to qualify for acceptance, several National Bodies submitted negative votes on the basis that a strong statement of requirements was lacking. Therefore, JTC1 did not make a formal project assignment [JTC1 N 1254]. SC21/WG3 responded with a revised scope of work and the project was added to the JTC1 programme of work in August 1991 [JTC1 N 1486] under the title *Extensions to the* IRDS *Services Interface*. WG3 recommended that it retain the same number as the IRDS *Framework* (ISO 10027) since the new standard is intended to be an upward compatible revision of the current IS.

The purpose of the revision is to:

- Align the IRDS *Framework* with the *Reference Model of Data Management,* (ISO 10032) which did not achieve CD status until after ISO 10027 was approved.
- Align the IRDS *Framework* with the ongoing work in the IRDS *Services Interface* (DIS 10728), SQL, RDA, and other related standards activities.
- Ensure that the IRDS *Framework* provides a sound basis for positioning standards needed to satisfy the user requirements as identified in the *ANSI* IRDS *Reference Model Draft Technical Report* (ISO JTC1 SC21 WG3 N 1208).

It will provide enhanced facilities in the following areas:

- IRDS class hierarchies, inheritance of data type and behavior, method registration and specification and method invocation
- IRDS data types, including abstract data types and aggregations
- IRDS triggers
- IRDS services and data structures to support Configuration Management tools
- Further operations on working sets and their contents, including the combination of the contents of two or more working sets and possibly the division of the contents of a single working set into two or more working sets
- Extensions to cross-referencing
- Extensions to versioning
- Access to large numbers of IRD objects, possibly by means of access to multiple rows in one service invocation
- Work on level independent objects and services
- Improved handling of IRDS Content Modules, their inter-relationships and interdependencies
- Archiving
- Handling of extended character sets
- Access control.

While this revision brings together two major database standardization activities, it further complicates the alignment of the ANSI and ISO standards. Efforts on the part of

ANSI X3H4 (IRDS) to seek reconciliation with ISO have not been successful [Ref. IST/21: 2499 1991]. WD status is expected in July 1992, CD in July 1993; DIS in July 1994; and IS in July 1995. [Ref. SC21 N 6252 1991]

Other ISO projects related to IRDS include:

- *IRDS Design Support for SQL Applications*, CD text is expected in June 1992
- *IRDS Export/Import.*, CD text is expected in July 1993
- *Support for SQL1 with Integrity Enhancement* , is scheduled for completion in 1993.

SC21/WG3 has also noted that there is a growing industry requirement for investigation of a unification meta model for the representation and manipulation of the data semantics managed by an information repository. In November 1991, WG3 posed a question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM). The new question was approved and work will begin in June 1992. This requirement shares objectives with the conceptual schema and common data modelling facility issues (see Section 5.2.5). Target dates for the proposed question are NWI: July 1992, WD: July 1993; CD: July 1994, DIS: July 1995, and IS: July 1996. [Ref. SC21 N 6251 1991]

WG3 has also noted a growing industry need for interoperability. In the IRDS context, CASE tools on workstations need to access dictionaries on servers. Therefore, WG3 recommended that SC21 ask JTC1 to initiate a ballot for the Registration of a Question on the Approach to Remote IRDS Access [Ref. SC21 N 6253 1991]. JTC1 authorized work to begin in June 1992.

Several ANSI IRDS efforts are nearing U.S. public review status while one has been completed and another new work area has been initiated [Ref. Winkler 1991]:

- *IRDS Export/Import File Format.* The ANSI draft proposal for IRDS Export-Import File Format, which supports the export-import requirements identified in the X3.138, was completed in 1990 and expected to be an ANSI standard in 1991.
- *Technical Report on the* IRDS *Reference Model.* This report will explain the relationship of the IRDS within the information environment of an enterprise. It is currently out for public review and was expected to be released in 1991.
- *IRDS Naming Convention Verification.* ANSI X3H4.4 was scheduled to have completed this in 1991.
- *Technical Report on Requirements for an* IRDS *in a Distributed Heterogeneous Environment.* This document, under development by X3H4.5, is progressing more slowly.
- *Technical Report on Integration of* IRDS *Schema.* This report is currently inactive. Instead, X3H4.6 is working on a *Technical Report on Model Unification for Data Repositories,* which will address the same problem but at a different level. The technical report will address the needs of IRDS users to

translate, integrate, reference, and/or use differing models or representations of enterprise information and behavior at various levels of complexity and abstraction. It will establish a framework for the analysis of models; analyze models; define the IRDS neutral unification model and its representation; reconstruct models using the unification model; develop an IRDS meta-schema; develop IRDS requirements; develop IRDS conceptual model architecture guidelines; and develop a test case. The target date is January 1993.

- *Standard on Export/Import Extensions.* ANSI X3H4 cannot progress this standard until the *Technical Report on Integration of* IRDS *Schema* is complete.

Accredited Standards Committee ANSI X3, Information Processing Systems, recently announced a development project for IRDS *Extensions to Support CASE Environment for Information Interchange*. This standard would define an IRDS, based on ANS X3.138-1988, capable of supporting the full range of IRDS applications. In particular, it would be capable of acting as the IRD in a traditional data processing environment and capable of providing the stable store necessary to support an integrated CASE environment. The standard would include both the semantics of the IRDS and a software interface suitable to the needs of active CASE and Dictionary tools. The development has been assigned to Technical Committee ANSI X3H4.2 [Ref. CSI 1990].

5.2.5 Conceptual Data Modelling Facility Standards

5.2.5.1 Conceptual Schema

SC21/WG3 has identified five different uses of the term "conceptual schema." The following identifies the five uses and provides WG3 comments on those uses [Ref. SC21 N 4195 1990]:

- The results of an analysis of the data and possibly the processes perceivable in some real-world situation.
  - There is considerable disparity among the data analysis techniques used in various parts of the world. Some are being energetically promoted by minority groups.
  - There are rapid developments in CASE.
  - Attempts to standardize on any one technique may be premature. Such efforts should await availability of the Reference Model on Information Systems Engineering being developed by SC7/WG4.
  - Work on a conceptual data modelling facility should be considered as content of an IRDS and be conducted in accordance with the IRDS Framework (ISO 10027).
- A repository of "metadata" in which it is possible to specify declaratively 100% of the semantics of the data in a computerized information system (the 100% principle of TR 9007). The "100% principle" now adopted by ISO [Refs. SC21 N 197 1982; SC21 N 236 1985] says:

> All relevant static and dynamic rules, law, etc., about the universe of discourse should be described in the conceptual

schema. The information system cannot be held responsible for enforcing those rules described elsewhere, particularly those described in user procedures.

- The 100% principle has had major influence on SC21/WG3 work in the development of SQL. The SQL draft proposal being progressed contains language specifications that make it possible to specify declaratively a very large percentage of the constraints on the data that a database designer is ever likely to want to define.
- While SQL is never promoted as a means of defining a conceptual schema, it is, in this very important respect, superior to many of the approaches developed especially for the purpose.

- A data definition that has the property of being independent of its representation in storage.
  - Some standards committees have adopted the term to refer to some kind of representation of the data definition that is above the level of stored representations.
  - SQL is a language that enables the preparation of a storage independent definition of data.
- A data definition that is common to the collections of data at two separate sites, such that it can be used as a common frame of reference when exporting data from one site and importing it at another site.
  - In EDI, one needs a definition of data to be interchanged that is common to all sites involved in a set of interchanges.
  - Much of the EDI work has been concerned with the specification of standard formats for an industry area, such as banking or travel. As EDI tends to adopt a more generalized approach to standardization, the need for a common definition facility becomes apparent.
- A data modelling facility (see DIS 10032, the *Reference Model on Data Management)* that is different from and therefore "neutral" with respect to broadly similar data modelling facilities used in commercially available database management systems.
  - Data modelling facilities are also called data models; merits of various approaches are controversial topics.
  - Another "neutral" approach would lead to confusion, is not required, and is not recommended by WG3.

5.2.5.2 Conceptual Schema Standardization

Work in the area of conceptual schema in ISO dates back to the early 1980s. In 1982, TC97/SC5 first published what is now TR 9007, *Concepts and Terminology for the Conceptual Schema and the Information Base*. This report was followed in 1985 by the *Assessment Guidelines for Conceptual Schema Language Proposals.*

SC21 held a workshop on conceptual schema and its relationship to the Conceptual Data Modeling Facility in the Netherlands in November 1990. A subsequent workshop was held in Anaheim, California, in January 1991 where papers on some 18 different modelling methods were presented. Two of the approaches presented included the ANSI IRDS approach and the ANSI X3.T2 Registering of Conceptual Schemas approach [Ref. Perez 1991].

ANSI has proposed that a new question be established in SC21 to determine the use, scope, and purpose of one or more standards for conceptual schema. The goal would be to address the need for models of a "universe of discourse (UOD)." Such models are needed to clarify in a formal way the notion of a particular universe of discourse to which a standard applies (e.g., for Directory schema) and to facilitate the specification of a common universe of discourse for information exchange (e.g., for *Application Layer Structure*, ISO 9545) [Ref. SC21 N 4511 1990]. Actions of such an international standards activity might include: (1) developing and maintaining a list of approved answers and comments on issues related the the topic of conceptual schemas; (2) registration; and (3) developing and maintaining one or more standards for specifying inter-application information requirements, semantics, concepts, and terminology for open applications. [Ref. SC21 N 5851 1991]

5.2.5.3 Conceptual Data Modelling Facility Standardization

Japan has proposed a new work item in SC21/WG3 for a conceptual data modelling facility [SC21 N 4280, February 1990]. The proposed standard would specify the facility to describe an application data model and the representation method of the result of the description of an application data model. A Special Meeting on Conceptual Schema and Common Data Modelling Facilities will meet in Renesse, Holland, 9-13 March 1992. It will address the following issues [Ref. SC21 N 6449 1991]:

- Requirements of various international standards groups using the concepts and terminology of conceptual schemas
- Interfaces and mechanisms employed to model, specify, use and relate conceptual schemas in these activities
- Identification of the standardization groups now using, or planning to use, conceptual schema techniques or common data modelling facilities
- Relation of the requirements and uses identified above. (Are the efforts and uses consistent? Need they be consistent?)
- Identification of activities for the standardization of conceptual schema techniques or common data modelling facilities and interfaces to them being undertaken by National Bodies or by other standards organizations. (Would international coordination or harmonization of diverse National Body standardization activity be desirable?)
- Planning and organization of future work on conceptual schemas. (How should conceptual schema usage and concepts in the various JTC1 groups and other ISO standardization activity be related?)
- Consideration of whether and how a conceptual schema can be stored and interchanged using standard database languages
- Addressing the short-term considerations of coordination amongst the various standardization groups within JTC1

- Relationship of proposals made to existing standardization activities in the area of reference models and frameworks.

5.2.5.4 Object-Oriented Database Support

In 1989, the ANSI X3 Standards and Planning Requirements Committee (SPARC) Database Systems Study Group organized the Object-Oriented Database Task Group (OODBTG) to gather information on object database management systems and to recommend standards needed in this area. Their final report, which was issued in October 1991, contains [Ref. ANSI 1991]:

- Recommendations for standards in object data management
- Reference model for object data management
- Glossary of object data management terms
- Report on a survey of object data management systems
- Report on workshops on object data management standardization
- Bibliography.

In June 1991, SC21/WG3 recommended that SQL support for objects continue to be developed via the SQL3 specification and that the Reference Model rapporteur group consider other requirements, as appropriate beyond SQL [Ref. Gallagher 1991].

5.2.5.5 Full Text Manipulation in Structured Data

SC21/WG3 is including in its work on SQL standardizing support for full text manipulation in combination with the management of structured data using SQL. SQL2 will support storage of a collection of text as a single data value, but will be capable of the complex requirements for full text manipulation [Ref. SC21 N 5141 1990].

Standardization of SQL metadata that goes beyond IRDS has been proposed. Currently, SQL is being used as both the IRDS modeling and implementation language. A new standard may be required for more general information modeling applications support, which would support metadata about classes of information other than those normally defined for data retrieval systems. Examples of data models for information modelling applications are binary entity-relationship data model such as IRDS, N-ary entity-relationship data model, and object-oriented data model. One effort being conducted in this area in SC21/WG3 is the Tool Integration Standard. Additional efforts on all of these models are now being conducted in the United States. One standards issue in this area, as noted above, is whether relationships as well as entities should be permitted to have attributes. The OSI management information model (DIS 10165-1) has a containment relationship whose constraints could be represented as attributes of a containment relationship [Ref. SC21 N 4593 1990].

5.2.6 Distributed Transaction Processing (TP) Standards

5.2.6.1 TP Reference Model

A reference model for distributed Transaction Processing (TP), DIS 10026-1, has been developed by SC21/WG5. TP service elements are viewed as pertaining to the Application Layer. While TP service elements are discussed in relation to the information and data management services, some TP service elements may be required for the communications services.

5.2.6.2 TP Requirements

The user requirements addressed by DIS 10026 are to:

- Define procedures that support distributed transactions in order to:
  - Allow a distributed transaction to be organized into a transaction tree
  - Provide multi-party coordination, including local resources
  - Allow restoration to a consistent state, following failure of the state/context of a distributed transaction and of distributed information
  - Allow the detection of failure to achieve consistency
  - Allow a distributed transaction to be restarted following successful state restoration
  - Indicate successful completion or failure of a transaction.
- Provide for the delimitation of a sequence of logically related transactions.
- Allow the grouping of transactions within an applications process.
- Allow for access control, access control granularity on groups of TP objects, authentication, and non-repudiation.
- Allow conformance testing of the protocol and delineate clearly the static and dynamic conformance requirements (through a PICS statement).

5.2.6.3 TP Standards

The main elements of TP are as follows:

- DIS 10026-1.2, *OSI TP Model* [SC21 N 5671, 5 February 1991], second DIS July 1991
- DIS 10026-2.2, *OSI TP Service* [SC21 N 5673, 5 February 1991], second DIS July 1991
- DIS 10026-3.2, *OSI TP Protocol* [SC21 N 6567, 15 November 1991], second DIS expected November 1991
- CD 10026-4.2, *TP PICS Proforma,* October 1991 [SC21 N 5794, 28 March 1991]
- CD 10026-5, *OSI TP Application Context Proforma* [SC21 N 5160, 6 February 1991], ballot closed 9 July 1991
- CD 10026-6, *Unstructured Data Transfer (UDT)* [SC21 N 6222, 23 August 1991]
- WD 10026-7, *Other Data Transfer,* CD text expected November 1992.

Significant changes to the TP model (DIS 10026-1) made in December 1990 were removal of dynamic switching between chained and unchained transactions, thus enabling conforming systems to implement any one of three modes of operation: application-supported transaction, provider-supported chained transaction, and provider-supported unchained transaction. Provided-supported chained transactions require that each transaction within a dialogue use full two-phase commit procedures (CCR), while provided-supported unchained transactions always start with application-supported transactions (no CCR) with explicit request for two-phase commit support for each transaction that requires provider-supported commitment.

The TP protocol document (DIS 10026-3) has been restructured into a form intended to be more easily understood with simpler descriptive techniques. In addition, there were changes to simplify and correct protocol procedures. Special care was given to the two-phase commit protocol and its use of CCR services to ensure that all collision cases were resolved [Ref. SC21 N 5603 1990].

A committee draft for a standard for *Unstructured Data Transfer (UDT) for OSI Transaction Processing* (CD 10026-6) has been developed by SC21/WG5. This standard would allow interconnection of computer systems from different manufacturers, including those under different management; of different levels of complexity; and of different technologies. UDT is not suitable outside the TP environment. The draft consists of a model, service, and protocol for UDT and an annex for the application context for UDT. CD text was issued in June 1991 [Ref. SC21 N 5183 1990] .

A new work item was accepted by JTC1 for *Other Data Transfer for OSI TP* (WD 10026-7). Included in the scope of this work is development of TP queue services that would support transactions broken down into multiple steps. These services could also be used as the basis for a deferred transaction initiation mechanism or as a mechanism for reliable message transfer [Ref. SC21 N 5184 1990]. In its current form, the document is SC21 N 6231, *Preliminary Model and Service for Queued Data Transfer*. CD text is expected in November 1992.

Draft taxonomies for TP profiles have been developed by EWOS, Interoperability Technology Association for Information Processing (INTAP), and NAOIW. It is intended that the three will be harmonized fairly since they are fairly close together [Ref. EWOS 1991].

DIS 10026 will be used by the RDA standard and is being considered for use by RPC, extensions to IRDS, and extensions to FTAM. It is the first Application Layer service for distributed processing [Ref. SC21 N 4759 1990].

TP is dependent on a revised version of CCR that was progressed in 1989. Two formal descriptions of TP have been produced, one each in Estelle and LOTOS; both will be progressed as informative annexes to the TP protocol. TP activity will be conducted in

coordination with work on RDA (SC21/WG3) and Application Layer standards (SC21/WG6).

5.2.6.4 TP New Work Items

Table 8 identifies the new work items that have been proposed for TP [Ref. Bainbridge 1989]. A new work item on TP security [SC21 N 6232, July 1991] is intended to expand the TP model, service, and protocol (DIS 10026-1,2,3) to provide a secure environment for distributed transaction processing interactions involving multiple open systems. PDAD text is expected in 1993, DAD in 1994, and AD in 1995.

Table 8. New Work Items Proposed in ISO for TP

- TP Association Management--to provide for the management of application associations in a distributed processing environment involving multiple open systems [SC21 N 5177]. PDAMs to Parts 1, 2, and 3 expected November 1992.
- TP Commitment Optimization--to improve the performance and functionality of the commitment operation of a distributed transaction. Mechanisms being considered include alternate commitment initiator, commitment indication service, explicit selection of commitment coordinator, last subordinate optimization, multiple commitment initiators, real-only optimization, reversible ready, and unsolicited ready [SC21 N 6239]. PDAMs to Parts 1, 2, and 3 expected November 1992.
- TP Dialogue Recovery--the third phase of recovery (as defined in DIS 10026-1); it is required to enable Transaction Processing Service User Invocations (TPSUIs) to continue normal operation following the re-establishment of bound data consistency [SC21 N 4170]. PDAMs are expected June 1992.
- TP Heuristic Decisions--provides advisory propagation of a heuristic decision to all nodes; advisory propagation to nodes in the subtree below the node taking the heuristic decision; mandatory propagation of a heuristic decision to all nodes; and mandatory propagation to nodes in the subtree below the node taking the heuristic decision [SC21 N 4167]. PDAMs to Parts 1, 2, and 3. Date of CD text dependent on national body input; if not input is received, project is liable to reassessment.
- TP Savepoints--service to enable a transaction to be able to save and later restore a consistent state of all bound data under its control [SC21 N 4171]; new work item not accepted by JTC1, June 1990.
- TP Security--considers requirements for provision of a secure environment for TP in areas such as access control, auditing, authentication, confidentiality, integrity, management, nonrepudiation, replay, and revocation [SC21 N 5176, approved June 1990]. PDAMs to Parts 1, 2, and 3 expected June 1993.
- TP Subtransactions -extensions to TP that would provide partial rollback and nested transactions [SC21 N 5156]. In the current TP standard (DIS 10026), all the bound data that are involved in a transaction tree for a transaction are committed together and, if the transaction fails, all the bound data are rolled back. PDAMs to Parts 1, 2, and 3 expected June 1993.
- TP Separate Data and Commit Associations - Amendments to Parts 1, 2, 3, and 4. PDAMs expected June 1993 [SC21 N 5157].
- TP Conformance Testing. A two-part standard. CD on suite structure and test purposes expected October 1992 [SC21 N 6244]. WD on testing methodology [SC21 N 6243].
- Application Context for Systems Management with TP. Defines the context to be available in the systems management environment [SC21 N 6462].

Sources: [Refs. Bainbridge 1989; amended August 1991 IST/21: 2933 and SC21 N 6462 dated October 1991].

Work has begun on TP association management. The work is expected to produce an addendum to DIS 10026: CD text is expected in 1992, DIS text in 1993, and international standard text in 1994 [Ref. SC21 N 5177 1990]. The statement of requirements for TP association management was issued by SC21/WG5 in June 1990 [Ref. SC21 N 5171 1990]. It addresses association management objects for both application associations and application association pools, negotiations with remote

systems, pool sizing, query/status information, and manipulation of the authority to release associations. SC21 N 5835, *Discussion Paper on Association Pools as an Extension of ACSE*, April 1991, provides a possible overall approach for the NWI covering TP Association Management.

In May 1991, WG5 issued a *Working Document on TP Commitment Optimizations* [SC21 N 6239]. It presents a tutorial on the OSI TP commitment-optimizations. It also issued a *Working Draft for a Conformance Test Suite for the TP Protocol, Part 1, Test Suite Structure and Test Purposes* [SC21 N 6244].

Two approaches are being considered for using RPC and TP together [Ref. SC21 N 5172 1990]:

- With RPC as the data transfer paradigm for TP with use being made of TP dialogue management functions
- Using TP commitment functionality to complement the operation of RPC-based services (without necessarily making use of TP dialogues) to support "exactly once" semantics.

In 1989 a potentially serious problem was identified for TP. Under certain circumstances, protocol exchanges from one transaction (such as rollback) could overtake those outstanding from a previous transaction (and could therefore be interpreted by the receiving node as pertaining to the previous transaction). This can occur if lower layer expedited services are used to convey particular PDUs. The interim solution that was adopted was to avoid the use of Transport expedited data transfer services. A long-term solution to this problem is required to progress TP.

5.2.7 Open Distributed Processing (ODP) Standards

Open Distributed Processing (ODP), as distinct from a distributed system, allows both users and applications to interact remotely with any other computational resources (including other applications)held at different locations. A single application might also be divided into sub-units for execution in parallel on a number of machines linked together by a network. In its most sophisticated form, this allows multiple "clients" (users or their local applications) to request services from multiple remote "servers" using various software protocols such as a Remote Procedure Call (RPC) to achieve the required communications and synchronization. [Ref. OSN 1991j]

ODP is a new area of standards development. Begun in 1987, the work has progressed so far in ISO that a new working group (SC21/WG7) has been formed by the JTC1 to progress the standards for an ODP Reference Model. The current work comprises the framework of abstractions (e.g., the nature of the different points of view of a system); functions and interfaces; and modelling.

The Basic Reference Model of ODP is being developed in SC21/WG7 to provide a framework for standardization of distributed processing systems. It addresses the following aspects:

- Modelling distributed processing in terms of components, the services they support, their environment, and the interactions between them
- Identifying levels of abstraction at which the services and interactions can be described
- Classifying the boundaries between components and identifying the points of interaction associated with them
- Identifying generic functions performed by distributed systems
- Showing how the elements of the model can be combined to achieve ODP.

The Basic Reference Model (CD 10746), to be issued in 1993, of ODP further defines levels of abstraction at which services and interactions can be defined in other standards, generalizing the concepts of service and protocol defined in the OSI Reference Model (ISO 7498). The structure of the Basic Reference Model is as follows [Ref. SC21 N 4025 1989]:

- WD 10746-1 Part 1: *Overview,* containing a motivational overview of ODP, giving the scope, explaining the key definitions (with no substantial architectural content), and enumerating required areas of standardization (not normative)--CD expected May 1993, DIS in 1994, and IS in 1995 [SC21 N 6083, 30 May 1991]
- CD 10746-2 Part 2: *Descriptive Model,* defining the concepts, analytical framework, and notation for normalized description of (arbitrary) distributed processing systems (not normative but establishes requirements for new specification techniques)--progression to DIS may be held up until Part 3 reaches CD status [SC21 N 6079, 30 May 1991]
- WD 10746-3 Part 3: *Prescriptive Model,* specifying the required characteristics that qualify distributed processing as open--these are the constraints to which ODP standards must conform--CD is planned for June 1992, DIS in 1993, and IS in 1994 [SC21 N 6080, 30 May 1991]
- WD 10746-4 Part 4: *User Guide,* describing the resulting ODP environment from the users' point of view and containing explanatory material of how ODP is intended to be viewed by system engineers designing distributed applications to be run in the ODP environment (not normative)--CD text is expected May 1993, DIS in 1994, and IS in 1995 [SC21 N 6083, 30 May 1991]
- WD 10746-5 Part 5: *Architectural Semantics, Specification Techniques, and Formalisms*--CD text expected May 1993, DIS in 1994, and IS in 1995 [SC21 N 6082, 30 May 1991].

Part 5 of ODP is a formalization of ODP modelling concepts defined in Part 2. Part 5 defines requirements on specification techniques for ODP and evaluates standardized formal description techniques (FDTs) against these requirements. The formalization of modelling concepts, provided by a mapping to the concepts of each FDT,

acts as a bridge between the ODP architecture and FDTs. Part 5 incorporates work on the architectural semantics project [SC21 N 4655]. ISO/CCITT Joint Modelling Group has proposed the abstract specification language Z as a candidate FDT for use in ODP [SC21 N 6088].

In November 1990, Australia proposed a new work item to develop a standard entitled: *ODP Trader -- A Standard to Define the Role and Function of the Trader in Open Distributed Processing* (ODP) [ISO/IEC JTC1/SC21 N 5564, 3 January 1991]. CD text is expected in June 1993. The Trader is a component of an ODP system that supports trading interactions. A standard is needed to ensure [Ref. SC21 N 6085 1991]:

- Portability of applications in an ODP environment
- Internetworking between ODP systems
- Distribution transparency in ODP systems.

The approach of SC21/WG7 is to identify and expand a number of ODP topics in parallel. The applicable documents are:

- *Topics List--November 1989 Version--for the Basic Reference Model of Open Distributed Processing*, December 1989 [SC21 N 4019]
- *List of Open and Resolved Issues--June 1991 Version*, June 1991 [SC21 N 6073]
- *Topic 1--The Problem of Distributed Processing*, March 1988 [SC21 N 2507]
- *Topic 2.2--Properties and Design Freedoms*, December 1988 [SC21 N 3288]
- *Topic 2.3--Framework of Abstractions*, December 1988 [SC21 N 3194]
- *Topic 3--Structure of ODP Standards*, March 1988 [SC21 N 2509]
- *Topic 4.1--Structures and Functions*, December 1989 [SC21 N 4022]
- *Topic 4.3--Function and Interface Definitions* [SC 21 N 6081]
- *Topic 5.1--Modelling Techniques and Their Use in ODP*, December 1989 [SC21 N 4023]
- *Topic 5.2--Formalisms and Specification*, December 1989 [SC21 N 4024]
- *Topic 7.1--Basic RM of ODP*, December 1989 [SC21 N 4029]
- *Topic 8.1--Draft Basic RM of ODP*, Part II, December 1989 [SC21 N 4025]
- *Topic 9.1--ODP Trader*, May 1991 [SC21 N 6084].

In addition, SC21/WG7 has prepared a set of definitions and a glossary [SC21 N 2511] and a register of documents and bibliography [SC21 N 3192]. Further, SC21 has proposed a new question on the relationship between the OSI Upper Layer Architecture (ULA, see Section 6.2.1) and ODP. This question has been accepted into the JTC1 work program [SC21 N 6609, 6 December 1991].

5.2.8 Other Database Service Standards

CODASYL data management standards are the responsibility of the CODASYL Systems Committee. A report on distribution alternatives and generic architectures for distributed database systems was produced by this committee in 1980 [Ref. CODASYL 1980]. One of the two standard ISO data management languages (NDL) is based on CODASYL concepts.

In 1985, ECMA[17] issued a final draft report [Ref. ECMA 1985] for remote database access service and protocol.

ANSI standards for database architectures are produced by the Database Architecture Framework Task Group (DAFTG) through the Standards and Planning Requirements Committee (SPARC). A draft report [Ref. DAFTG 1982] from the DAFTG in 1982 provided a framework to support distributed databases, multiple data models, and data dictionaries. One concept, the ASN.1, has been specified [ISO 8824 and 8825].

CCITT does not provide standards for data management. The U.S. Government Open Systems Interconnection Profile (GOSIP, see Section 6.4.3) does not address standards for data management [Ref. GOSIP 1988].

5.3 Standards for Data Management

5.3.1 Data Element Standardization

The ISO has issued a draft proposal (DP 7826) on the representation of data elements. This draft proposal sets out standard procedures for the identification and representation of existing and new coding systems, without providing any guidance on specific coding systems.[18] It also specifies a technique for interchange of coded representations and the requirements for the administration of International Coding System Identifiers (ICSIs). This will permit the use of more than one coding system, reduce the possibility of ambiguity, reduce the need for human intervention, and diminish the time required to negotiate interchange of coded representation agreements. DP 7826 identifies three types of data element attributes: administrative, relational, and representative.

The U.S. Army has published an Army Regulation (AR 25-9) [Ref. DISC4 1988] to prescribe policies, responsibilities, and concept of operation for the management of data used in manual and automated information systems throughout the U.S. Army. This document has been coordinated with ISO, ANSI, and the NIST, as well as with the U.S. Joint Chiefs of Staff, to ensure alignment in the area of a data element naming convention.

---

[17] ECMA full membership is open only to companies who develop, manufacture, and sell computers in Europe. The restricted membership makes full consensus among participants in standards-making easier and quicker to reach than in ISO.

[18] ISO 646, ISO 2022, ISO 6937, and ISO 8859 are examples of standard coding system (see Appendix D, Sections I & E).

The U.S. Army plans to maintain a Service-wide data encyclopedia of information about all data elements that have gone through a standardization process and are designated as Army standard elements. AR 25-9 has been used for initial work on data element standardization for CIM. Additional information on AR 25-9 is provided in ATCCIS WP 7L [Ref. WP7L 1989].

Substantial work has been done cooperatively by ISO JTC1/SC14 and ANSI X3L8 during the last 3 years. This work has resulted in an X3L8 document entitled *Coordination of Data Elements*, which was accepted by SC14 as document SC 14 N 492. The objective is for application areas to interchange data among themselves predicated on shared generic concepts that would be documented in a Data Element Concept Taxonomy [Ref. Kenworthy 1991]. The general approach to the structure of data recommended in AR 25-9 and ATCCIS WP 7L was derived from discussions with ISO JTC1/SC14 and ANSI X3L8.

The data element naming convention and rules presented in AR-25-9 were derived from an emerging standard from the NIST *Guide to Data Entity Naming Conventions* [Ref. NIST 1987], which is expected to be offered to ISO in the near future. However, the rules were expanded in ATCCIS Working Paper (WP) 7L to support the concepts and structure of data consistent with the needs in NATO, SHAPE, and ATCCIS, as well as the emerging ISO taxonomy.

5.3.2 Policy and Issues for Data Management

5.3.2.1 NACISC Policy on Data Management

There is currently no promulgated data management policy for NATO. However, a working paper [Ref. ISWG 1991] was developed for the October 1991 meeting of the Information Systems Working Group (ISWG) of the NACISC that addresses data management policy [Ref. NACISC 1991]. The working paper was distributed by the Secretary of the ISWG in August 1991. The purpose of this document, jointly revised and refined by staff of the ISWG and ADSIA, is to provide a NATO policy for data management throughout the NATO Interconnected Information System (NIIS). It specifies the requirements and identifies the (1) elements of data management subject to NATO policy, procedures, and standardization and (2) activities required. It further identifies the extent of standardization required for different elements of data management. Table 9 provides excerpts from the working paper.

Table 9. Excerpts from the 1991 Working Paper by the NACISC on the Requirement for a NATO Data Management Policy

- Efficient interoperability in the NIIS requires consistency and integrity of data throughout these systems. This in turn requires the application of NATO-wide data management standards in this situation. The use of invalid data or the incorrect interpretation of data by other information systems can be disastrous for any type of operations. Each form of data exchange is worthless unless the meaning of data is understood unambiguously on both sides. Furthermore, if data is represented in different ways, translation will be required, which in turn hinders effective communication. Therefore, data management with its inter-system functions has to be planned and implemented to support the interoperation of systems by *preserving meaning and relationship in the exchange of data.* (Emphasis added.)
- Data management functions support the operation of a stand-alone as well as a distributed system and the information exchange among systems. These functions are
  - Data security
  - Data definition
  - Data manipulation
  - Data distribution
  - Data availability.
- Data availability is the capability to enable the users to access their data from predetermined locations, within agreed response times, and must expect recovery with predesignated times following preplanned, accidental, or other loss of service. This implies five subfunctions:
  - Data monitoring
  - Data system monitoring
  - Data backup
  - Data recovery and restart
  - Data audit trails.
- Data management functions are supported by the following tools:
  - Data model
  - Data dictionary
  - Database management system
  - Normalization.

Source: *NATO Data Management Policy*, Working Paper, AC/317(WG/2)WP/67, ISWG, 28 August 1991, NATO UNCLASSIFIED.

5.3.2.2 ADSIA Recommendations on Data Management

In April 1986, ADSIArevised a working paper [Ref. ADSIA1987] on the need for standardization of data management. The following actions were recommended:

- NATO Communications and Information Systems Agency (NACISA) to identify and collect the requirements for database management systems and for standardization of database schemes, file transfers, database information exchange, and configuration management procedures
- Subsequently, the Information Systems Working Group (ISWG) to develop a NATO policy on data management and on the use of database management systems in NATO CCISs
- ADSIA to coordinate the development of technical and procedural standards for databases
- ADSIA to develop the procedural standards for database information exchange
- TSGCE SG9 to develop technical standards for database schemes and file transfer

- NACISA to control the implementation of the developed standards and NATO policy paper to ensure the interoperability of command and control systems within the NATO CCIS.

5.3.2.3 NATO Interoperability Management Plan (NIMP)

Many aspects of data management are procedural in nature and will be controlled by procedural and not technical standards. Several of these standards are also identified below. The NATO Interoperability Management Plan (NIMP) [Ref. ADSIA1988] specifically identifies standards and rules for representing data as information procedural standards and assigns the responsibility for these standards to the Allied Data Systems Interoperability Agency (ADSIA). To emphasize the role of data management in achieving interoperability, the NIMP states:

> In order for the information exchange to be effective, it is necessary that the meaning and relationships associated with that information [received from other facilities] is common and preserved, irrespective of the interoperability service and transmission media. A single common definition for all operational information throughout NATO is needed to achieve this goal.

5.3.2.4 SHAPE Policy

The purpose of data management in NATO is to provide methods to ensure data availability, security, integrity, quality, and interoperability, and to provide data sharing. The *ACE Manual (AM) on Data Management,* AM 96-1-4 [Ref. SHAPE 1988], defines data as representing the elementary facts, descriptions, and qualifications about things of interest to some headquarters, unit activity, or enterprise. It further defines the role of a data dictionary as an automated tool that provides a centralized library of metadata covering all aspects of all types and structures of data residing in databases, file systems, and manual systems within an organization. AM 96-1-4 further asserts that:

- Evolution towards an ACE ACCIS will only succeed from the data management point of view by ensuring that the standardization of data definitions, the control of the data, and the maintenance of its overall integrity are systematically established on a command or site basis.
- The fundamental key to data management is the early definition and identification of data elements and, later, data fields. The definition and corresponding name should be clear, accurate, and meaningful, but reference should be given to connotation, which relates to the interpretation that bears upon the specific context of usage of data.

5.3.2.5 STC Work

In 1975, Shape Technical Centre (STC) published a Technical Memorandum (TM) (TM-776) on data management standardization for the ACE ACCIS [Ref. SHAPE 1985]. TM-776 recommends standardization of the architecture, functionality, and structure of the Data Management Subsystem (DMS) of the ACE ACCIS. These areas of standardization

include data management methodologies and the tools used to design, build, and maintain the ACE ACCIS databases. TM-776 accomplished the following:

- Identified the requirement that the DMS at each ACE ACCIS node must agree on the semantics and syntax of the information exchange.
- Recommended that there be a standard ACE data definition or conceptual schema, where a schema defines all application object types, including their attributes, relationships, and static constraints, and where a database is an instance of a schema.
- Stated that a data classification method must be used that is based on the principle of sorting data according to the type of information provided by their values, independent of their use in particular databases, messages, or applications.
- Identified the need for a methodology for formal definition of data elements based on standardized terminology, including the use of naming conventions:
  - A data element is defined as a basic unit of data that has a name, a definition, and a set of values for representing particular facts. A data element and its definition should not include any application or usage information.
  - A method is needed for analysing, defining, and controlling data elements. This method should have three components: a type classification of data elements, syntax rules for the structure and completeness of formal definitions, and a controlled vocabulary of permitted terms for formal definitions.
  - Standard data elements and relationships should be placed into an ACE common data structure.

5.3.2.6 NATO Publications on Data Management

AAP-6, *NATO Glossary of Terms and Definitions (English and French)*, standardizes terminology used throughout NATO, thereby promoting mutual understanding. The criterion for inclusion is that the term be of a general military application. While earlier editions put qualifiers immediately following the term, such qualifiers are now embedded in the definition. In addition, terms and definitions are not to be composed of, nor contain, abbreviations and acronyms. A term and definition are included in the glossary only when they have been agreed upon by all nations in both English and French.

The terms defined in ADatP-2 [Ref. ADatP-2 1985], *Automatic Data Processing (ADP) NATO Glossary, English and French*, are derived from glossaries, dictionaries, and vocabularies from ANSI, American National Directory for Information Processing, ISO, International Business Machines, and ACP 167. The definitions are annotated by source and may include abbreviations, examples, notes, diagrams, accepted synonyms, contrasting terms, related terms, and cross-references for multiple uses. This information is noted when harmonization is being examined for multiple uses.

ADatP-3 (STANAG 5500) [Ref. ADatP-3 1986], *NATO Message Text Formatting System (FORMETS)*, provides the rules, constructions, and vocabulary for standardized character-oriented message text formats that can be used in both manual and computer-assisted operational environments.

ACP 167 [Ref. ACP 167 1981], *Glossary of Communications-Electronics Terms*, provides definitions of terms used by communications, electronic warfare, and operational personnel for Allied networks.

5.3.2.7 Data Management Issues in EDI

The Special Working Group on Electronic Data Interchange (SWG-EDI) of JTC1 has identified a number of data management issues that require coordination within JTC1 (SCs 14, 18, 21, and 24) and with other Technical Committees (TCs) such as TC 46, 68, 154, and 184. The issues include [Ref. SC21 N 3925 1989]:

- Ensuring a complete separation of semantic and form of data elements, for which the conceptual schema is defined at a level other than the actual applications
- Accommodating different types of data representations, specifically with regard to the data models for different types of data, so as to assure logical relationships between data of different types can be expressed
- Structuring precisely the dictionaries of data elements and groupings, to include all the attributes of data elements and to permit unambiguous reference to other directories
- Assuring coherence of dictionaries across time (updating and maintenance) and sectors and also with generic dictionaries.

5.3.3 Data Management for Distributed Applications

The Workshop on Distributed Applications held by JTC1 in March 1990 noted that "very similar data management requirements are being addressed by differing standards applications" and that "potential exists for prevention of a considerable amount of duplication of effort and overlap...by increasing the extent of utilization of common aspects of data management facilities." Coordination was recommended among SC21/WG3 (Database) and WG7 (ODP), SC14, SC18, SC22, SC24, SWG-EDI, TC46, and CCITT SGs VII and VIII. Table 10 identifies common requirements for data structures and data models being addressed in ISO [Ref. SC21 N 4524 1990].

Table 10. Data Management Requirements Identified in ISO Relating to Data Structures and Data Models

• Federated data models
• Mapping to user-oriented data structures/operations
• Ability to support access control to data structures
• Wide range of sizes--large and small volumes of data
• Logging of operations for audit
• Ability to combine separately defined data types (static and dynamic)
• Application-oriented operations (e.g., searching)
• Support for internationalization
• Version control (including data structure modifications)
• Distribution, transparency support, and modelling location
• Handling of uninterpreted data
• Support of different levels of consistency and data integrity
• Ability to relate families of specifications for different levels of abstraction
• Support for recursive and structured definitions
• Persistent storage of results of operations
• Ability to support pointer types
• Ability to support powerful query languages
• Support for Directed Acyclic Graphs (including selection)
• Support for uniqueness requirements
• Independence from programming languages and means of access
• Support of declaration of hotspots and triggers
• Choice of granularity

Source: *Consideration of the Data Management Component of Application Standards*, Workshop on Distributed Applications, SC21 N 4524, 23 April 1990.

5.4 Assessment of Coverage by Standards

Until recently, there were very few international standards that applied to the database services other than those for SQL and NDL. Even so, the SQL standard is not very mature, and extensions will have to be agreed to and options reduced before SQL implementations can be expected to be interoperable. An example of a deficiency with SQL1 is that it does not address interactive queries to a DBMS.

ANSI and ISO are progressing different IRDS standards which could pose interoperability problems.

Standards for RDA and concepts for ODA show promise for use with standardizing database services and protocols. It is too early to tell how well these standards activities will cover the CCIS requirements. Moreover, technical deficiencies are holding up the progression of the RDA standard.

SC21 has identified three issues regarding its future study items, all related to databases. These issues are [Ref. SC21 N 3134 1988]:

- There is an urgent need to develop clear views on the relationships between database activity and OSI activity. Two major areas need to be addressed:

  - Relationship between IRDS work and activity on directories, and on the structure of management information
  - Relationship between export-import requirements and distributed database work, and OSI standards, in particular those to do with the storage and manipulation of information (i.e., FTAM).
- There is a need to clarify conformance requirements in relation to database standards, in particular:
  - Nature of conformance statements in database standards
  - Need for, and nature of, conformance test specification standards.
- There is a need to clarify security requirements in relation to database standards, in particular:
  - Security needs
  - Security approaches and mechanisms
  - Relation of SC20 work to database security requirements
  - Relationship of database security needs to other security work (in particular to OSI security) and to overall system security policies.

The objective of information and data management services for CCISs is to provide not only data processing functionality but also support for data objects. Not all of these objects can be specified with a relational model. Therefore, SQL will not, alone, be a satisfactory standard for database interfaces in CCISs. Some technical issues, together with related findings, that need to be addressed by the architecture before the adequacy of standards can be determined are:

- Degree of distribution or centralization for data management. Two classes of standards are being developed for distributed systems (Distributed Transaction Processing and Open Distributed Processing), but the basic standards work will not be completed before 1994, at the earliest. Moreover, the Distributed Transaction Processing standard cannot be progressed until a technical problem with the transport (lower layer) expedited data transfer services is solved.
- Determination of what models are required for the conceptual schema, in addition to the relational model for information items to be managed. Database languages are mature only for the hierarchical (NDL) and relational (SQL) models. The current standard for SQL does not address many important database interface services, but some of these will be standardized by SQL in 1992. Further work is required (SQL3), but this work is still in a preliminary stage, with no set scope or schedule.
- Functionality to be provided to the user for ad hoc queries. Menu-driven functionality may be adequately supported by emerging standards for user interfaces (Terminal Management and X-Windows), but direct interface to SQL may require use of nonstandard extensions. Some of these extensions may be available in products in 1995, but lack of standardization may reduce the degree of interoperability and portability of implementations.
- Need for expert system or other artificial intelligence-base interface mechanisms to the database. Standards for such interfaces have not been developed.

- The technologies to be employed, such as special-purpose database hardware (to improve, for example, access time), optical storage devices, fibre-optic communications, and high-speed local area networks. Standards in these areas are being developed but are not yet mature.

(This page intentionally left blank.)

6. NETWORK SERVICE STANDARDS

6.1 Network Service Requirements

Network services provide the standard utilities that allow applications, operating systems, and database management software executing on distributed, heterogeneous computers to achieve interoperability with acceptable performance levels. CCIS architectures will address such topics as real-time communication; synchronization; quality of service; security; incorporation of video, audio, and data onto a single system; priority; and preemption. Network services address data communications, transparent file access, and remote process execution. An overview of the status of standards for network services is given in Table 11 (TFA is transparent file access).

Network services provide functionality to allow different parts of a CCIS, or two CCISs, to invoke services one from another. These include data transfer protocols, services of the communications infrastructure, and services to manage data transfer and communications.

Quick Reference

Topic	Page
ACSE	120
ALS	100
Application Layer	99
Applic Service Element	120
ASN.1	126
Assessment	137
ATM	134
Broadband ISDN	133
BER	128
CCR	121
Directory	113
FDDI	136
FTAM	108
Interworking	97
ISDN	132
JTM	119
MHS/MOTIS	105
MMS	108
OSI Reference Model	95
Requirements	95
ROSE	123
RPC	124
RTSE	122
Stacks of Standards	103
TCP/IP	129
Time Synchronization	131
XALS	101

6.2 OSI Reference Model, Interworking, and Application Layer Structure

This section summarizes the elements of the OSI Reference Model, interworking of layers, and the structure of the Application Layer. It also addresses the characteristics of distributed applications and related architectural standards work.

Table 11. Status Overview of Key Network Service Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
OSI (e.g.,GOSIP)	●	○	●	●	○	○	○
TFA		○					
OSF/1 NCS/RPC							

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

6.2.1 Status of OSI Reference Model, ISO 7498

The OSI Reference Model has four elements: *Basic Reference Model* (ISO 7498), *Security Architecture* (ISO 7498-2), *Naming and Addressing* (ISO 7498-3), and *Management Framework* (ISO 7498-4). Connectionless-mode aspects were originally addressed as Addendum 1 to ISO 7498. Multipeer Data Transmission (MPDT) is addressed as Addendum 2 and Upper Layer Architecture (ULA) as Addendum 3.

Balloting for SC21 N 3287,[19] *Proposed Draft Addendum 2 on MPDT* (ISO 7498-1/PDAD2), ended 15 July 1989. Work in ISO on MPDT has been suspended in SC21/WG1, since the nations did not demonstrate specific interest in continuing this work. The completed work is planned to be released as a technical report. New work in ISO on MPDT may come in the form of standards for multi-party communications (MPC), defined as information distribution within groups of end open systems. A May 1990 Canadian contribution to SC21 identified the basic driving forces for MPC as the coordinated interworking of more than two application processes in a single activity and use of inherently shared resources of certain subnetwork types. "Group" processing was identified as one of the next "hot topics" for standardization and was expected to include such activities as conferencing, co-authoring, sensor-based data collection, and process control--all of which involve MPC [Ref. SC21 N 4681 1990]. The U.S. requested reactivation of the MPDT project at the May 1991 meeting of WG1. The request was rejected pending technical contributions.

ISO 7498 is being revised to incorporate general aspects, upper layers, and lower layers into ISO 7498-1, *Basic Reference Model.* A committee draft of the revised text [SC21 N 6152] was distributed in November 1991. The revision will permit routing and relaying between individual local networks in the Data Link Layer. This work is being coordinated with CCITT [Ref. SC21 N 5074 1990]. Other work includes clarifying the distinction between connectionless and connection-mode operation, aligning the service definitions for the lower layers and also for the upper layers, improving consistency of layer descriptions, adding Reset as a facility to the Data Link Layer, adding Suspend and Resume as functions in the Transport Layer, and aligning this work with CCITT [Refs. SC21 N 5095 1990; SC21 N 5096 1990].

DTR 10730, *Tutorial on Naming and Addressing*, has been developed to introduce the main concepts and mechanisms that are defined in 7498-3 to fulfill the needs for naming and addressing objects in the OSI environment. It also includes the rationale for some of the important decisions made in the naming and addressing architecture.

---

[19] SC21 N xxxx denotes an ISO working draft standard or technical paper distributed throughout SC21. Such drafts applicable to CCISs are listed at the end of the first section of Appendix E.

The OSI Reference Model is being supplemented by a number of other models and frameworks within the context of OSI. These include Application Layer Structure, Internal Organization of the Network Layer, and the Transaction Processing Model [Ref. SC21 N 5081 1990]. Conventions for specifying OSI service definitions are also being developed. DIS text has been distributed in ISO for a new standard, *Conventions for Service Definitions*, DIS 10731 [SC21 N 6341, August 1991]. The three parts are *General Model and Conventions, Application Layer,* and *Layers 1-6*. DIS 10731 will supersede TR 8509, which provides interim guidance to users and definers of service standards.

6.2.2 Interworking of Lower Layers in OSI

The basic interworking standards used for specifying relays are the following (examples of relay profiles using these standards are given in Appendix B):

- DIS 10028-1, *Definition of the Relaying Functions of a Network Layer Intermediate System, Part 1: Connection-mode Network Service* (awaiting DIS ballot)
- CD 10028-2, *Definition of the Relaying Functions of a Network Layer Intermediate System, Part 2: Connectionless Network Service* (awaiting CD ballot)
- TR 10029, *Operation of an X.25 Interworking Unit,* March 1989
- ISO 10030-1, *End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878,* 11 October 1990
- CD 10030-2, *End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878, Part 2: PICS Proforma* (awaiting CD ballot)
- DIS 10038, *Media Access Control (MAC) Sublayer Interconnection (MAC Bridging)* (awaiting DIS ballot).

ANSI X3S3 has three MAC-related liaison projects with JTC1/SC6 underway:

- To develop a technical report that will provide a description of the representation of MAC Addresses. The report will record all values assigned for the use of Standards in one document, whereas at present this information is scattered across a number of documents [Ref. X3 1991b].
- To develop an amendment to DIS 10038 that will extend the scope to include source routing capability [Ref. X3 1991c].
- To develop a technical report that will provide guidelines for LANs implementing "source routing operation" defined in DIS 10038/PDAM2, *MAC Bridging - Source Routing Supplement* [Ref. X3 1991d].

TR 10172, *Network/Transport Protocol Interworking Specification,* 15 October 1990 [SC6 N 5906, March 1990], addresses the inability of end systems operating in the CO network protocol (ISO 8208/8878 X.25) and CL network protocol (ISO 8473) to interwork with each other. A mediating device, called the Interworking Functional Unit (IFU), is defined to perform relaying and/or conversion of protocol data units (PDUs) from

one network protocol type to another. Three modes of operation are considered in DTR 10172:

- Network Layer Relay (NLR). In the NLR mode the IFU operation functions as a regular intermediate system. CL NLR operation is in accordance with ISO 8473 and CO NLR with ISO 10177 and ISO 10028.
- Passive Transport Layer Relay (PTLR). PTLR does not itself operate on the PDUs of transport connections, but passes transport PDUs received in network service data units from each end system transparently to the other end system.
- Active Transport Layer Relay (ATLR). ATLR provides an end-to-end transport service by operating a separate transport connection to each of the connected end systems and relaying data from one connection to the other.

Since the PTLR and ATLR modes of operation lie outside the scope of the OSI architecture, the technical report is not planned to be converted to an ISO standard.

Network Relay (also called Routing), however, is the most important outstanding issue in the Network Layer. The standards that describe the protocols and algorithms for routing over a connectionless network service have progressed rapidly over the last 3 to 4 years, after a slow start, and final standards and products that implement them should start appearing before the end of 1991. The equivalent work on routing for connection-oriented networks has proceeded more slowly, and it is not clear when draft standards will be published. Examples of network relay profiles appear at the end of Appendix B. Three OSI standards are of particular importance to the provision of open routing:

- ISO 8473, *Protocol for Providing Connectionless-Mode Network Service*
- ISO 9542, *End System to Intermediate System (ES-IS) Routing Exchange Protocol*
- DIS 10589, *Intermediate System to Intermediate System (IS-IS) Intra-domain Routing Exchange Protocol* (IS expected during 1991) [Ref. OSN 1990b].

EWOS has released a *Technical Guide to Routing in the Context of OSI*, EWOS-EGLL/91/72 [IST/21:2860], 27 May 1991.

Task Group ANSI X3S3.7 of Accredited Standards Technical Committee X3S3 - Data Communications is developing a draft standard describing the interworking between two packet switched data networks (PSDNs) via an X.25 link. This draft standard (Project 682-D) would typically be used for interworking between a packet switched public data network (PSPDN) and a packet switched private data network (PSPvtDN). It specifies the general addressing and routing principles associated with two PSDNs and their interworking as well as the procedures to be followed by an interworking function (IWF) that is used to connect the PSPDN and the PSPvtDN [Ref. X3 1991e].

The following comment on CL-mode and CO-mode interworking was provided to SC21 following a February 1990 meeting of CCITT SG VII regarding the proposed update to the OSI Reference Model (ISO 7498-1) [Ref. SC21 N 4559 1990]:

> The connectionless/connection-mode crossover rules currently proposed by ISO appeared, to many of the Q23/VII attendees at this meeting, to be unacceptable for use in fully supporting connectionless-mode CCITT applications, due mainly to interconnectivity problems. Many of the attendees felt that, for "across-the-board" support of connectionless CCITT applications, within the lower layers, there is a need to have common (mandatorily provided) support required that would assure interconnectivity among all connectionless-mode OSI CCITT applications. It was unanimously agreed that the concept of attempting to solve such interconnection problems exclusively through introduction of any "transport relay" concept in CCITT Recommendations is totally unacceptable.

Accredited Standards Committee X3 recently formed a new Technical Committee, ANSI X3T6, Non-Contact Information Systems Interface (NCISI). The primary goal of this committee will be to develop a non-contact standard interface between computer devices for the transfer of information. The committee is developing a standard for U.S. activities; however, it eventually intends the standard to be submitted to ANSI as a JTC1 Fast Track Candidate for approval as an international standard. The committee will review current technology in radio frequency data/communication, infrared, and similar non-contact data transfer technologies with the objective of standardizing the interface between like devices. The standard would be restricted to the interface, allowing unrestricted development of computer components on either side of the interface [Ref. X3 1991f].

6.2.3 Application Layer Concepts

The Application Layer differs from the other layers of OSI in several respects. Entities in the Application Layer are made up of a collection of application service elements (ASEs), each of which is defined by a set of service and protocol standards. These ASEs are combined in various ways to form several types of Application Elements (AEs).

Standards in the Application Layer define procedures for the support of distributed information processing. The Presentation Layer supports the Application Layer by providing facilities for representing information exchanged between AEs. The Session Layer provides the mechanisms that may be used for controlling interactions between AEs.

6.2.3.1 ISO Studies on Application Layer

In its November 1989 Strategic Plan, JTC1 directed five initial major technical studies in order to address new or expanding areas to provide a basis for planning the JTC1 long-range program. The studies of required standards are all applicable to the Application Layer:

- Defining interfaces for application portability
- Defining interfaces required for distributed systems and applications

- Integrating voice, data, text, graphics, and image information at the user application level
- Addressing the area of artificial intelligence
- Supporting modelling of user requirements.

6.2.3.2 Application Layer Structure (ALS)

ISO 9545, *Application Layer Structure,* was published by ISO in December 1989. This was based on work done by SC21/WG6. ISO 9545 defines the nature of standards in the Application Layer and the relationships among them, the architectural framework in which individual OSI Application Layer protocols shall be developed, and the categories of identifiable objects that are necessary for the specification and operation of protocols. It also relates distributed information processing activities to the standards in the Application Layer. Key concepts from the ALS are the following:

- Association (application association)--a cooperative relationship between two AE invocations for the purpose of communicating information and coordinating their joint operation. This relationship is formed by the exchange of application protocol control information using the Presentation Service.
- Application context--a set of rules shared in common by two service element (SE) invocations in order to enable their cooperative operation. The application context is an example of a shared conceptual schema. SC21 N 5502 is a liaison to CCITT Q23/VII concerning application context negotiation during association establishment.
- Single association object (SAO)--the collection of things in an AE invocation related to a single application association.
- Single association control function (SACF)--the component of a single association object that represents the use of those rules in the application context concerning interactions among ASEs within a single application association.
- Multiple association control function (MACF)--a component of the AE invocation that coordinates the interactions among multiple associations within an AE invocation in order to provide a coordinated service.

An amendment to ISO 9545 for connectionless mode transmission has been in the working draft stage since 1988. Progression to PDAM status was proposed in July 1991.

SC21 N 4903, PDTR xxxx, *Methodology and Guidelines for the Development of Application Layer Protocols,* June 1990, is being developed by SC21/WG6 to provide a discipline for the development of application protocol standards in order to generate precise specifications. It describes a step-by-step procedure for generating ASE definitions and protocol specifications. This new work item of 1988 failed but the program of work with CDTR is still active, making its status uncertain. SC21 N 6061 requested comment on progression of the work by 20 March 1992.

A question concerning Versions and Extensibility [SC21 N 6060, 30 May 1991] of the ALS has come to the attention of SG6. Variants of Application Layer protocols may arise for a number of reasons; for example, a protocol may be revised to support additional capabilities or to provide different capabilities. It is important to ensure that Application Layer protocols are designed so as to enable implementations of different variants to co-exist and interwork (where feasible), and, equally importantly, to provide an environment that facilitates the orderly migration from one network systems configuration to another.

SC21 N 6068, *Modelling Recovery in the Application Layer*, 12 June 1991, is potentially the basis for a new part or an amendment to ISO 9545. It adds to concepts and principles of ISO 9545 by categorizing the nature of failures visible in the Application Layer and defining the concepts and modelling principles for recovery.

6.2.3.3 Extended ALS

Work on an extended ALS (XALS) model has begun (ISO 9545 PDAM 1). The purpose of XALS is to supplement ISO 9545 (*Application Layer Structure*) by providing a more complete framework for development of Application Layer protocol standards that use other Application Layer protocol standards. A central focus of XALS is extension of the architecture for use of multiple associations [Ref. SC21 N 4901 1990]. An Editing Meeting in July 1991 recommended that the amendment be forwarded to ITTF for DAM registration and letter ballot. [Ref. SC21 N 6304 1991]

XALS is planned to provide a revised ALS model that is significantly richer in scope and descriptive capability than is provided in ISO 9545. As a result, it will provide more options for the specification of Application Layer standards. Examples of new features being proposed for the XALS are:

- Defining Application Service Elements (ASEs), application service objects (ASOs), and control functions. An ASO is made up of one or more ASEs and/or ASOs, and a control function. A control function is the component of an ASO that controls the interactions among ASEs and/or ASOs within the containing ASO [Ref. SC21 N 4002 1989].
- Providing guidance for ASE specifications in the areas of the reference model the ASE supports, the service definition, the abstract protocol definition, and the ASE environment requirements specification.
- Addressing peer-to-peer (application level) relationships as well as the established concept of application association, such as are used on MHS, TP, EDI, and Directory.
- Accommodating both peer-to-peer and client-server interaction styles. (ROSE supports both styles of interaction. X-Windows and DOAM use client-server styles, for which the terminal in the X-Window environment is the server, whereas the terminal in the DOAM model is the client.)

An approach being considered for XALS for defining ASEs is that each ASE is a complete specification of a function, together with the application protocol data units

(APDUs) that support it. The APDUs are defined in one or more abstract syntax specifications within the ASE standard. The name of the specification is a parameter used when establishing a presentation connection, with each resulting transfer syntax assigned its own presentation context. Concurrent use of multiple ASEs would be accomplished by either APDU concatenation or embedding one APDU in another as user data. FTAM, CCR, VT, and ACSE fit this proposed model, but not Directory, ROSE, or RTSE. The Directory protocol, for example, is used in conjunction with ROSE to completely specify an abstract syntax--the relationship between Directory and ROSE is not one of APDU concatenation or user data embedding. Use of XALS would benefit work in RPC and other ASE areas [Ref. SC21 N 4519 1990].

Future work on XALS is expected to include the following:

- Peer-to-peer relationship (in addition to application associations) [Ref. SC21 N 4905 1990]
- Recovery model, new work item (JTC1 N 764) approved June 1990 [Refs. SC21 N 4910 1990; SC21 N 5011 1990]. [SC21 N 4106; CD target date not available]
- Multi-level structures, new work item (JTC1 N 846) approved June 1990 [Ref. SC21 N 4909 1990].

6.2.4 Distributed Applications

Application Layer standards often define, at least partially, distributed applications. Examples are MHS, Directory, and FTAM; specifically, Directory contains a specification of a directory information tree (DIT) and its associated navigation rules. The nodes of the DIT for CCITT are envisioned to be distributed worldwide. Such standards contain elements that relate to features (and models) of distributed applications, in addition to features related to communications transfer. In this regard, these standards relate both to the ODP model and the ALS model.

The following are examples of tasks being proposed in generic work on distributed applications [Refs. IST/21: 1721 1989; SC21 N 4520 1990]:

- Model information held by distributed applications and address issues of distribution and local transparency (the ODP work has chosen to recognize five different viewpoints from which various features of a distributed application can be modelled); *Modelling for Communications Aspects of Distributed Applications* has been accepted by JTC1 and assigned to SC21/WG6 [Ref. SC21 N 4911 1990]. CD target date not available.
- Formalize management interactions between application processes in specific protocols in such functions as establishing relationships, distributing data, and replicating data.
- Devise global security mechanisms for use throughout the entire domain of the distributed application.

- Enable the schema for information held at an applications process to be distributed among cooperating systems.
- Address database issues such as data integrity and consistency, together with replication of data.
- Identify constraints on process decomposition and interaction types (communication among subprocesses).
- Specify distributed application support for configuration management, reconfiguration, and routing.
- Define application features to allow migration for future extensions.
- Address real-time effects associated with distribution.
- Provide for time synchronization of application processes.

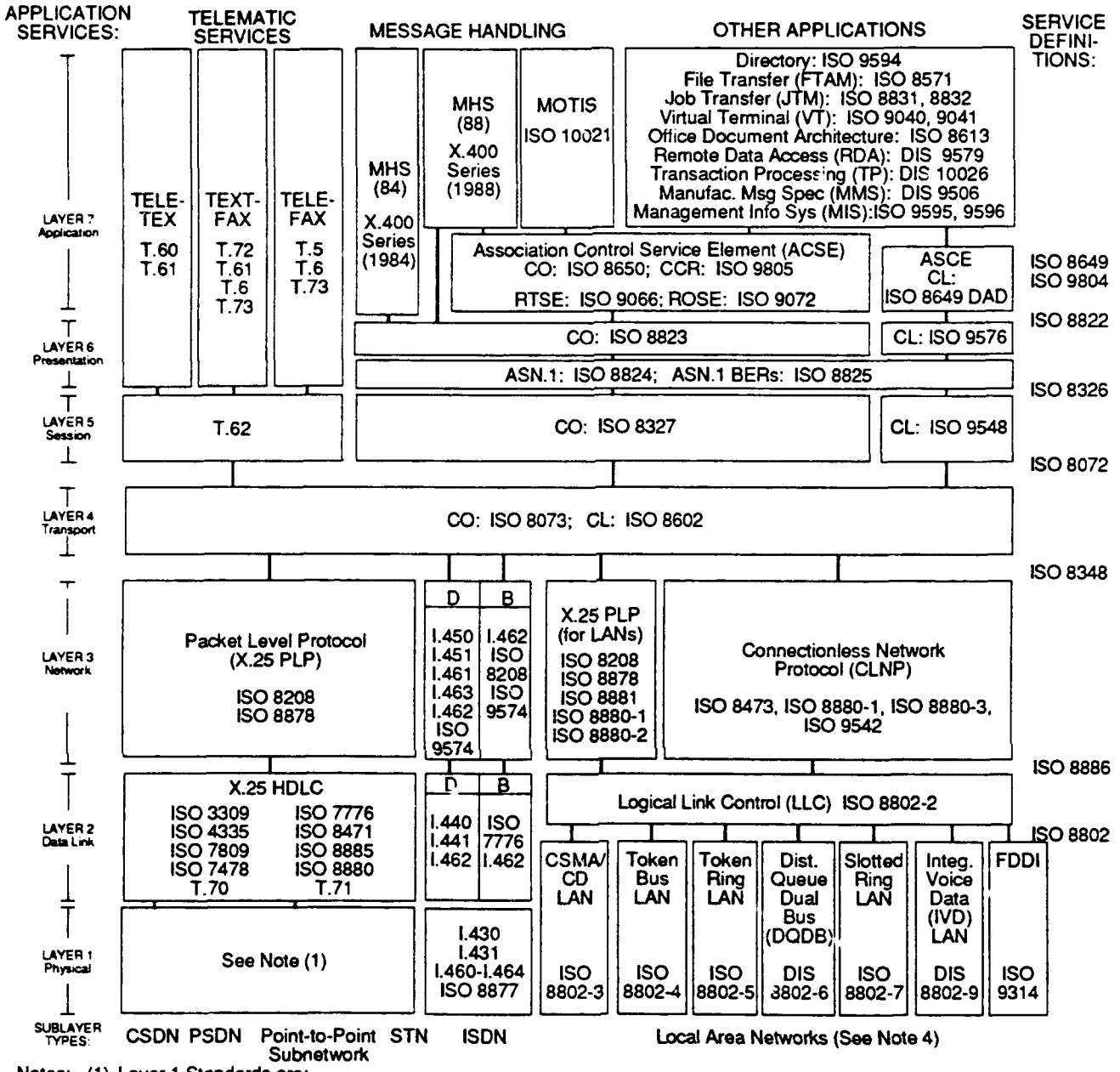
However, true distributed applications have yet to be achieved since the network is not hidden. A promising tool in this area is the RPC tool (see Section 6.3.6.5), which allows applications at run-time to move from one transport, such as TCP/IP, to another such as OSI [Ref. OSN 1990c].

6.3 Standards for Network Services

This section begins with a description of the base standards that have been defined for the OSI seven-layer model. Stacks of base standards are described separately for application options, transport options, and relay options. The chapter concludes with an overview of ongoing work for developing international standardized profiles and OSI environments.

6.3.1 OSI Base Standards and Stacks of Standards

Figure 13 provides an overview of the standards applicable to network services for data communications. The layer OSI standards are connected by vertical lines to depict a wide range of stacks for application and transport options. OSI management, security, registration authorities, conformance testing, and other standards applicable to all the classes of services are identified and discussed in Chapter 9--these are not included in Figure 13. U.S. GOSIP is based on the standards shown in Figure 13.



Notes: (1) Layer 1 Standards are:
(a) CSDN/PSDN: ISO 2110, 2593, 4902, 4903; V.24, V.28, V.35, V.36; X.21, X.21bis, X.22, X.24, X.26, X.27,
(b) Point-to-Point Subnetwork: Predefined
(c) STN: ISO 2110, 2593, 4902, V.10 or V.11, V.20, V.24, V.27, V.31bis, V.35, V.36, V.37, V....

(2) Standards are CCITT unless designated ISO, DIS, or DP.
(3) Stacks are based on 1989 *NTIS Transition Strategy*.
(4) Each LAN standard addresses both Layer 1 and Layer 2 (Media Access Control).

Figure 13. Stacks of Standards for Application and Transport Options

Figure 13 depicts examples of possible application and transport options. The types of transfer service options are identified along the bottom of the figure. Standards and options in a layer common to several stacks are shown in blocks. For example, the Logical Link Control (LLC) in Layer 2 is common to stacks for all types of LANs shown in Figure 13. Above the LLC, the CO-mode X.25 Packet Level Protocol (PLP, ISO 8208, 8878, 8880-1, 8880-2, and 8881), and the connectionless network protocol (CLNP) apply to each of the four LAN options. The X.25 PLP (ISO 8208 and 8878) in Layer 3 and the High-Level Data Link Control (HDLC) in Layer 2 are required for the stacks for four types of circuits: Circuit Switched Data Network (CSDN), Packet Switched Data Network (PSDN), Point-to-Point Subnetwork, and Switched Telephone Network (STN).

Task Group X3S3.7 of Accredited Standards Technical Committee ANSI X3S3 - Data Communications has begun an effort to develop a standard to be used in conjunction with frame relay standards. It could be used in other cases where X.25 virtual circuit (VC) establishment and clearing procedures and other non VC-specific procedures are not needed. This standard will be a subset of Recommendation X.25 and ISO 8208 [Ref. X3 1991g].

6.3.2 MHS and MOTIS

6.3.2.1 Message Handling Standards

Table 12 summarizes the set of standards that define MHS (CCITT X.400) and the Message-Oriented Text Interchange System (MOTIS, ISO 10021) services. Efforts have been made by CCITT and ISO to converge MHS and MOTIS. The result, defined by standards released in 1988, is a substantially but not completely compatible set of new standards. [Balloting for the previous MOTIS standards (DIS 8505, DIS 8883, and DIS 9065) was suspended, and the scope of these standards has been incorporated in ISO 10021.]

The relationship of the X.400-1984 (MHS-84), X.400-1988 (MHS-88), and MOTIS-1988 standards is also provided in Table 12. Notice that MOTIS still has no parallel to the X.408 standards for algorithms used when converting between different types of encoded information, no parallel for the X.430 (now T.430) Teletex access protocols, and none for X.443.

MHS-88 provides new (relative to MHS-84) capabilities for message store (listing, summary, fetching, and deletion of stored messages); security services (origin authentication, secure access management, data confidentiality, data integrity, nonrepudiation, and security management); distribution lists (members, submit permission, expansion point, and owner); directory services (authentication, name resolution, data list expansion, and capability assessment); physical delivery service (basic physical rendition, ordinary mail, physical forwarding, and return of undeliverable mail); and conformance

testing (methods, criteria, and notation). In addition, MHS-88 revises MHS-84 standards for naming, addressing, routing, and special access.

Table 12. Base Standards for Message Management

LAYER	MHS CCITT X.400-1984	MHS CCITT X.400-1988	MOTIS ISO-1988
7 7	X.400 X.401	X.400[a]	ISO 10021-1
7	X.400	X.402	ISO 10021-2
7	N/A	X.403[b]	None
7	N/A	X.407	ISO 10021-3
7	X.408	X.408	None
7	X.409	X.208 X.209	ISO 8824 ISO 8824 DAD1 ISO 8825 ISO 8825 DAD1
7	X.410	X.218 X.219 X.22 X.2298	ISO 9066-1 ISO 9072-1 ISO 9066-2 ISO 9072-2
7	X.411	X.411 X.419[c]	ISO 10021-4 ISO 10021-6
7	N/A	X.413	ISO 10021-5
7	X.420	X.420	ISO 10021-7
7	X.430	T.430	None
7 (ACSE)	N/A	X.217 X.227	ISO 8649 ISO 8650
6	N/A	X.216 X.226	ISO 8822 ISO 8823

Source: Provided by OMNICON on 8 September 1988.

[a]1988 X.400 is double-numbered with 1988 F.400.

[b]Citation for 1988 X.403 includes three manuals.

[c]1988 X.419 and ISO 10021-6 have a wider scope than the part of 1984 X.411 and DIS 8883 that they replace.

6.3.2.2 MHS-1984 and MHS-1988 Profiles

The standards for MHS-84 include delivery notification, disclosure of other recipients, explicit conversion (Message Transfer Service), grade of delivery selection, hold for delivery, prevention of non-delivery notification, probe, stored message alert, and stored message automatic forward.

The 1988 CCITT X.400 recommendations are supplemented by a new series of standards on the service aspects of MHS. These standards are:

- F.400 *System and Service Overview*
- F.401 *Naming and Addressing for Public Message Handling Services*
- F.410 *The Public Messaging Transfer Service*
- F.415 *Intercommunication with Public Physical Delivery Services*

- F.420 *The Public Interpersonal Messaging Service*
- F.421 *Intercommunication Between the IPM Service and the Telex Service*
- F.422 *Intercommunication Between the IPM Service and the Teletex Service.*

According to analyses conducted by TSGCE SG9/WG2, MHS-88 is not fully backward compatible with MHS-84 (due to changes in data type formats in the P1 protocol) and, even with a gateway between systems using different versions of MHS, there are several differences [Ref. Rose 1990] that could cause interoperability problems. For example, MHS-84 is unable to use the physical delivery capability of MHS-88. In addition, MHS-88 users may not be able to communicate with Telex terminals on an MHS-84 system. Finally, MHS-84 systems will reject some addresses that may be valid for MHS-88 systems. Addressing these problems without service request rejection will require a complex gateway. The incompatibilities of the MHS-84 and MHS-88 standards could present serious interoperability issues since ADP-supported CCISs might adopt the newer standard, but a variant of the older standard [*Standard Automated Message Interface for NATO's ACCISs (STAMINA),* described in Appendix K] has been mandated for the ACE Automated Command and Control Information System (ACE ACCIS) that supports battlefield command and control entities at echelons above corps. Note that while the 1989 *NTIS Transition Strategy* [Ref. NATO 1989] identifies the MMHS(84) as an intercept interoperability functional profile, the following caveat is included:

> It must be clearly stated that the MMHS-STANAG will be based on CCITT X.400 series version 1988, which offers a considerably enhanced functionality, including security services. Problems with backward compatibility cannot be precluded.

However, backward compatibility of MHS-88 with MHS-84 is being claimed by many technical experts [Refs. NIST 1988; NIST 1989; Manvos 1989; X.400 1989; OSN 1988]]. According to Jim White [Ref. OSN 1988], CCITT Special Rapporteur for X.400, "backwards compatibility between 1984 and 1988 P1 has been achieved." P1 is the relay protocol from one Message Transfer Agent (MTA) to another. 1988 and 1984 products implementing P1 would be able to interwork because the 1988 P1 is a superset of the 1984 P1. However, the same is not true of the P3 protocol used for submission and delivery access for a remote User Agent. Specifically, it is not possible for a 1988 UA to use the P3 protocol to communicate with a 1984 messaging system. The rules that a 1988 system shall obey when interworking with 1984 systems are defined in Annex B, *Interworking with 1984 Systems,* of CCITT X.419.

6.3.2.3 ACP 123 Common Message Format

Beginning in May 1990, subject matter experts from many nations have been meeting to develop a common messaging strategy that can be deployed to facilitate interoperability among the Allies. The strategy, which will include the definition of a new

Common Message Format (CMF) and corresponding procedures, is to be based on X.400. The end goal is to replace the existing messaging system currently based on the Allied Communication Publication 127 (ACP 127) and associated documentation (i.e., ACP 117 and ACP 121). The work in the United States is being conducted under the auspices of the Defense Message System.

The X.400-based ACP will be called ACP 123. Major work has been completed in the area of requirements, and some, but not all, procedural issues have been resolved. The new standard will satisfy not only the ACP 127 requirements, but also national requirements such as the US Joint Army, Navy, Air Force Publication (JANAP) 128 message requirements. The work will use the MMHSwork of the TSGCE SG9, including the mappings between ACP 127 and X.400 that have been defined in draft STANAG 4406 (provided in December 1991 to SG9 for promulgation for ratification--see Section 15.3.8). [Ref. ACP 123 1991]

6.3.2.4 Manufacturing Message Specification (MMS)

A Manufacturing Message Specification (MMS) has been defined. MMS is the key component of the Manufacturing Automation Protocol (MAP), the OSI protocol promoted worldwide by General Motors. MMS was originally developed as Electrical Institute of America (EIA) RS-511 [Ref. INI 1987]. The MMS standard has two parts: ISO 9506-1 *(Service Definition)* and ISO 9506-2 *(Protocol Specification)*. While MMS is a standard primarily used for industrial automation, it is included because its wide use may affect some military message standards. Section 6.3.8.2 discusses the time-critical communications requirements of MAP.

The MMS work in ISO is under TC184/SC5/WG1, which is responsible for communications systems in the area of industrial automation [Ref. Kirk 1990]. In 1989, a new work item to develop an international standard, *Framework for CIM Systems Integration*, was assigned to SC5/WG1. Efforts are focused on ENV 40 003 based on the CIM-OSA work from the European Strategic Programme of Research and Development in Information Technology (ESPRIT).

6.3.3 File Transfer, Access, and Management (FTAM)

6.3.3.1 FTAM Standards

FTAM defines a file service and specifies a file protocol within the Application Layer (Layer 7). The standard is concerned with identifiable bodies of information that can be treated as files, which may be stored within open systems or passed between application processes. ISO 8571 defines the basic file service for FTAM. It provides sufficient facilities to support file transfer and establishes a framework for file access and file management. This standard does not specify the interfaces to a file transfer or access facility within the local system. An addendum may be added that reflects quality of service

developments and integration. The FTAM standard currently has five parts with amendments and addenda. An additional standard describes a performance test suite. The pertinent FTAM standards are:

- ISO 8571-1, Part 1: *General Introduction*
  - AM 1 Amendment 1: *Filestore Management*
  - DAM 2 Amendment 2: *Overlapped Access*
  - PDAM 3 Amendment 3: *Service Enhancement*
  - WDAM 4 Amendment 4: *Security Enhancement*
- ISO 8571-2, Part 2: *Virtual Filestore Definition*
  - AM 1 Amendment 1: *Filestore Management*
  - DAM 2 Amendment 2: *Overlapped Access*
  - PDAM 3 Amendment 3: *Service Enhancement*
  - WDAM 4 Amendment 4: *Security Enhancement*
- ISO 8571-3, Part 3: *File Service Definition*
  - AM 1 Amendment 1: *Filestore Management*
  - DAM 2 Amendment 2: *Overlapped Access*
  - PDAM 3 Amendment 3: *Service Enhancement*
  - WDAM 4 Amendment 4: *Security Enhancement*
- ISO 8571-4, Part 4: *File Protocol Specification*
  - AM 1 Amendment 1: *Filestore Management*
  - DAM 2 Amendment 2: *Overlapped Access*
  - PDAM 3 Amendment 3: *Service Enhancement*
  - WDAM 4 Amendment 4: *Security Enhancement*
- ISO 8571-5, Part 5: *PICS Proforma* (awaiting publication)
  - WDAM 1 Amendment 1: *Filestore Management*
  - WDAM 2 Amendment 2: *Overlapped Access*
  - WDAM 3 Amendment 3: *Service Enhancement*
  - WDAM 4 Amendment 4: *Security Enhancement*
- *Conformance Test Suite for the* FTAM *Protocol*
  - ISO 10170-1, Part 1: *Test Suite Structure and Test Purposes,* November 1990 (IS text was expected October 1991)
  - WD 10170-2, Part 2: FTAM *Abstract Test Suite* (CD expected October 1992)
  - WD 10170-3, Part 3: ACSE *Abstract Test Suite Embedded Under* FTAM (CD expected June 1993)
  - WD 10170-4, Part 4: *Presentation Abstract Test Suite Embedded Under* FTAM (CD expected June 1993)
  - WD 10170-5, Part 5: *Session Abstract Test Suite Embedded Under* FTAM (CD expected June 1993).

The current FTAM standard treats a filestore as an unstructured collection of files. Amendment 1 defines a structured filestore to allow the organization and manipulation of individual groups of files. Addendum 2 on Overlapped Access allows more efficient access to contents of a structured file. The Overlapped Access working draft specification uses the formal description language LOTOS. These extensions will support needs of the

Network File Store, but harmonization with DTAM (CCITT) and DFR (SC18) will be needed. PICS proformas such as ISO 8571-5 provide a framework for specifying compliance with all the interoperability parameters for the implementation of a protocol; this concept is discussed in Section 9.4.1.

In order to cope with the wide range of possible file mechanisms, FTAM uses a virtual filestore model. In FTAM's virtual filestore model, files are structured. Each file has a set of attributes (e.g., owner information and contents type), in addition to the data association with the file. The contents type of the file defines the file structure. Currently FTAM is not easily exportable to other application services. The new work will attempt to improve efficiency by reducing the number of confirmed requests (e.g., needed for file transfer over long-haul communications), extend and simplify FTAM services to allow other applications services (e.g, TP) to easily use FTAM services (e.g., for data transfer) with minimum overhead by providing high-level services, and to provide file services for other user services, such as CCITT telematic services.

As a consequence of the proliferation of FTAM implementations over the past few years, the document types included in the base standard are not sufficient for the wide variety of applications served by FTAM. For example, new document types for CGM, EDI, and COBOL have been submitted to the FTAM Group for comment and review. The FTAM group believes that ISO should set up an International Document Type Registry where the already defined document types can be held and publicized. Moreover, ISO should set up a mechanism to manage the document types that involve those ISO Groups. [Ref. SC21 N 6229 1991]

In addition, some existing document types include optional facilities that have led to interoperability problems. It was therefore proposed in June 1991 that document type definitions include a statement of conformance requirements. This information could be included as Annex F to ISO 8571-2 or as a Tutorial Addendum on Interoperability in ISO 8571. [Ref. SC21 N 6230 1991]

SC21/WG5 is developing a document type to enable FTAM to transfer CGM files as a structured file rather than (with current FTAM) as a transparent sequence of octets. The new work would provide access to the whole metafile, to the metafile descriptor, or to the individual pictures with an associated metafile descriptor. All three CGM encoding techniques would be supported: binary, clear text, and character text [Ref. SC 21 N 4192 1989]. The FTAM Rapporteur Group reviewed the latest version of the CGM document type in May 1991, found it technically satisfactory, and recommended that it be registered following the *Procedures for the Registration of Document Types* (ISO 9834, Part 2). [Ref. SC21 N 6225 1991]

In May 1991, SC21 WG5 proposed an EDIFACT/FTAM Document Type (see also Section 9.1.4) in an attempt to merge existing FTAM implementations with existing EDI systems with a minimum of change [Ref. SC21 N 6224 1991]. PDAM 3, *Service*

Enhancement to ISO 8571-2, FTAM *Virtual Filestore Definition,* which is currently undergoing letter ballot, would add the CGM and EDIFACT document types.

In August 1991, a new work item (NWI) on the *Definition of a New* FTAM *Document Type for Directory* was proposed to define an FTAM document type that represents Directory information, which would be used when FTAM is transferring Directory information. The document type could be documented as a new part of the Directory standard, as an amendment providing a new normative annex to an existing part, or as part of an existing external international register. [Ref. SC21 N 6007 1991]

EWOS is developing a Remote Actions (RA) service and protocol for use with FTAM to support the ability to perform a remote action upon completion of a file operation. Examples of a remote action would be execution of a batch job that is transferred to another system via FTAM and to spool a print file to a printer after being transferred using FTAM. Both RPC and JTM could provide this support, but JTM is viewed in EWOS as too complex for simple remote actions. RA would not compete with JTM and specifically would not support such JTM services as gathering information for input to a job, spawning jobs to several systems, manipulating entries in job queues (e.g., kill a job), monitoring progress of jobs, or preparing progress reports [Ref. EWOS 1990].

The FTAM standards include an annex, *Commitment Control with File Transfer,* which defines a specific example of how FTAM could be used with CCR. This was originally developed when CCR was at DIS status. In response to an earlier defect, this annex was suspended until CCR restabilized. Following the publication of CCR, an input document was drafted to replace the old annex. During the process of drafting the annex, it became apparent that while FTAM can recover from an application or communication failure during data transfer, CCR treats a failure before the end of Phase I as a (presumed) rollback. This relation between FTAM recovery and CCR recovery requires careful examination. [Ref. SC21 N 6228 1991]

The Joint European Standards Institution (CEN/CENELEC) has issued four European Standards (ENVs):

- ENV 41 204, FTAM - *Simple File Transfer*, September 1989
- ENV 41 205, FTAM - *File Management,* June 1989
- ENV 41 206, FTAM - *Positional File Transfer,* June 1989
- ENV 41 207, *FTAM- Positional File Access,* June 1989.

6.3.3.2 FTAM Options and Profiles

Protocols and services for FTAM are specified in ISO 8571. The ISO standard (ISO 8571-2, Annex B) provides for three document types: unstructured text, sequential text, and unstructured binary. NAOIW Stable Implementor's Workshop agreements have been published by NIST for four others: sequential file, random access file, indexed file, and file directory file. Six implementation profiles have been defined by the European

Standards Promotion and Application Group (SPAG), which have the following corresponding profiles from the NIST OSI Implementor's Workshops:

- *Simple file transfer* (SPAG A/111, NIST T1, ENV 41 204)
- *Positional file transfer* (SPAG A/112, NIST T2), ENV 41 206)
- *Full file transfer* (SPAG A/113, NIST T3)
- *Simple file access* (SPAG A/122, NIST A1)
- *Full file access* (SPAG A/123, NIST A2)
- *Management* (SPAG A/13, NIST M1).

An International Standardized Profile (ISP) is being developed by the JTC1 Special Group on Functional Standardization (SGFS) for FTAM. There are currently six parts and one addendum:

- ISP 10607-1, AFT nn - *File Transfer, Access, and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM*, 17 January 1991 [SGFS N 282] (submitted by SPAG) ISP accepted December 1990.
- ISP 10607-2, AFT nn - *File Transfer, Access, and Management - Part 2: Definition of Document Types, Constraint Sets and Syntaxes*, 17 January 1991 [SGFS N 285] (submitted by SPAG) ISP accepted December 1990.
- ISP 10607-2 AD 1, *Addendum 1: Additional Definitions*, Approved 27 May 1991 [SGFS N 363].
- ISP 10607-3, AFT nn - *File Transfer, Access, and Management - Part 3: AFT 11 - Simple File Transfer Service* (Unstructured), 17 January 1991 [SGFS N 286] (submitted by SPAG) ISP accepted December 1990.
- ISP 10607-4, AFT 12 - *File Transfer, Access, and Management - Part 4: AFT 12 - Positional File Transfer Service (Flat)*, approved 27 May 1991, SGFS 360.
- ISP 10607-5, AFT 22 - *File Transfer, Access, and Management - Part 5: AFT 22 - Positional File Access Service (Flat)*, approved 27 May 1991, SGFS 361.
- ISP 10607-6, AFT 3 - *File Transfer, Access, and Management - Part 6: AFT3 - File Management Service*, approved 27 May 1991, SGFS 362.

6.3.4 Directory

CCITT is developing a database application standard for logically storing directory information. The Directory is a distributed database on users, processes, and other objects, used to provide access to information that people or processes require prior to communicating. The standards are in the following X.500 Series recommendations: X.500, X.501, X.509, X.511, X.518, X.519, X.520, and X.521.

6.3.4.1 Directory Services and Models

The Directory services provide a specialized hierarchical database, called the Directory Information Tree (DIT), for OSI applications. The Directory contains

information about objects and provides structured mechanisms for accessing that information. These services are intended to provide user friendly naming to permit a user to specify an object's name and then retrieve additional addressing information. The two key aspects of the OSI Directory, which distinguish it from other database and name-server work, are [Ref. OSN 1990d]:

- The Directory can be read, modified, and searched remotely via OSI protocols.
- A highly distributed database is provided by Directory System Agents (DSAs).

The following four models define the Directory services:

- The informational model describes the Directory Information Base (DIB). The DIB contains all the information to which the Directory provides access. This model is concerned only with the logical structuring of the information.
- The functional model describes interactions that take place between the various DSAs that comprise the Dictionary.
- The organizational model describes how portions of the Directory tree map onto the DSAs. This includes issues of replication and access control.
- The security model of Directory services describes the service in terms of authentication and authorization. ISO 9594-8, *OSI Directory Authentication Framework*, has now been transferred to SC21/WG1 (Security).

6.3.4.2 Directory Standards

SC21/WG4 is working on OSI directories. ISO standards for the Directory are:

- ISO 9594-1, *Overview of Concepts, Models and Services*, December 1990 [SC21 N 4701] (CCITT X.500)
  - PDAM 1.2, *Replication, Schema and Access Control* [SC21 N 5942, 15 May 1991]
- ISO 9594-2, *Models*, December 1990 [SC21 N 4702] (CCITT X.501)
  - PDAM 1.3, *Access Control* [SC21 N 5952, 16 May 1991]
  - PDAM 2.2, *Schema Extensions* [SC21 N 5952, 16 May 1991]
  - PDAM 3.2, *Replication* [SC21 N 5944, 16 May 1991]
- ISO 9594-3, *Abstract Service Definition*, December 1990 [SC21 N 4703] (CCITT X.511)
  - PDAM 1.3, *Access Control* [SC21 N 5953, 16 May 1991]
  - PDAM 2.2, *Replication, Schema and Enhanced Search* [SC21 N 5945, 16 May 1991]
- ISO 9594-4, *Procedures for Distributed Operations*, December 1990 [SC21 N 4704] (CCITT X.518)
  - PDAM 1.3 *Access Control* [SC21 N 5954, 16 May 1991]
  - PDAM 2.2: *Replication, Schema and Enhanced Search* [SC21 N 5946, 17 May 1991]
- ISO 9594-5, *Protocol Specifications*, December 1990 [SC21 N 4705] (CCITT X.519)

- PDAM 1.2 *Replication* [SC21 N 5947, 17 May 1991]

- ISO 9594-6, *Selected Attribute Types*, December 1990 [SC21 N 4706] (CCITT X.520)
  - PDAM 1.2 *Schema Extensions* [SC21 N 5948, 16 May 1991]
- ISO 9594-7, *Selected Object Classes*, December 1990 [SC21 N 4707] (CCITT X.521)
  - PDAM 1.2 *Schema Extensions* [SC21 N 5949, 16 May 1991]
- ISO 9594-8, *Authentication Framework*, December 1990 [SC21 N 4708] (CCITT X.509)
  - PDAM 1.2 *Access Control* [SC21 N 5955, 16 May 1991]
  - WDAM on Security Enhancement to Directory [SC21 N 6172]; PDAM expected December 1992 (see also Section 8.2.2.7).

During the ISO/CCITT collaborative editing meeting held in Berlin from 21 October 1991 to 1 November 1991, the National Body and Liaison Organization CD and PDAM ballot comments were resolved, and the National Bodies present recommended progression of the CD and the twelve PDAMs to DIS status. It is also reported that the NAOIW is expected to publish Stable Workshop Agreements based on these enhancements and that vendors are willing to develop conformant products (International Computers Limited (ICL), DEC, Hewlett-Packard, Retix, and Siemens Nixdorf). [Ref. Messeh 1991]

The following standards are under development by ISO:

- CD 9594-9.2, *Replication* [SC21 N 5951, 14 May 1991]
- WD 9594-10, *Directory PICS Proforma*, July 1989 [SC21 N 4039] (CD text expected in June 1992, DIS text in June 1993, and IS text in June 1994)
- WD 9594-X, *Text Suite Structure and Test Purposes and Abstract Test Suite for the OSI Directory*, August 1990 [SC21 N 4951] (NWI not accepted)
- WD 9594-Y, *Replication and Knowledge Management*, July 1990 [SC21 N 4913] (CD text expected June 1992).

The CCITT Directory Defect Resolution Committee has produced a *Directory Implementor's Guide* [SC21 N 6314, July 1991], which is a compilation of reported defects in the 1988 CCITT X.500 Recommendations (ISO 9594) standards and their resolutions. It is a CCITT record of defects, not a formal ISO record of Directory defects, intended to be an authoritative source of information for implementors to read in conjunction with the Recommendations/Standards themselves. The Guide is in its fifth version and provides guidance to implementors on how they may submit defects as well as insight into the procedures by which their reported defects will be processed. [Ref. SC21 N 6012 1991]

6.3.4.3 Enhancement to Directory Standards

CCITT SGVIII and SC21/WG4 are collaborating on enhancements to the Directory (CD 9594-9.2 and twelve PDAMs are listed above). Two areas being addressed are the

Extended Information Model and Extended Search. The Extended Information Model work covers the generic way in which information is viewed in the Directory, from the viewpoint of both users and system administrators. The Extended Search work covers how extensions to the current searching mechanisms might be provided to offer a better service to the users of the Directory [Ref. IST/21: 2041 1990].

Extensions have been proposed to the DIT Structure Rule used to control the positioning of entries in the DIT based on the values of the Object Class attributes. The extensions would allow the subschema administrator to specify, within the portions of the DIB to which the subschema is applicable, criteria that allow the existence of entries based not only on the Object Class attributes of child entries and their parent entries, but also on the Object Class attributes of their other ancestor entries [Ref. SC21 N 4804 1990].

The concept of extensible matching rules is being developed in CCITT SG VII and SC21/WG4 for use in Directory and Enhanced Search. Capabilities such as approximate matching, diacritics-ignore matching, regular expressions, and word-sensitive searching are supported [Ref. SC21 N 4623 1990].

Work on a replication abstract service for the Directory is based on MHS abstract service definition conventions (ISO 10021-3). An underlying assumption is that the replication abstract service will be realized by means of ASEs. Data transfer systems, external to the DSA, may be needed to carry shadow updates. Replication operations are Request Shadow, Request Update, Refresh Shadow, and Terminate Shadow [Ref. SC21 N 4806 1990].

EDI users have requirements for use of Directory in which the naming structure would not necessarily be country oriented but would enable the current trading practices that use certain trading partner names [Ref. SC21 N 4799 1990].

CCITT and SC21 are considering the following features and facilities for joint work on Directory [Ref. SC21 N 4801 1990]:

- Inverted directories for Telex and Teletex services
- Additional information with or after the result of a query
- Query cost information
- Information about services, service instructions, tariffs, etc., in standardized formats, taking into account additional attributes
- Additional service controls
- Full functionality of access control mechanisms
- Ability of the user to indicate the desire not to receive partial results when service control maximum parameters are exceeded
- Return of multiple responses in groups of any specified number
- Administrative procedures for authentication
- Standardized error service messages

- Shadowing (controlled replication) of Directory information
- Geographical extension
- Consequences of distributed Directory services.

In October 1990, the United States offered a working document [SC21 N 5351] on Time Stamps for consideration by the collaborative meeting of CCITT and SC21/WG4 in Ottawa. It contends that time stamps are likely to be useful in the administration of directory user information, knowledge information, and replication information. With respect to time stamps in the Directory Information Model, it suggests two modifications: (1) to include (optionally) the identity of the principal responsible for the last modification of an entry and (2) to correct the redundancy that has occurred in the working documentation: the entry time stamp is documented in both the schema and the replication document in slightly different ways. Moreover, knowledge attributes may be multi-valued and time stamp information for each value is likely to be of interest. Therefore, in order to time stamp knowledge information, the definition of knowledge itself must be modified. The document suggests how to do this. Finally, it suggests that there are two forms of replication in the directory replication model--caching and shadowing--and that each form should have its own form of time stamp.

A number of standards in Distributed Office Applications (DOA) (see Section 9.1.3) make use of the filter concept defined in ISO 9594-2 that permits target objects of an abstract operation to be selected on the basis of their attribute values. The current definition suffers from a number of problems that prevent it from answering many of the requirements of DOA. A liaison statement [SC21 N 5561] describes these problems. [Ref. SC21 N 5561 1990]

In May 1991, SC21/WG4 requested a NWI on the *Use of Systems Management for Administration of the Directory* [SC21 N 6006]. The scope of this NWI would be to define a set of Managed Objects to support Directory operational information (i.e., that information that the Directory uses to guide its own operations). This operational information would be accessible through the CMIS and CMIP. The NWI may either be documented as a new part of the Directory standard or as amendments providing new normative annexes to the existing parts. An initial document was provided with the NWI request. Proposed dates are WD in June 1992, PDAM or CD in November 1992, DIS in June 1993, and IS status in June 1994. [Ref. SC21 N 6006 1991]

Another new work item proposal is for an FTAM document type for Directory [SC21 N 6007]. It is as yet undecided whether this should be part of ISO 9594, an amendment to an existing part, or part of an external international register.

WG4 proposed the following question on Directory schema migration in May 1991 [Ref. SC21 N 6008 1991]: "How does one extend or modify the Directory schema allowing the use of new representations or relations, while insuring that less up to date Directory User Agents (DUAs) can manipulate the information using older schema

definitions?" The question was approved in December 1991 and work will begin in May 1992 [SC21 N 6612, 6 December 1991].

Another Directory-related question that WG4 posed in May 1991 was [Ref. SC21 N 6008 1991]: "Should ISO 9594 be changed to allow two or more entries in different DSAs referring to the same real-world object to share the same name?"

A June 1991 WG4 *Liaison Statement to SC21 on Directory's Use of ISO 9066 (ROSE)* [SC21 N 6002] addresses the need to provide recovery procedures in the Directory Shadowing Protocol, which potentially involves the transfer of very large amounts of data between Directory systems.

The EWOS Directory Expert Group (EGDIR) has issued a *Working Document on Behaviour of DSAs for Distributed Operations* [SC21 N 5826]. In the Distributed Directory, one mode of interaction is the chaining (including multicasting) of enquiries in accordance with the procedures laid down in ISO 9594-4. Another is the following of referrals and of embedded continuation references. While the procedures are comprehensively defined in these documents, a number of options and issues arise for which little or no guidance is provided. The objective of this document is to lay down requirements where appropriate and provide guidance and recommendations to be used by DSAs when they carry out these procedures, in addition to the requirements and guidance provided by ISO 9594-4.

The Directory group is concerned about the differences between the proposed Distinguished Encoding Rules (DER) (see Section 6.3.7.2) in CD 8825-3 [SC21 N 6296] and the provisions in the existing Directory standard. In particular, the two documents specify mutually incompatible encodings for all constructed types, since they specify different length forms, and for string types, since the DER requires the constructed form for strings longer than 1000 octets. The Directory group requests that the editing meeting for CD 8825-3 consider aligning with the Directory Authentication Framework in critical respects in order to permit Directory to recommend use of the DER for its intended purposes. [Ref. SC21 N 6532 1991]

6.3.4.4 Example Interoperability Parameters for Directory

Two international groups are working on functional standards (profiles) for the Directory. The issues being addressed by the NAOIW Directory Services SIG and the EWOS/ETSI Directory Expert Group indicate options within the Directory standard and areas where baseline standards may be exceeded to address practical implementation problems. Examples of the issues and options are [Ref. IST/21: 1868 1989]:

- Classification of minimum schema capabilities.
- Classification of baseline structure rules--mandates the capability to access a standard Directory tree (which may be extended to a wide variety of entries).

- Definition of maximum APDU size--eases design of high-performance DSAs (e.g., to ensure the Directory can respond in seconds) and eases network problems in providing quality of service.
- Pragmatic constraints on filters--protects the Directory from pathological conditions and potentially simplifies design.
- Holes in distributed operation definitions--there are many undefined aspects for distributed operations (e.g., how to handle errors).
- Constraints on alphabets--Directory uses T.61 strings. Directory profiles are addressing rejection of strings that contain non-T.61 characters and restrictions on permissible characters (e.g., escape characters).
- Constraints on integer values--defines a minimum size integer that must be supported.
- Classification of authentication--mandate use of simple uncorroborated authentication that supports external authentication within a closed domain.
- Augmentation of attribute syntax rules--augments the standards material with practical rules.
- ASN.1 rules--mandates support of ASN.1 identifier tags that are three octets in length (and no longer) and requires constructed string elements not to be nested more than one deep.
- Strong authentication algorithms--proposing alternatives to the use of RSA™ (a licensed product) for digital signatures.

6.3.5 Job Transfer and Manipulation (JTM)

JTM (ISO 8831 and 8832) was originally designed for remote off-line (batch) processing. It uses a processing model based on movement of entities called "documents" and the exchange of these entities with users. Exchanges are specified in work specifications that include a data structure and an envelope carrying the document. In Basic Class JTM a single document can be sent to a processing element. In Full JTM (ISO 8832/AM1, Full Class Protocol) multiple documents and multiple processing steps are permitted.[20] Capabilities of JTM are being included in standards for FTAM (e.g., RA) and the ASEs (e.g., RPC) [Ref. SC21 N 4356 1990].

The United States stated in ISO in March 1990 that there are no U.S. user requirements nor any organization in the United States willing to provide resources for JTM standards [Ref. SC21 N 4641 1990]. AFNOR has similarly found little interest in industry for JTM and recommended further work be suspended [Ref. SC21 N 4603 1990]. Nevertheless, the reassessment report for JTM Full Class [SC21 N 4679 Revised] recommended completion of the International Standard texts, given the advanced state of

---

[20] ISO 8832/AM 1, *Extension to Specification of the Full Protocol*, approved 12 June 1991; IS text expected November 1991 [SC21 N 6272]. Merged text of ISO 8832 1989 with revised text of AM1 is provided in SC21 N 5225 dated 28 May 1990.

the work. The recommendation was approved by SC21 in June 1990 [Ref. IST/21: 2160 1990].

The second edition of JTM (DIS 8831) was published in December 1991. SC21 also agreed in June 1990 to prepare a formal tutorial/usage guide that includes JTM scenarios and shows how JTM fits with other ASEs [SC21 N 4679].

6.3.6 Application Service Elements

The services performed in the Application Layer of the OSI model can be thought of as application processes whose communication aspects are represented by application entities. The OSI Application Layer structure permits an application process to have multiple communication aspects and, hence, multiple application entities.

An application entity is a collection of one or more ASEs. Each of the peer application entities have identical ASEs. Additionally, each ASE talks only with its peer in the remote application entity. The remainder of this section discusses the ASEs:

- Association Control Service Element (ACSE), which provides association control and manages connections between application entities
- Commitment, Concurrency, and Recovery (CCR), which provides fault tolerance and manages error indication and recovery
- Reliable Transfer Service Element (RTSE), which manages bulk data transfers
- Remote Operations Service Element (ROSE), which manages request/reply interactions
- Remote Call Procedure (RPC).

A typical application process might have a user element orchestrating the application entities' actions. This user element could use RTSE services to manage associations via ACSE services and could use the ROSE, which invokes RTSE services, to transfer data through the use of the presentation service.

6.3.6.1 Association Control Service Element (ACSE)

The ACSE provides service to both user elements and to specific application service elements. The purpose of this service is to support the establishment, maintenance, and termination of application associations. Because the ACSE manages the association of application entities, all OSI applications contain an ACSE. The services provided by ACSE are:

- ASSOCIATE, which sets up an application association
- RELEASE, which releases an association in an orderly fashion
- ABORT, which terminates application association simultaneously with the underlying presentation and session connections.

The ISO definition of the service is technically aligned with the 1988 CCITT recommendation on the ACSE service. The differences between the ISO definition and the

CCITT definition are quite small and are not expected to affect interoperability between implementations written against either document [Ref. Rose 1990]. There are five relevant ISO standards:

- ISO 8649, *Service Definition for the Association Control Service Element (ACSE)*
- ISO 8650, *Protocol Specification for the Association Control Service Element (ACSE)*
- DIS 8650-2, *ACSE, Part 2: PICS Proforma* (Document will not be balloted until session PICS is at DIS Status)
- ISO 10035, *Connectionless* ACSE *Protocol Specification*
- ISO 10169-1, *Conformance Test Suite for the* ACSE *Protocol, Part 1: Test Suite Structure and Test Purposes* , 24 September 1991 [SC21 N 6421].

In addition, ISO 8650 and 8649 have two draft addenda: *Authentication* and *Connectionless* ACSE *Service*. A third, *A-Context Management Service*, is expected to reach PDAM status in June 1993. WD 10035-2 is the *PICS Proforma for Connectionless* ACSE *Protocol*.

A discussion paper [SC21 N 5835] on association pools as an extension of ACSE appeared in April 1991.

6.3.6.2 Commitment, Concurrency, and Recovery (CCR)

The CCR service and protocol standards are used to supply a more fault tolerant association than is possible with ACSE. The ACSE has two basic flaws [Ref. Stallings 1987]:

- A system crash leaves ambiguous results.
- A lack of coordination of multiple systems could produce inconsistent results.

These flaws are resolved in CCR by adding the concept of commitment. The master asks the subordinate for a commitment to perform a task (request) before the call for the execution of the task (commitment) is made. This allows for a record to be kept by both the master and the subordinate as to the status of the task. Use of CCR can have an adverse performance impact.

Concurrency is a concept that is necessitated by the concept of commitment. Once an application entity has offered to commit, conflicting requests cannot be made against the application until the commitment is fulfilled. Concurrency is the mechanism by which committed resources are "frozen" until the committed application is completed.

Recovery is the process of determining the status of a task after an application or communication failure. The CCR service provides partial support for recovery; however, the actual recovery process is specific to the application.

There are three standards relating to CCR:

- ISO 9804, *Service Definition for the Commitment, Concurrency, and Recovery Service Element*
- ISO 9805, *Protocol Specification for the Commitment, Concurrency, and Recovery Service Element*
- CD 9805-2.2, *CCR, Part 2: PICS Proforma*, August 1991 [SC21 N 6332].

ISO 9804 and ISO 9805 have three draft addenda: *Enhancements, Session Mapping Changes,* and *Restart.*

In January 1990, a CCR *Conformance Test Suite* was proposed as a new work item [SC21 N 4279]. CD status is expected in June 1992. Another new work item [SC21 N 6126] has been accepted to write a formal description of the CCR service and protocol using LOTOS. PDTR text is expected May 1992, DTR June 1993, and TR June 1994.

6.3.6.3 Reliable Transfer Service Element (RTSE)

RTSE provides a service of reliably moving arbitrarily large objects from one application entity to another. The RTSE accomplishes this service by dealing with ASN.1 data types rather than a string of octets and by abstracting the complexity of the underlying service session into an easily usable service.

When an application context contains an RTSE, it is the sole user of ACSE services and the presentation service. The RTSE is used to signal to application elements that a transfer has been completed successfully. The ISO standard for RTSE comes in two parts:

- ISO 9066-1, *Reliable Transfer,* Part 1: *Model and Service Definition*
- ISO 9066-2, *Reliable Transfer,* Part 2: *Protocol Specification.*

Since RTSE was developed in the early MHS work that preceded the definition of the presentation service and ULA, it demands syntax conversions be done in the Application Layer (rather than in the Presentation Layer as specified by the ULA). Thus, RTSE does not fit well with the OSI ULA. [Ref. SC21 N 5997 1991]

6.3.6.4 Remote Operations Service Element (ROSE)

Remote operations are a popular technique for building distributed applications. The ROSE manages operations for application entities via a mechanism that is analogous to services performed by CCR for data transfer. In its most primitive form, an operation is a simple request/reply interaction. The request, or invocation, consists of:

- An operation number--a unique identifier for the operation to be performed
- An arbitrarily complex argument--the "input" for the operation
- An invocation identifier--a unique identifier for a particular invocation
- A linked invocation identifier--an indication that this operation is being invoked as a part of the processing of another invocation.

An invocation can have one of three outcomes:

- A result--an invocation identifier corresponding to the operation that succeeded and an arbitrarily complex result
- An error--an invocation identifier corresponding to the operation that failed, an error number uniquely identifying the error that occurred, and an arbitrarily complex parameter that provides clarifying information
- A rejection--an invocation identifier corresponding to the operation that was performed and a reason that describes the rejection that occurred.

The standards that apply to the ROSE are:

- ISO 9072-1, *Remote Operations,* Part 1: *Model, Notation, and Service Definition*
- ISO 9072-2, *Remote Operations,* Part 2: *Protocol Specification.*

ROSE is a set of communications facilities to distributed applications. ROSE was derived from the Remote Operations (RO) service defined in CCITT MHS-84. The standard (ISO 9072) also provides a notation for defining them (an extension of ASN.1). Remote operations service is asynchronous, so a client need not wait for a response before invoking another operation. ISO 9072 defines the structure of remote operations and the abstract services and protocol to support them. The services are generic in that their effect on the remote object is defined by their users.

The basic interaction with a remote object is an operation that is similar to a procedure call in a programming language. An operation is invoked on a target object, to which the operation argument is passed. Operations have one of two possible structures, and invocations have two possible outcomes. Some operations return either a Result, when they are executed successfully, or an Error; other operations produce only a response (Error) if the operation fails.

In July 1991, a new work item [SC21 N 6151], *Enhancements to ROSE Service Definition, Protocol Specification, and Concepts, Model and Notations,* was proposed to amend the ROSE standards to (1) include the use of new ASN.1 constructs as an alternative to the deprecated ASN.1 MACRO notation and (2) produce a new part of the ROSE standard to cover concepts, model, and notation. The Untied States voted "No" on this NWI because the proposed base documents exceed the proposed scope of the NWI by adding new functionality to ROSE; however, the new work item was approved and PDAM status was expected by the end of 1991. [Ref. ANSI 1991a]

6.3.6.5 Remote Procedure Call (RPC)

The ECMA standard for RPC is ECMA 127. As defined in ECMA 127, an RPC is a communication service to transfer procedure calls to a remote server and return results, errors, or associated call backs. One of the central notions of RPC is that of a stub. A stub builds protocol information for RPCs (marshalling) and translates protocol information to server procedure calls (unmarshalling). ECMA 127 defines an Interface Definition Notation (IDN) to facilitate the transfer of data across an interface. The IDN supports a

union of programming language-specific data types such as pointers, arrays, and records, and primitive data types such as integers and bit strings. ECMA 127 limits the number of outstanding procedure calls to one per association, in order to prevent livelock situations and preserve fairness; it is unclear if this is the most efficient solution to the livelock problem. SC21/WG6 proposes to address RPC using an IDN that is based on abstract data types rather than on a union of programming language-specific data types.

Text for DIS 10148, *Basic Remote Procedure Call (RPC) Using OSI Remote Operations* [SC21 N 3463], was based on ECMA 127 and submitted in 1989 on a fast-track ballot, which failed.

DIS 10148 was withdrawn, and a September 1989 proposal for a new work item was accepted by JTC1 in May 1990 [Ref. SC21 N 4027 1990]. RPC is now in its third working draft [SC21 N 6111, 25 June 1991] and WG6 has requested authorization to progress the first four parts to CD status. The draft standard, CD 11578, has five parts:

- CD 111578-1, Part 1, *Model*
- CD 111578-2, Part 2, *Interface Definition Notation;* uses data types defined by SC22/WG11 and defines a mapping of these to ASN.1
- CD 111578-3, Part 3, *Service Definition*
- CD 111578-4, Part 4, *Protocol Specification.*
- WD 111578-5, Part 5, *PICS Proforma.*

Some of the work being undertaken in ECMA with respect to RPC includes the following:

- *Position on RPC Modelling* [SC21 N 5816, 28 March 1991]
- *Binding Concepts within RPC* [SC21 N 5817, 28 March 1991]
- *Proposal for RPC Service Definition and Protocol Specification Parts* [SC21 N 5818, 28 March 1991]
- *Modelling Rationale for OSI RPC* [SC21 N 5819, 28 March 1991]
- *Contribution on Computation Model* [SC21 N 5821, 28 March 1991]
- *Proposal for the Use of XALS in the Standardization of RPC* [SC21 N 5822, 28 March 1991]
- Position on RPC Context Handles [SC21 N 5823, 28 March 1991].

ISO work with respect to RPC includes the following:

- *Nature of the OSI RPC Service Boundary and Service Provider* [SC21 N 5586, 7 January 1991]
- *Working Definitions for Client and Server* [SC21 N 5590, 7 January 1991]
- *Call for Comment on OSI RPC IDN* [SC21 N 5588, 7 January 1991].

The aim of the current work in ISO on RPC is to provide a mechanism for writing distributed applications that are both syntactically and semantically similar to a local procedure call.[21] The scope of RPC includes a language-independent IDN for specifying interfaces between components of distributed applications. The RPC protocol for a particular interface definition is derived from the IDN.

RPC is closely related to two projects in SC22: Common Language Independent Data Types (CLID) (ISO 11404) and Common Language Independent Procedure Call Mechanism (CLIP or CLIPCM) (see also Section 8.3.1). SC22/WG11 has agreed that there is no overlap between the CLI projects and RPC. However, there should be cross references between the standards. The CLI projects identified below are giving an abstract definition of data types and procedure call mechanism, while RPC is a concrete definition that extends the procedure calls to the distributed environment [Ref. SC21 N 5583 1991]:

- CLID defines a set of data types, independent of any particular programming language specification or implementation. The set should be rich enough so that all common data types in standard programming languages and service packages can be mapped onto some data type in the set. Hence, the CLID standard is an abstract definition of the set of data types in terms of the values a data type can take and some of the operations that are valid on the data type. The ISO RPC standard will define the set of data types it supports, including the presentation of values of these data types when exchanged in parameters of a remote procedure call.
- The aim of CLIP is to define a generic model for procedure call semantics and therefore is an abstract definition of a procedure call mechanism. ISO RPC aims to extend the semantics of a local procedure call in a distributed environment and, in particular, that RPC be semantically and syntactically similar to a local procedure call.

It is not at all clear whether remote operations (ISO 9072) can be used to satisfy RPC requirements or whether collaborative work with CCITT will be conducted for RPC [Ref. SC21 N 4926 1990]. SC21/WG6 has identified requirements for RPC and IDN [Ref. SC21 N 4928 1990] and has begun coordination of these requirements with SC22/WG11 and CCITT SGVII.

ASN.1 may not be adequate as a basis for the IDN, even if extended for this purpose. Some requirements for the IDN identified in SC21/WG6 are [Ref. SC21 N 4767 1990]:

- Be user friendly in the sense that an applications programmer can translate from the IDN to the programming language of choice in a straightforward, approximately one-to-one manner

---

[21] The ISO approach to RPC could be a problem for Ada. This issue needs to be addressed by the CCIS architecture.

- Be useable to automatically generate language-specific interfaces that support procedure calls using the RPC service
- Be useable to automatically generate the programming language-specific procedure declarations that correspond to the procedures in an IDN for use by a server.

There would appear to be some danger of duplication of effort--and possibly even rival standards--unless RPC is brought together, in some manner, with ROSE [Ref. OSN 1990e]. For example, ROSE has already standardized an IDN, called RO-notation, that uses ASN.1 as a language-independent way of describing the data types of the parameters. ROSE is already used widely, and a program of enhancements to allow it to meet additional needs is underway. However, ROSE is not even mentioned in the new RPC work item proposal.

Two RPC implementations currently exist: Sun RCP and OSF RPC. The two are not mutually exclusive and the key issue for the user is agreement on the application program interface so the user does not have to worry about differences in various RPCs. This requires a standardized interface definition language such as the Network Interface Definition Language (NIDL), which was developed by Apollo and is being enhanced by Digital and is the basis of an ANSI recommendation to ISO [Ref. OSN 1990g].

6.3.7 Abstract Syntax and Basic Encoding Rules

6.3.7.1 Abstract Syntax Notation One (ASN.1)

At present, ASN.1 is the only abstract syntax language that exists in OSI. Abstract syntax languages describe data types in a machine-independent manner, thus freeing data representation from machine restrictions. For example, a protocol specifying that a data type is an integer need not concern itself with the number of bits required for the internal machine-dependent representation of this data type.

ASN.1 has a rich syntax for describing data types and provides a macro facility for extending its grammar. According to Rose [Ref. Rose 1990],

> ASN.1 is destined to become the network programming language of the 90s, just as the C programming language is largely seen as having been the systems programming language of the 80s.

The pertinent specifications for ASN.1 are ISO 8824, ISO 8824/DAD1 (incorporated into ISO 8824), ISO 8824/WDAM 2, and recommendation X.208 from CCITT. The ISO specifications are compatible with those of CCITT, but include a few extensions [Ref. Stallings 1987].

A revised ASN.1 standard will make the current ISO 8824 into Part 1 of a four-part standard arranged as follows:

- Part 1: *Basic Notation* [SC21 N 6294, 8 July 1991].

- Part 2: *Information Object Specification* [SC21 N 6289, 8 July 1991] - provides notation that allows information object classes as well as individual information objects and sets thereof to be defined and given reference names.
- Part 3: *Constraint Specification* [SC21 N 6290, 8 July 1991] - describes how the notation can be defined that further constrains the values that can appear in the notation of Parts 1 and 2, which define a structured data type to convey their semantics.
- Part 4: *Parameterisation of* ASN.1 *Specifications* [SC21 N 6291, 8 July 1991] - describes how specifications may leave certain aspects (e.g., bounds) undefined at the time of abstract syntax definition, being completed by the specification of ISPs for functional profiles from some other body. The requirements not met by Parts 2 and 3 are met in Part 4 by the provision for parameterised reference names and parameterised assignments by this part of the ASN.1 specification.

The Framework for the Support of Distributed Applications (DAF), a new activity established by CCITT SG VII to standardize common aspects of distributed applications, has been working for various enhancements to ASN.1. There are presently five working documents for possible extensions to ASN.1 in the 1992 time frame. The areas covered by these documents are [Ref. OSN 1990f]:

- Provide a firmer framework for the specification of table types and functions
- Improve current definitions of character strings
- Provide new encoding rules, Packed Encoding Rules (PER), Confidential Encoding Rules (CER), Light Weight Encoding Rules (LWER), and Distinguished Encoding Rules (DER), to supplement or replace the current Basic Encoding Rules (BER)
- Improve machine processability
- Provide miscellaneous enhancements.

A new standard, ASC X3.208-199x, *Transfer Syntax Description Notation (TSDN)*, is currently out for review by ANSI X3T2. It defines a notation for describing the structures of data volumes, files, records, and fields to facilitate the moving of data files between computer systems. While it provides a generalized syntax for describing the data records, it does not restrict or define their contents. It was originally developed as an internal standard by the Consultative Committee on Space Data Systems (CCSDS) to handle the transmission of space data [Ref. Freeman 1991].

6.3.7.2 Basic Encoding Rules (BER)

The mechanism that translates the abstract representation of data to its physical characteristics, either for machine storage or for transmittal, is called transfer syntax. The transfer syntax in OSI corresponding to the abstract syntax ASN.1 is contained in *Basic Encoding Rules*, ISO 8825. The relevant standards for BER are ISO 8825, ISO

8825/DAD1, ISO 8825/AD2, and CCITT X.209. Again, the ISO and the CCITT specifications are compatible.

Additional sets of encoding rules are being incorporated into ISO/IEC 8825 by making the current standard Part 1 and developing a revised ISO/IEC 8825, *Specification of Encoding Rules for Abstract Syntax Notation One (ASN.1)*, into a multi-part standard as follows:

- Part 1: *Basic Encoding Rules (BER)* [SC21 N 6295, 8 July 1991]
- Part 2: *Packed Encoding Rules (PER)* [SC21 N 6292, 8 July 1991]
- Part 3: *Distinguished Encoding Rules (DER)* [SC21 N 6293, 8 July 1991]
- Part 4: *Light Weight Encoding Rules for* ASN.1 *(LWER)* [SC21 N 6131, 8 July 1991].

Parts 2 and 3 have reached CD status. A working draft, *Generic Transfer Syntax Providing Upper Layers Security*,[22] is being proposed for inclusion as a new part of ISO 8825. The new work item was accepted provisionally by JTC1 with a request that SC21 reevaluate the need for the project, the wording of the scope, and the effort required for progress on the project. Several National Bodies have raised concerns regarding the benefits to be derived from progression of the project [SC21 N 6604, 4 December 1991].

There is a requirement for an upper layer international standard or recommendation to specify a "quality of service" that implies the use of transfer syntaxes they will provide, within the upper layers, a high level of security, including confidentiality and integrity features. This specification defines a generic transfer syntax whose use is negotiated by the presentation protocol or announced in an ASN.1 external. It provides a generic transfer syntax that can be applied to any abstract syntax defined using ASN.1. CD registration is planned for June 1992. [Ref. SC21 N 6130 1991]

The BER use a "TLV" approach to mapping between abstract and physical data: each data type is encoded as a Tag, a Length, and a Value. The tag field corresponds to the label defined by the data type's abstract syntax, the length field normally indicates how many octets are used for the encoding of the value portion of the data type, and, finally, the value of the data type is encoded.

PER achieve a more compact representation than that achieved by the BER. For each value the DER select just one encoding from those allowed by the BER, eliminating all of the sender's options. LWER encode and decode data much faster than the BER.

FIPS 121, *Videotext/Teletext Presentation Level Protocol Syntax*, adopts ANS X3.110-1983 (with the same title) as the specific data syntax to be used at the presentation layer (and some specific semantics for the application layer) for videotext and teletext

---

22 The title given to this document at the May/June 1991 meetings in Arles was *Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression.*

applications. It is based on the American National Standard Code for Information Interchange (ASCII) and its extensions. FIPS 121 provides formats, rules, and procedures for the encoding of alphanumeric text and pictorial information to be used with broadcast television videotext service.

CCITT recommendations F.200, S.60, S.61, S.62, and S.70 define the service, the terminal equipment, character repertoire, control procedures, and supporting transport services for Teletex, CCITT X.430 Recommendation (Red Book 1984) describes the access protocol for Teletex Terminals.

6.3.8 Other Standards

6.3.8.1 U.S. DoD Standards for Internetting Networks

The U.S. military has developed and widely implemented (e.g., in the Defense Data Network) unique Internet protocols for Layers 3 and 4 that are not OSI conformant. These protocols will serve as a costandard for the U.S. DoD until transition to OSI is complete. These protocols are identified since they will be implemented in the transition strategy for tactical data systems to be fielded in the 1990s by the U.S. Army [Ref. Army 1989]. Details are provided in Chapter 17. A connection-oriented transport service (COTS) is provided by the Transmission Control Protocol (TCP), which provides end-to-end reliability, and a connectionless-mode network service is provided by the Internet Protocol (IP). *The IP provides connectivity over diverse network technologies.*

Historically, TCP/IP arose to meet the need for reliable transmission of information over media that did not guarantee reliable, error-free delivery of information (e.g. Ethernet, Packet Radio, and Satellite). The Defense Advanced Research Projects Agency (DARPA) sponsored research into survivable multi-media packet networking in order to improve the only then-existing network, ARPANET. This research resulted in the U.S. DoD sponsored Internet suite of protocols.

TCP/IP corresponds to Layers 3-4 of the OSI model. In terms of network service, the closest comparison is between the connectionless network service (CLNS) and the service offered by the IP. The services offered by the the OSI CO-mode TP4 and the TCP are similar, however, three major differences exist:

(1) The TCP service is stream-oriented, whereas the OSI transport service is packet-oriented.

(2) The TCP service offers a graceful release, whereas the OSI offers this release in the session service.

(3) The TCP has an urgent data facility, whereas the OSI has an expedited data service.

The major emphasis of the Internet suite is on the connection of diverse network technologies (Layers 1-4). In addition, several applications for use in the Internet suite are available (see Appendix H; for a more complete listing see [Ref. Reynolds 1987]):

- Simple Mail Transfer Protocol (SMTP)
- File Transfer Protocol (FTP)
- TELNET
- Domain Name System (DNS).

These services are the analogs of MHS, FTAM, VT, and Directory, respectively. All of the Internet application protocols are rather simple. They offer a basic level of service and have a very narrow scope. The OSI applications are, in general, functionally more capable than the corresponding applications in the Internet suit [Ref. Rose 1990]. In fact, the U.S. Government, as well as manufacturers and users, endorse OSI rules at the upper layers while preserving the established TCP/IP networks for the transport of information [Ref. OSN 1990h]. Observers at the INTEROP 90 Conference and Exhibition held in San Jose, California, in October 1990 noted a shift away from pure TCP/IP topics in contrast to the previous year where strongly divided feelings about the merits of OSI versus TCP/IP were revealed [Ref. OSN 1990g]. Until recently, TCP/IP has been a *de facto* U.K. standard. However, a current IS notice [Ref. CCTA 1991] issued by the U.K. Central Computer and Telecommunications Agency (CCTA) of HM Treasury included an annex entitled, *Towards Open Systems: TCP/IP to OSI Migration,* which provided a Statement of Direction for use by U.K. Government Departments:

> It is an inevitable consequence of the move to utilize open systems standards that U.K. Government departments, in common with other European Public Sector procurement agencies, require the communications and network products that they procure to conform to relevant OSI standards. Departments are therefore advised to make the relevant OSI standards a mandatory condition of a procurement for communications systems where the availability of appropriate standards and products can be confirmed. However, where such availability is questionable, conformance to relevant OSI standards will probably be made a desirable option, but tenders that incorporate OSI standards-based solutions will be viewed as a more acceptable solution in any evaluation of "OSI versus TCP/IP" bids.

The technical body that oversees the development of the Internet suite of protocols is termed the Internet Activity Board (IAB). The IAB is composed of senior researchers, the majority of whom are the designers and original implementors of the Internet suite. Any member of the Internet community can design, document, implement, and test a protocol for use in the Internet suite. The IAB requires that protocols be documented in the Request for Comments (RFCs) series.

There are four RFCs that define the status of documents in the RFC series. The first is the *Assigned Numbers* [Ref. Reynolds 1987], which lists the assigned values used for the parameters in the Internet suite of protocols. The second is *Official Protocols,*

which lists all official protocols. The third is *Gateway Requirements*, which lists all protocols and practices that relate to network nodes. And the fourth is *Host Requirements*, which lists all protocols and practices that relate to host nodes. These RFCs are periodically updated, with the most recent document always taking precedence. A list of current RFCs is provided in Appendix H.

6.3.8.2 Time Synchronization

CCITT SG VII(Q19) has begun work on a time synchronization service (TSS). The work is based on the U.S. DoD RFC-1119, *Network Time Protocol (NTP)*, currently being used by the Internet community (see Section 6.3.8.1). The TSS time standard is based on the Coordinated Universal Time (UTC), determined by the Bureau International de l'Heure (BIH) from astronomical observations provided by the U.S. Naval Observatory and other observatories.[23]

The TSS can be used in distributed systems in several ways: to measure elapsed time, to preserve the order of events, and to coordinate activities of a set of processes. The elements of the TSS model are the following:

- Local clock--an oscillator that, once set with a time value, attempts to maintain a local estimate of global time
- Time user agent (TUA)--the user of the TSS
- Time synchronization agent (TSA)--the provider of the service.

Each TUA interacts with a set of TSAs to obtain information, from this information to determine the best estimate of global time, and to set the local clock to this value. The TUA may adjust the frequency of the local clock to compensate for drift in the hardware. Synchronization of clocks is by continuous distribution of time--TUAs build up information based on samples of a number of servers for the delay characteristics of the communication path between itself and each of the TSAs.

Time is distributed through the system via a hierarchical set of TSAs. Stratum 1 TSAs, at the top of the hierarchy, have local clocks that are set by external means from the most accurate sources available. These means could include radio receivers and such satellite devices as the Global Positioning System. Clocks that have been set by TUAs that have obtained time information directly from Stratum 1 TSAs are said to be at Stratum 2. At each level of the hierarchy, except the top and bottom, each TUA may have an associated TSA that can be used to distribute time information in the local clock to TUAs at the next lower level of the stratum. It is expected that there will be a number of Stratum 1 TSAs, some being provided as public services. Each site using LANs would have two or more Stratum 2 TSAs, and each LAN segment could have two or more Stratum 3 TSAs.

---

[23] Discussion on time synchronization was taken from SC21 N 4565, *Liaison Statement to SC21/WG4/WG7 on Time Synchronization*, CCITT SG VII, March 1990.

Individual end systems might not need to have clocks at much more than Stratum 4 [Ref. SC21 N 4565 1990].

A task force has been set up under ISO/TC184/SC5/WG2 to look at the requirements for a time-critical communications architecture (TCCA) because the network architectures set up so far are primarily intended for general traffic and are not always capable of providing adequate performance and resilience for time-critical communications, especially where time-critical and non-time-critical traffic coexist. In particular in many CIM and control installations there appears to be a requirement for an intermediate network, between general enterprise-wide networks (e.g., MAP) and field-bus-type networks. This intermediate network would carry both bulk data transfers and time-critical messages, and be able to operate over considerable distances and in hostile environments. A liaison between TC184/SC5/WG2 and SC21/WG4, OSI Management [Ref. SC21 N 5602 1991]. ANSI X3.102, *Data Communication Systems and Services User Oriented Performance Parameters*, 1983, Revised 1990, is being used as a basis for the effort. A key requirement of a TCCA is a set of services aligned with ISO/IEC, MMS (see Section 6.3.2.3). One aspect of Time-Critical Communications Systems (TCCS) is Time Synchronization.

6.3.8.3 Integrated Services Digital Network (ISDN)

ISDN is the result of the current evolution of the networks and services available from the various PTTs (Post, Telephone, and Telegraph). The original telephone or telegraph networks (PSTNs, Public Switched Telephone Networks) were based on analog equipment. In recent years, analog equipment has been replaced with digital equipment. This has lead to the replacement of the analog PSTN with the digital IDN (Integrated Digital Network). The IDN incorporates the latest in digital switching and transmission. The extension of the IDN to provide additional user services has resulted in the ISDN.

The ISDN makes an all digital interface available to the network subscriber. This system features a high data or bit rate and digital transmission and switching. Digital switching provides a fast connect or call setup time for voice and data communications. The networks that an ISDN node can connect to include packet based and circuit based networks. The networks can be switched or nonswitched. The ISDN provides a digital interface to the user. This allows the user to "directly" connect digital devices to the network.

The protocols, services, and interfaces to an ISDN network are defined or specified in the CCITT I series recommendations (see end of Appendix E). For example, the CCITT I.430 Recommendation specifies the physical interface to an ISDN network. It describes the bit, octet, and channel synchronization, as well as the D channel and access control. Recommendation CCITT I.440 describes the data link logical connection via the D channel. This includes the ability to transfer a packet via the D channel. The protocol used on the D channel is LAP D. LAP D is based on HDLC. The CCITT Recommendation also

indicates how to establish and clear a call through a circuit switched or packet switched network. CCITT I.440 and CCITT I.441 collectively provide the service and protocol definitions and specifications for an ISDN network.

Recommendations CCITT I.450 and CCITT I.451 describe how to establish a network connection in a circuit or packet switched network. They describe the protocols for the transfer of a data packet or datagram over a connectionless network. They also describe how to perform the same task using a virtual circuit in a connection oriented network. To allow satellite ISDN connection, work has been undertaken to help ensure compatibility between CCITT ISDN recommendations and satellite link parameters [SC21 N 5572, January 1991].

ISDN use varies greatly in Europe from non existence in some countries to thousands of lines in France and Germany. The European Commission has been actively urging European Community members to implement ISDN services so that by 1994 all member countries will offer commercial ISDN. Some progress is being made toward standardized interconnection between different countries' ISDN services. The first phase of the European Telecommunications Standards Institute (ETSI) calls for all countries' ISDN services to be connected by December 1993; however, to date, a standard has not been developed for such interconn .ctions. [Ref. Computerworld 1991]

6.3.8.4 Broadband ISDN

BISDN or B-ISDN refers to Broadband ISDN. Note that ISDN concepts include broadband--the terminology BISDN exists only to focus attention on the broadband aspects of ISDN. The ISDN network can handle audio, video, and data communications. The ISDN or BISDN provides a wide range of services through flexible user-network interfaces over a limited number of connection types. BISDN can include a switched or nonswitched network connection which operates in a circuit or packet mode network.

The BISDN can offer different forms of applications and communications capabilities. The communications and applications could support distribution oriented services and/or interactive services. These services include: conversational, messaging, retrieval services, and distribution services with and without individual presentation control. Conversational services are those services which provide bidirectional (although unidirectional could be included) dialogue communications. These services could include video surveillance, videotelephony, video teleconference, and high speed data communications.

Message services are the "typical" mail functions extended to films or moving pictures, high resolution images, and audio information. These services allow a user to create, edit, process, convert, store, and forward messages. This service allows end users to communicate with each other.

Retrieval services allows an end user to retrieve information from a "central" location or archive site. The information could be film, high resolution image, or audio information. The information is retrieved on demand. The archive site only delivers requested information.

Distribution services can exist with or without individual presentation control. Distribution services without individual presentation control include broadcast services for television. A television viewer can select a channel, but has no control over the presentation. The start and finish of the presentation is under the control of the distribution service. A distribution service with individual presentation control broadcasts in a cyclic manner. Upon user selection, the user receives the presentation from the its beginning.

Some examples of broadband services could include: video telephony, video conference, high definition television, and videotext.

The types of services mentioned can require substantial amounts of network capacity. In addition to the ISDN B, H0, and H1 channels, this service must support the H2 and H4 channels. As with ISDN, all channels are multiples of 64 kbps. The H21 channel is 32,768 kbps and the H22 channel could have a capacity up to 45 Mbps. The H4 channel could have a rate as high as 138.240 Mbps. The broadband user interface will provide ISDN and broadband services. The user interface standard bit rates will be approximately 150 Mbps and 600 Mbps.

6.3.8.5 Asynchronous Transfer Mode (ATM)[24]

The Asynchronous Transfer Mode (ATM) was developed for use with Broadband ISDN, which, as noted above, is based on optical fiber cable and is intended to support transfer of voice, data, and video at rates on the order of 150 Mbps (applications on the order of 600 Mbps are also being considered). ATM is, in effect, a packet-oriented protocol based upon a relatively short, fixed-length frame (called a cell), supporting a hierarchical structure of virtual channels and virtual paths (that contain one or more virtual channels), over multiple physical links. The ATM is a connection-oriented technique that can be used to support both connection-oriented and connectionless services. Signalling (such as call set up and clear) and user information are carried on separate virtual channels. ATM is designed to offer a flexible transfer capability common to all services.

The ATM standard is being developed by CCITT SGXVIII. It is expected to be completed and adopted in the 1992 timeframe and to be in service in the 1994-1996 timeframe. Although ATM assumes an optical fiber physical medium, other media are being considered for ATM use, include satellite.

---

[24] Discussion is based on comments prepared by MITRE for U.S. Army CECOM in August 1990, at the request of the US Representative to TSGCE PG6 (Sal Manno).

ATM involves switching, transmission, and terminal technologies; the switching technique is still being refined and is not yet stable. The ATM network is characterized by the transmission of short packets of fixed length, each of which carries a 5-octet header and a 48-octet user information field. The content of the header is routing information and virtual circuit identification. The virtual circuits are fixed at call set up. The transmission rate of the cells is not uniform and is dependent on the instantaneous bit or cell rate of the terminals. As compared to circuit switching, connections are identified by headers not by time slots. As compared with X.25 packet switching, the packets are constant length to enable simpler protocols, minimum processing requirements, and improved efficiency.

In its analysis of ATM, MITRE has noted the following with regard to military features for ATM [Ref. MITRE 1990]:

- The protocol is flexible and efficient. Since it is designed for a highly reliable physical medium (fiber optic cable), it may be unsuitable for some tactical media. The ATM could operate over a low bandwidth medium. The two major areas that might preclude ATM from use in the tactical environment are:
  - ATM may be inefficient in sending short cells over a medium in which synchronization is difficult, such as combat net radio. Further, the short cell size could require multiple short messages when a more optimal length would be more efficient.
  - The ATM error detection and correction capability may be inadequate. There is an eight-bit cyclic redundancy check for the header and a separate ten-bit cyclic redundancy check for the user information field. Only a single bit for forward error correction capability on the header as well as on the user information is provided.
- There is no provision within ATM for precedence and preemption; however, these features could be achieved at higher layers over ATM.
- ATM would be reasonably efficient for real-time communication, except that messages requiring multiple cells create the extra overhead of additional transmissions and reassembly.
- Nothing in the ATM addresses security or network management. Network management functions are assumed to take place by the layer or system manager, which has interfaces at each sublayer.
- Nothing in the ATM precludes features such as multihomed end-systems or mobile hosts.
- There is no provision for multi-peer data transmission or multicasting.

6.3.8.6 Fiber Distributed Digital Interface (FDDI)

The Fiber Distributed Digital Interface (FDDI) is a 100-Mbps LAN based on a fiber optic token ring protocol. As a standard, FDDI is still under development, but is planned for inclusion in the U.S. GOSIP Version 3. The FDDI standards are:

- ISO 9314 - 1, FDDI, [ANSI X3.148-1988] Part 1: *Physical Layer Protocol,* April 15, 1989

- ISO 9314-2, FDDI, Part 2: *Media Access Control (MAC)*, May 1, 1989, [ANSI X3.139-1986]
- ISO 9314-3, FDDI, Part 3: *Physical Layer Medium Dependent (PMD)*, August 1, 1990 [ANSI X3.166-1989]
- CD 9314-4, FDDI, Part 4: *Single-Mode Fiber/Physical Layer Medium Dependent* [ANSI X3.184-199X]
- CD 9314-5, FDDI, Part 5: *Hybrid Ring Control (FDDI-II)*, 24 May 1990 [ANSI X3.186-199X]
- DP 9314-6, FDDI, Part 6: *Station Management (SMT) Standard* [ASC X359.5 Project 503-D].

ANSI X3T9.5 has proposed a project to define a new family of standards, FDDI Follow-On LAN (FFOL). The general requirements for FFOL include:

- The ability to provide a backbone for multiple FDDI networks
- The ability to provide efficient interconnections to wide area networks (e.g., B-ISDN)
- The ability to support for a wide variety of "integrated" services such as data, graphics, video, and audio
- An initial data rate less than 1.25 Gbps
- A data rate matched to SDH
- The ability to use existing FDDI cable plant, where feasible.

The target date for completion of the basic FFOL standards is December 1995. The estimated life of the FFOL family of standards is 10 to 15 years. In May 1991, ASC X3 announced the approval of six new FFOL projects to be developed by Task Group ANSI X3T9.5:

- FFOL - Physical Medium Dependent (FFOL-PMD)
- FFOL - Physical Layer Protocol (FFOL-PHY)
- FFOL - Service Multiplexer (FFOL-SMUX)
- FFOL - Asynchronous Media Access Control (FFOL-AMAC)
- FFOL - Isochronous Media Access Control (FFOL-IMAC)
- FFOL - Station Management (FFOL-SMT).

Another fiber-based system, the Synchronous Data Hierarchy (SDH), (CCITT G.707, G.708, and G.709) also provides support for communication in the 100- to 600-Mbps range.

6.4 Assessment of Coverage by Standards

MHS-88 provides a number of the military features identified by the U.S. PSSG, and the TSGCE SG9/WG2 (Upper OSI Layers) for a Military Message Handling System (MMHS). Work on a draft STANAG for MMHSthat was based on MHS-84 was completed as an intercept strategy, and analysis is now being performed in TSGCE

SG9/WG2 to identify additional features required for military application of MHS (see Section 15.3.8). Analysis of the relationship of MHS to ACP 129 and Abstract Syntax Notation One (ASN.1) to STANAG 5500 and other message standards is needed. NATO has requirements for media independent data communications protocols (e.g., for Link 1 replacement) that have not yet been developed; these standards could be applicable to the communications services, and more work needs to be done in this area (see Section 15.3.4).

Allied Communications Publication (ACP) 127 is a NATO standard for message handling services. In a comparison of the 65 service elements of ACP 127, a recent analysis [Ref. USPR 1989] has identified 55 as common to MHS-88. An additional five service elements were shown to be related to, but not the same as, those in ACP 127:

- Precedence levels (MHS-88 provides an Importance Indicator)
- Message identification (MHS-88 provides somewhat different features)
- Prosign C (MHS-88 has an obsoleting indication)
- Bell signal (MHS-88 provides a stored message alert)
- Date-time group (MHS-88 has a submission time stamp).

Five services provided in ACP 127 are not supported in MHS-88: financial accountability, service message, network continuity indication, off-line accountability, and tracer action. Version 4 of STAMINA provides MHS-84 services and ACP 127 functionality (see Section 16.2.7).

ISO SC21/WG1 is still refining the OSI Reference Model regarding the specification of the boundaries of Layers 1 and 2. Some of the protocols needed for the communications services may be determined to lie outside the Reference Model. These might include forward error correction coding[25] (several ISO standards provide for error detection) and other mechanisms such as interleaving of bits from a sequence of octets to reduce the impact of the environment on certain transmission media. Protocols for handling requirements of cryptographic devices (e.g., synchronization) and media access may also lie outside the Reference Model. Standardization of these features should, wherever possible, be accomplished with media-independent standards.

Network services can be provided for CCISs using OSI protocols for electronic mail, Directory, file management, and exchange of telematic information and documents. ISO and CCITT have made great strides in the last five years in getting agreements in many areas of OSI and bringing the base standards to mature status. Directory and MHS-88 are two of the major achievements during the past two years. At the present time there are not many high-level services provided by the OSI stacks, but the communications aspects at

25 Whether forward error correction (FEC) is outside of the OSI Reference Model is still a contentious issue in ISO, U.S. PSSG, and NATO. Valid arguments exist for FEC at either layer 1 or layer 2.

lower layers is mature for connection-oriented services and maturing rapidly for connectionless-mode services.

(This page intentionally left blank.)

7. OPERATING SYSTEM INTERFACE SERVICE STANDARDS

7.1 Requirements

Quick Reference	
Topic	Page
Assessment	152
Conformance Testing	149
IEEE P1003	146
POSIX	146
Operating Systems	151

Operating system services allow applications to gain access to system resources in terms of task initiation, management, scheduling, resource allocation, logical and physical device access, interrupt handling, communication, synchronization, accounting, file management, and a range of utilities that assist efficient development, testing, and execution of applications software. Operating system services address kernel services, commands and utilities, system administration and management, and security. An overview of standards for operating system interfaces is given in Table 13.

7.2 Standards for Operating System Services

The key enabler for standardizing operating system services is the use of a robust standard for the operating system *interfaces*. If the interface standard is sufficiently robust (providing a wide range of services), then adherence to the standard can provide the needed functionality without having to be limited on choice of an operating system and thereby an operating environment. Many implementations available today provide the basic operating system interface. Use of options for additional services outside a standard interface could defeat the goal of adopting a standard interface for operating system services, namely ensuring a high degree of applications portability while providing the necessary system services for information exchange and applications.

Table 13. Status Overview of Key Operating System Interface Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
POSIX.1	●	○	●	●	●	●	●
POSIX.2				●			
GNMP	○						
POSIX.6				○			

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

7.2.1 POSIX

The Portable Operating System Interface for Computer Environments (POSIX) is an interface standard for operating systems that is designed to be vendor independent and to promote application portability.

7.2.1.1 POSIX Development

Development of the POSIX standards is through the Institute of Electrical and Electronics Engineers (IEEE) Computer Society's Technical Committee on Operating Systems (TCOS). The TCOS has formed a large number of working groups. These working groups and the POSIX standards being developed are identified by the same label, namely P1003 with an appropriate extension. Of these, only three, IEEE 1003.1, IEEE 1003.3, and IEEE 1003.9 have achieved standards status. The scope and status of the POSIX work in IEEE is provided in Table 14.

Table 14. POSIX Standards Being Developed by the IEEE for Submission to ISO Through ANSI

P1003.0, *POSIX Guide*--accelerates consensus on Open Systems for Applications Portability and provides timely guidance to users on how to develop applications profiles. (Draft 13, September 1991, Draft 15 to be balloted in July 1992)

P1003.1, *POSIX - System Interface* --defines a standard operating system interface and environment to support application portability at the source code level (approved by ANSI in November 1989 and revised September 1990; approved by ISO as ISO 9945-1, December 1990. IEEE 1003.1-1988 approved as FIPS 151-1, March 1990. FIPS 151-2 was to be proposed in November 1991.

P1003.1a *Language Independent Specifications*--to provide a computer-language independent specification that corresponds exactly with IEEE Std 1003.1-1990. (Draft 6, July 1991) (Ballot spring 1992; target completion late 1992)

P1003.1b *System Interface Extensions*--adds functions and provides preparatory work for language-independent specifications. (Draft 5, December 1990) (IEEE balloting planned for summer 1992.)

P1003.2, *Shell and Tools*--defines a standard source-code-level interface to shell services and common utility programs for applications programs. (Draft 11.2 balloted October 1991) (IEEE standard expected 2Q 1992) (Draft 10 was submitted to ISO and balloted as DP 9945-2, but failed. A new draft was requested for registration , but is on hold)

P1003.2a *User Portability Extension*--provides extensions...to support terminal users in a consistent manner across all conforming systems. (Draft 8 balloted October 1991) (IEEE standard expected 2Q of 1992)

P1003.3, *Test Methods: General*--defines general requirements and test methods for test suites to measure conformance of an implementation to IEEE POSIX and related standards; seeks to define what to test rather than how to test and promotes the development of testable standards. (IEEE 1003.3-1991 approved March 21, 1991. ISO standard proposed; international ballot initiation pending)

P1003.3.1, *Test Methods for POSIX.1*--defines test methods and requirements for implementations of test suites to measure conformance of an operating system product to POSIX.1. (Draft 13 balloted December 1991; approval of final text expected in 1Q 1992.)

P1003.3.2, *Test Methods for POSIX.2*--defines test methods and requirements for implementations of test suites to measure conformance of an operating system product to POSIX.2. (Draft 6, July 1991; ballot planned for mid-1992; approval of final text expected early 1993.)

Table 14. (Continued)

P1003.4, *Real-Time Extensions*--defines a real-time extension to POSIX environments. (Draft 11 ballot closes November 1991; approval expected late 1992)

P1003.4a, *Threads*--defines interfaces for handling multiple threads of control within a single POSIX P1003.1 process. (Draft 6 balloted December 1991.)

P1003.4b, *Language-Independent Specifications for P1003.4*--rewrites interfaces defined in P1003.4 and P1003.4a into a language-independent binding. (Draft 3, June 1990)

P1003.4c, *Extensions to P1003.4*--extends interfaces defined in P1003.1 and P1003.4 to include additional real-time facilities. (Draft 10, January 1991; balloting was planned for 2Q 1991.)

P1003.5, *POSIX Ada Binding*--determines the Ada environment interface and Ada extensions required for POSIX; provides a specification for the Ada environment interfaces and Ada required extensions so that applications programs can be written to operate consistently on all conforming POSIX/ Ada environments. (Draft 8, November 1991; approval expected in 2Q 1992)

P1003.6, *Security Interface for POSIX*--develops specifications for standard interfaces to security services and mechanisms for portable applications to include Systems Call Interfaces and System Commands. (Draft 12 balloted October 1991; approval expected 3Q 1992)

P1003.7, *Administered Systems (name changed from System Administration Interface)*--defines a standard interface to utility programs for administering systems that conform to POSIX. Work is being "sliced" into ballotable partitions which will be balloted separately in October 1992.

P1003.7a, *Printing*- (Draft 1, May 1991.)

P1003.7b, *Software*-. (Draft 1, July 1991)

P1003.8, *Transparent File Access (TFA)*--develops system interfaces and other mechanisms to permit portability of applications into environments where files, directories, etc., may reside on remote systems. (Draft 5, October 1991; mock balloting 4Q 1991.)

P1003.9, *POSIX FORTRAN Binding*--defines a FORTRAN-1977 language binding to applicable POSIX interfaces and functionality as specified in P1003.1,2,4, etc., and establishes an interface for FORTRAN to POSIX such that FORTRAN applications using POSIX functionality will be portable at the source code level. (Draft 11 approved October 1991)

P1003.10, *Supercomputing Application Environment Profile (AEP)*--develops an AEP for supercomputing environments. (Draft 5, March 1991; Draft 9 to be balloted July 1992)

P1003.11, *Transaction Processing*--develops a standard profile for transaction processing application environments. (Draft 2, March 1991; mock ballot of Draft 5 planned for January 1992; ballot expected mid-1992)

P1003.12, *Protocol Independent Interfaces*--defines programmatic interfaces that allow a portable application to communicate with another entity in the network such that the application may be independent of the underlying protocols. (Working pre-draft July 1991; balloting planned for 1992.)

P1003.13, *Real-Time AEP*--defines an AEP for real-time applications using the POSIX interfaces; addresses three profiles: full-function real-time system, embedded control system, and intermediate real-time system. (Draft 2, March 1991)

P1003.14, *AEP for Multiprocessing Application Support*--defines an AEP for multiprocessing applications environments based on relevant POSIX standards. (Draft 5, October 1991; mock balloting October 1991.)

P1003.15, *POSIX Batch Environment Amendments*--define utilities, library routines, system administration interfaces, and a host-to-host protocol to provide a network queueing and batch system in a POSIX environment. (Draft 6, July 1991, balloting of Draft 10 planned for July 1992.)

P1003.16, C *Binding for POSIX.1*--defines a C-language binding between ISO/IEC 9945.1:199x and the C standard. (Draft 1, May 1991; balloting expected 2Q 1992)

P1003.17, *Directory Services API*--defines an application programming interface to a directory service,...X.500 functionality . (Draft 2, September 1991; balloting planned for 2Q 1992)

P1003.18, *POSIX Platform Profile*--establish a Platform Environment Profile based on the ISO 9945 work and related standards which describes a simple foundation for an interactive, multiuser application platform. (Draft 4, January 1991; ballot planned for Spring 1992)

P1003.19, *POSIX* Ada *Language Interfaces*, Part 1: *Binding for Real-Time Extensions* (PAR approved September 1991)

Source: "Applications Portability and Open Systems Environments: Status Report," Roger J. Martin, NIST, presented at the *8th APP/OSE Workshop*, NIST, Gaithersburg, Maryland, 12 November 1991.

POSIX 1003.0 was sent to mock ballot in October 1991 in preparation for a real ballot in February 1992. NIST issued FIPS 151-1 based on the 1988 version of IEEE 1003.1. NIST held a workshop in November of 1991 to discuss the possibility of moving to a FIPS 151-2 based on the 1990 revision to the IEEE standard. POSIX 1003.1 was provided to ISO by the ANSI. WG15 of SC22 within the JTC1 was formed in September 1987 and assigned responsibility for POSIX. The IEEE standard P1003.1 has been adopted as ISO 9945-1. SC22/WG15 eventually intends to remove the focus on UNIX and the C language to create a generic interface specification between any language and a multiuser environment. WG15's division of work items is as follows:

- ISO 9945-1, *System Interface* (P1003.1 and .1a)
  - DP 9945-1.1, *Language Independent Base* (P1003.1c)
  - DP 9945-1.2, *Real Time and Extensions* (P1003.4 and .1b)
  - DP 9945-1.3, *Distribution Services* (P1003.8)
    - -- DP 9945-1.3.1, *Transparent File Access* (P1003.8)
    - -- DP 9945-1.3.3, *Transport Interface* (P1003.11)
    - -- DP 9945-1.3.4, *Name Space/Directory Services* (P1003.13)
- DP 9945-2
  - DP 9945-2.1, Shell and Utilities (P1003.2)
  - DP 9945-2.2, User Portability Extensions (P1003.2a)
- DP 9945-3, *System Management*
  - DP 9945-3.1, General Services (P1003.7)
  - DP 9945-3.2, Batch Services (P1003.10).

Part 2 of the POSIX standard is for interfaces to shell and utilities (P1003.2). Draft #9 of IEEE P1003.2 was submitted[26] to ISO through ANSI as DP 9945-2. It failed the registration ballot, however, and the project is now on hold since a new draft was requested for registration. Part 3, *Test Methods (General)*, was approved as IEEE standard 1003.3-1991 on March 21, 1991.

ANSI is developing a standard interface for the C language (ANSI X3J11) that is compatible with POSIX. As shown in Table 14, IEEE is working on Ada, FORTRAN, and C bindings for POSIX; the FORTRAN binding was approved in October 1991; the Adabinding should be complete in 1992. POSIX is intended to be compatible with both Database Language SQL and IRDS database management languages, as well as with OSI data communications and interprocess communications.

Other planned FIPS based on the POSIX standards include a Transparent File Access FIPS based on P1003.8 and a System Management FIPS based on P1003.7. Plans are to make the initial FIPS proposal for the Transparent File Access FIPS in the second quarter of 1992 with the expectation that a FIPS would be approved by early 1993. The

---

[26] P1003.2 (Draft #9, 1989) was proposed as a FIPS; however, it was determined that draft was not sufficiently mature or stable to become a FIPS.

System Management FIPS is only in the early planning phase, and an initial FIPS proposal will not be forthcoming until 1992. It has been proposed that the P1003.7 System Management area be subdivided into 10-15 subprojects, only 2-3 of which would be active at any one time. The primary motivation for the change is the recognition that some aspects are much further advanced than others. It is anticipated that the first set of subprojects will be Print Management, Software Management, and User Environment Management. [Ref. IEEE 1991]

IEEE POSIX Security Working Group (P1003.6) is defining security extensions to the base POSIX interface standard (ISO 9945-1), to include support for audit, privilege, discretionary and mandatory access control, and information labels. The P1003.6 draft from the April 1991 meeting was subjected to mock IEEE ballot in July 1991, the output of which entered the IEEE ballot in August 1991. Balloting is expected to take one year. The result, when converted to language independent format, could be then registered as a CD in SC22. Further work items, such as management, networking, and integrity requirements, were addressed at the July 1991 meeting of P1003.6. [Ref. IST/21: 2852 1991]

In August 1991, the National Body of Japan proposed a new work item, *Generic Operating System Interface (GOSI)*. At the same time it proposed the establishment of a new JTC1 Subcommittee on Application Portability to which this NWI would be diverted. The Japanese do not believe that existing base standards are sufficient for constructing AEPs. Specifically, a generic operating system interface standard is missing. While POSIX is an operating system interface standard, the Japanese do not believe it is generic since it is an extension of a *de facto* operating system interface. They propose to define a GOSI at a sufficiently higher abstraction level than the level at which POSIX or other *de facto* operating systems are defined. The ballot for this NWI closed 13 December 1991. [Ref. SC21 N 6403 1991]

7.2.1.2 POSIX Conformance Testing

The NIST Computer Systems Laboratory (NCSL) has developed a POSIX Conformance Test Suite (PCTS) based on IEEE 1003.1, Draft 10. The suite was in beta testing for over a year and is available from the National Technical Information Service (NTIS). The NIST National Voluntary Laboratory Accreditation Program (NVLAP) will accredit testing laboratories which will be referred to as Accredited POSIX Testing Laboratories (APTLs). On May 1, 1991, NVLAP announced the initial group of seven labs. The policy document for POSIX Conformance Testing is *NVLAP Program Handbook Computer Applications Testing - POSIX Conformance Testing*. Testing is done through agreement between the testing lab and the client, without NIST/CSL involvement. However, NIST/CSL issues the certificate of validation [Ref. Hall 1991]. As of November 12, 1991, NIST/CSL had issued Certificates of Validation for ten products.

The Conformance Testing Service has established a CTS-2 POSIX Project with the goal of a harmonized European and internationally recognized conformance testing service for POSIX. Participants in the project include the National Computing Centre Ltd (UK), the Computer Resources International A/S (Denmark), X/Open Company Ltd (UK), and British Telecommunications (UK). The project will be establishing test laboratories throughout Europe and seeking cross recognition with NIST [Ref. Pink et al. 1991].

7.2.2 Consortia Recommendations

Standards activities in areas related to the operating systems have been primarily in the area of developing international, nonproprietary standards for *interfaces* to operating systems. It appears unlikely that an international standard for an operating *system* will be developed, in part because operating systems are closely tied to the hardware architecture of vendor products.

As indicated earlier, POSIX is becoming a widely accepted approach to standardizing interfaces to operating systems; the initial standard for POSIX (ISO 9945-1) has been completed. Consortia have been formed to develop and promote profiles of standards that could be the basis for open environments and portable systems within these environments. All the consortia have adopted POSIX; however, there are differences in the approaches being taken. Activities of these consortia in the POSIX area are discussed in this section; additional information on portability profiles is provided in Chapter 13.

The international nonprofit consortium X/Open is developing extensions to UNIX System V Interface Definition (SVID), which will define a distributed (two-phase) transaction processing environment that meets OSI standards. A layered functional model for this environment that consists of resource, commit, and transaction management has been proposed. This model requires certain extensions to the UNIX kernel (guaranteed output to files and concurrent input from peripherals). The X/Open System V Specification (XVS) is the initial recommended standard for the operating system. The extensions would be part of a Common Applications Environment (CAE), a concept to promote software portability. This would be achieved by adopting and adapting existing industry and *de facto* standards, rather than by creating a new standard. Future goals for the CAE are alignment with POSIX P1003.1 (with a large number of extensions) and ANSI X3J11 C together with interfaces for Indexed Sequential Access Method (ISAM) and an embedded standard relational database language (SQL). The X/Open version of ISAM is based on a major (implementation nonspecific) subset of C-ISAM Version 2.10 (January 1985) from the Informix Corporation. The initial X/Open version of SQL is not fully compliant with ANSI X3.135-1986 [Refs. X/Open 1987; X/Open 1988; Lambert 1987]. Standards recommended for the CAE are discussed in Section 13.4.3.4.

Another approach to developing standard interfaces to UNIX-type systems is being taken by the OSF, an international consortium formed in May 1988. In December 1990, it

issued the first release of its OSF/1 Operating System. OSF has integrated a number of existing advanced technologies into its vendor-neutral operating systems. Sections 13.4.2.4 and 13.4.3.5 discuss OSF and OSF/1.

A third approach to developing POSIX-conformant operating systems is underway. This approach is based on providing a version of the Berkeley UNIX with a POSIX interface.

A fourth approach has been announced by the consortium called OPEN88. This consortium is reported to be planning to have a POSIX-conformant version of UNIX.

The NIST has developed an APP as an approach to identifying standards that could be used to achieve an open environment that would ensure a high degree of applications portability. In addition to the operating system, this environment includes data management, data interchange, network services, user interface, graphics services, and programming services. Security and system management services underlie the seven basic services since they are integral to them all. In addition to providing open systems interconnection, NIST believes POSIX is the key to such an environment. NIST has identified [Ref. Hankinson 1988] a number of areas in which the current POSIX definition must be extended in order to "provide full operating system functionality." These extensions include shell and tools, system administration, and terminal interface extensions. Extended POSIX would be part of an integrated set of non-proprietary standards. Efforts are still required to specify the appropriate standards and "bindings" for the open environment. The complete APP proposed by NIST, together with the status of relevant standards other than POSIX, is discussed in Section 13.4.3.3.

7.2.3 Operating System Standards

When common operating systems are used, there is a potential to reduce the development of CCIS system elements by sharing software. Even when different operating systems are used, adoption of operating system interface standards can increase application software portability. For CCISs, the recommended approach would be to agree on a standard operating system *interface* (i.e., POSIX), but *not* to seek agreement on a standard operating system. Standards for applications portability are addressed in Section 3.4.3.

SC21 has begun work in the area of Operating Systems Command and Response Language (OSCRL). A draft proposal for OSCRL is planned, but has not yet been promulgated.

Two communities of operating systems standards have received strong support from vendor groups promoting application portability. One group is UNIX International (formerly Archer, with a membership of 42 corporations and user groups), which promotes UNIX System V, a proprietary standard of AT&T. Availability of Release 4.0 of

UNIX System V was announced at the UNIX EXPO (November 1989) and is now commercially available. This release aims to:

- Merge all the major versions of the UNIX operating system (i.e., the /user/group Xenix, the Berkeley 4.x BSD, and the Sun Operating System)
- Enhance data networking with the addition of Remote File Systems and Remote Procedure Calls
- Address real-time applications and environments
- Ensure conformance to POSIX through enhanced signal handling, multiple groups and ownership, and job control
- Achieve and maintain full compliance with the X/OPEN CAE.

The other major group promoting operating systems is the OSF, which has adopted the IBM AIX Version 3 of UNIX. This version conforms to POSIX, and future releases will comply with Issue 3 of the X/Open Portability Guide (XPG3). IBM intends to support both TCP/IP and OSI protocol (to include X.25) that will operate over various physical connections. Other features of this operating system are the provisions for network management functions via OSI's Common Management Information Service/Protocol (CMIS/CMIP), electronic mail via X.400, and presentation services via X-Windows [Ref. OSN 1990j].

7.3 Assessment of Coverage by Standards

Standardization of operating systems appears unlikely. Further, there is no need to select a standard operating system for an automated CCIS, since such a selection is viewed as an implementation issue. When mature, adopting the POSIX interface standard for CCISs appears to be an attractive option, both to achieve some of the required system services and to promote applications portability during implementation. Adoption of the current POSIX standard would probably not fully meet system service requirements. For example, POSIX addresses independent operating systems cooperating in a distributed environment, not a single operating system running on multiple machines. It is not specifically designed for distributed applications, and therefore may not serve a CCIS's needs completely. However, further refinement of the CCIS requirements and extensions of the POSIX standard are needed to assess additional requirements for a specific CCIS.

8. SECURITY, MANAGEMENT, REGISTRATION, AND CONFORMANCE TESTING STANDARDS

This chapter summarizes the status of standards in five areas: security, network (OSI) management, registration authorities, conformance testing, and formal description techniques (FDTs). Appendix F identifies organizations and standards bodies that have contributed to development of these standards.

Quick Reference	
Topic	Page
Assessment	196
BLACKER	168
COMPUSEC	169
Conformance Testing	187
Database Security	161
Directory Security	161
Estelle	192
FDTs	191
FTAM Security	160
G-LOTOS	194
ISP Security	161
LOTOS	192
Managed Objects	172
Management SIGs	186
NATO AHWG on Sec	164
NOSA	164
ODA Security	161
OSI Management	170
PICS Proformas	191
QoS	184
Registration Authorities	195
Requirements	153
SDL	193
SDNS	165
Security ASE	162
Security Exch Info	162
Sec Framework	156
Secure LANs	168
Security Models	156
Structure of Mgmt Info	181
Systems Management	179
TMN	182
TP Security	160
Z (FDT)	194

8.1 Requirements for Security and OSI Management Services

Security services protect the components, mechanisms, and information of the CCIS. Basic security features include authentication, access control, confidentiality, integrity, and non-repudiation. OSI management addresses fault management, configuration management, accounting management, performance management, and security management.

Standards for security and OSI management are described first (Sections 8.2 and 8.3, respectively). These are followed by standards for conformance testing (Section 8.4) and registration authorities (Section 8.5). FDTs are addressed with conformance testing standards in Section 8.5.

8.2 Status of Standards for Security

Security features are required by both civil and military systems and may be expected to be addressed by ISO and CCITT standards in the future. Specific military requirements for security and the TSGCE recommendations for addressing these requirements are treated in Section 15.3.7.

8.2.1 Overview of Civil and Military Security Standards

Standards for security are being addressed in the following:

- ISO 7498-2, *Security Architecture*, February 1989.
- DIS 10181, *Security Frameworks in Open Systems*, December 1989.

- *NATO OSI Security Architecture (NOSA),* March 1988, UNCLASSIFIED [Ref. NOSA 1988], defines the security services, based upon ISO 7498-2, required in the NATO OSI Reference Model.
- *Security Architecture for NATO Information Systems Interconnection (SANISI),* Version 2.0, April 1989, NATO CONFIDENTIAL [Ref. SANISI 1989]. SANISI is planned to be standardized as STANAG 4250-2.
- Security annexes (Annex B) for NATO OSI STANAGs 4250-56 and 4261-66 and other STANAGs planned for Layers 6 and 7 (a draft Annex B has been prepared for STANAG 4253 and 4263).
- A series of appendixes to SANISI are expected to be developed to expand on the actual implementation of a secure protocol. The first of these, Trusted Communications Sublayer (TCS), is defined in the NOSA and SANISI documents.
- Lower layer security protocols, including the Network Layer Security Protocol (NLSP, CD 11577) and the Transport Layer Security Protocol (TLSP, DIS 10736) and the Secure Data Network System (SDNS) security protocols that service, in part, as the basis for NLSP and TLSP. (There is a close correspondence of services between the NLSP security protocol and TCS [Ref. PC 1989]; future work in TSGCE SG9 on the TCS will be based on the NSLP.)
- Extensions to SDNS protocols, such as the End-to-End Security Protocol (EESP) being developed in the United Kingdom for submission to ISO SC21/WG1.
- IEEE P1003.6 and JTC1 SC22 standards for POSIX security (see Sections 7.2.1 and 8.2.2.12).

8.2.2 Security Standards Work in ISO[27]

SC21/WG1, SC21/WG3, and SC21/WG6 have begun a number of initiatives to address the models and standards frameworks required to progress OSI security standards. These include:

- Management plan for security [SC21 SD-7, June 1990]
- OSI security architecture (ISO 7498-2)
- Guide to Open Systems Security [SC21 N 6167, July 1991], a technical report (which is in WD status) developed to provide an overview of the security-related work within SC 21
- Security framework overview (WD 10181-1)
- Authentication framework (DIS 10181-2)
- Access control framework (CD 10181-3)
- Non-repudiation framework (WD 10181-4)

---

[27] Discussion taken from *Work on Security within IST/21*, SC21 N 5757, March 1991.

- Confidentiality framework (WD 10181-5)
- Integrity framework (WD 10181-6)
- Security audit trail function (CD 10181-7)
- Key management (WD 10181-8)
- Upper layer security model (CD 10745, June 1991)
- Network Layer Security Protocol (NLSP, CD 11577) and Transport Layer Security Protocol (TLSP, DIS 10736).

Other work is progressing in SC21 on security enhancements to presentation standards, to association control standards, and (as necessary) to other Application Layer standards:

- Reference model of data management (DIS 10032)
- RDA (DIS 9579)
- Systems management tutorial (ISO 10040)
- Security alarm reporting function (ISO 10164-7)
- Objects and attributes for access control (CD 10164-9.2)
- CMIS access control (ISO 9595/DAM 4)
- CMIP access control (planned amendment to ISO 9596-1)
- Directory access control (ISO 9594-1/PDAM 1, ISO 9594-2/PDAM 1, ISO 9594-3/PDAM 1, and ISO 9594-4/PDAM 1)
- Directory authentication access control (ISO 9594-8/PDAM 1) (see Section 8.2.2.7)
- FTAM security services (new work item JTC1 N 955, amendment to ISO 8571)
- TP security (new work item SC21 N 5176, amendments to DIS 10026-1, 10026-2, and 10026-3)
- Security Exchange ASE service and protocol (SC21 N 6096, 6097, 6098)
- ACSE authentication (ISO 8649/AM 1)
- Conditions for ACSE authentication (new work item proposed in JTC1/SC10 and transferred to SC20 and then to SC21)
- Presentation confidentiality and integrity (SC21 N 5059)
- Presentation cryptographic techniques (transferred from SC20/WG3 to SC21); merged in SC21 with presentation confidentiality and integrity (above).
- ODP security (SC21 N 4888)
- Authentication services for distributed applications (SC21 N 6099) (see Section 8.2.2.11)
- ASN.1 encoding rules to provide upper layer security and compression (SC21 N 6130)
- Alignment of upper and lower layer security protocols (SC21/WG6 N 6130, November 1991)

- Positioning of encipherment and decipherment functions (Application Layer versus Presentation Layer) (SC21 N 5503, January 1991).

SC27, Security Techniques is also working with SC21 on several projects [Ref. SC21 N 6066 1991]:

- *Security Information Objects* [SC27 N 332, 14 October 1991]
  - Part 1: *Method and Guidelines for the Definition and Registration of Security Information Objects*
  - Part 2: *Generic Security Information Object Class Specifications*
- *Key Management* (see Section 8.2.2.1)
- *Zero Knowledge Techniques* [SC27 N 345, 4 November 1991]--the means by which possession of information can be verified without any part of that information being revealed, wither to the verifier or to any third party. These techniques are applicable to entity authentication, data authentication, and digital signature.

8.2.2.1 Security Framework

DIS 10181, *Open Systems Security Framework,* defines the framework within which security services for open systems are specified. These open systems include database, distributed applications, ODP, and OSI. The framework addresses data elements and sequences of operations (but not protocol elements) that are used to obtain security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems and to data managed by systems. Note that the security framework is being developed by SC21/WG1, whereas the Upper Layer Security Model is the responsibility of SC21/WG6 and the Lower Layer Security Model is the responsibility of SC6/WG2 and SC6/WG4. Table 15 identifies the scope of the individual parts of the framework.

8.2.2.2 Security Models[28]

The purpose of the security models is to apply the security concepts detailed in the Security Frameworks to specific areas of open systems architectures.

Upper Layer Security Model. The Upper Layer Security Model is intended to provide the necessary basis for the development of security-related protocol elements for the secure exchange of information between open systems, with the interchange of information related to security policy control and management, and with services and mechanisms for controlling access to resources accessible via OSI. It will address the following:

- Security aspects of communication in the upper layers of OSI

---

[28] Discussion for this section was taken from *Guide to Open Systems Security*, SC21 N 5533, 3 January 1991.

- Relationships between security services and mechanisms in the upper layers, to be considered in greater detail than is provided in ISO 7498-2
- Properties of the possible combinations of security services and mechanisms in the upper layers
- Interactions among Application, Presentation, and Session Layers in providing security services
- Invocation of lower layer security services
- Requirements for security management in the upper layers.

Table 15. OSI Security Framework--DIS 10181

- Part 1 (WD 10181-1), *Overview,* 29 July 1991 [SC21 N 6166]--Describes the organization of the security framework, defines security concepts that are required in more than one part of the security framework, and describes the interrelationship of the services and mechanisms identified in other parts of the framework. CD expected June 1992.
- Part 2 (DIS 10181-2), *Authentication Framework,*-[SC21 N 5281]-Authentication is the process of corroborating an identity. Overlap with DIS 9798-1, Security Techniques, Part 1: Entity Authentication Mechanisms. SC27 proposed a joint meeting to align terminology and concepts relating to authentication during January - March 1991. Voting began 18 July 1991. IS expected March 1992. Two amendments are in WD status: *Refinement of Subcomponents of Claimant and Verifier* and *Classification for a New Class of Mechanisms to Defeat Opportunistic Attacks.*
- Part 3 (CD 10181-3), *Access Control Framework,* June 1991 - [SC21 N 6188]-Access control is the process of determining whether the use of resources within an open system is permitted. DIS expected March 1992.
- Part 4 (WD 10181-4), *Non-Repudiation Framework,* 29 July 1991 [SC21 N 6165]--Non-repudiation is a security service that provides proof of origin or delivery of data in order to protect the sender against the false denial by the recipient, that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent. The use of appropriate mechanisms is coupled with the necessary assurance mechanisms providing proof about certain properties of the communications between the entities involved, such as its integrity, origin, time, and destination. Non-repudiation implies the existence of an agreed third party whose primary role is to arbitrate disputes resulting from non-repudiation. CD status expected in June 1992.
- Part 5 (WD 10181-5), *Confidentiality Framework,* 29 July 1991 [SC21 N 6164] - The maintenance of the secrecy of data is called confidentiality. CD expected June 1992.
- Part 6 (WD 10181-6), *Integrity Framework,* 29 July 1991 [SC21 N 6163]--The integrity framework addresses the constancy of a data value and not any other form of invariant that such a value may possess. In particular, it does not address the constancy of any information that the data is deemed to represent. There are two types of integrity mechanisms needed for two types of constancy. The first is the constancy of the value of data in an environment in which a *random* modification to integral data may be made. The second is the constancy of the value of data in an environment in which a modification to integral data may *deliberately* be made to defeat the integrity mechanism. CD status expected in June 1992.
- Part 7 (CD 10181-7), *Security Audit Framework,* 14 August 1991 [SC21 N 6169]. This CD describes a model of a system's audit trail, a description of audit events and the different types of information involved, and its relationship to management activities. DIS expected March 1992.
- Part 8 (WD 10181-8), *Key Management,* November 1991. Work on this part is being carried out in SC27. The first working draft is SC21 N 6606, December 1991. The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms. Key management includes: key generation, key distribution, key installation, key storage, key archiving, and key deletion. A fundamental problem is to establish keying material whose origin, integrity, and, in the case of secret keys, confidentiality can be guaranteed.

The Upper Layer Security Model [SC21 N 6095] progressed to CD status [CD 10745] in June 1991. It addresses primarily FTAM security requirements, not those

of distributed applications such as Directory, TP, and X.400.[29] Associated projects include:

- Service and protocol for security application service element [SC21 N 4110, proposal for NWI, January 1990]--name changed from Authentication Exchange ASE to Security ASE; see Section 8.2.2.11
- Presentation cryptographic techniques (project transferred from SC20)
- Practical conditions for ACSE authentication (project transferred from SC20)
- Generic transfer syntax providing upper layer security (SC21 N 6130, August 1991), possibly to become a new part of ISO 8825
- Presentation Layer security provisions for the Upper Layer Security Model (SC21 N 5732, April 1991).

Lower Layer Security Model. The purpose of this standard is to provide standards developers with the necessary basis for the development of security-related protocol and security-related protocol elements appropriate to the lower layers of the OSI Basic Reference Model. The model addresses:

- The concepts that are generally applicable to the lower layer protocols
- General guidelines for the selection and placement of security services and mechanisms
- Interactions between the layers--both within the lower layers and between the upper and lower layers--relating to security
- General requirements for security management across the lower layers.

Lower Layer Security Guidelines. While an OSI Lower Layer Security Model [SC6 N 5333] was begun, it was decided at a joint meeting of SC6/WG2 and SC6/WG4 in October 1990 not to progress it. However, the guidelines document [SC6 N 6957, working draft out for ballot] may form the basis of a future standard [Ref. SC6 N 6219 1990]. A number of security issues need to be resolved before this would be likely. [Ref. Walters 1991]

The issue of adding security services to OSI layer 2 in ISO 7498-2 was raised by SC21/WG1 in May 1991. The IEEE standard for Interoperable LAN Security (802.10 Part B) provides data confidentiality, connectionless integrity, data login authentication, and access control security services at OSI Layer 2 while 7498-2 provides only data confidentiality.

Network Layer Security Protocol (CD 11577). The NLSP is based on three standards efforts. One part of the US Secure Data Network System[30] (SDNS) is a connectionless Layer 3 security protocol (see Section 8.2.4.1) equivalent to the end-to-end

---

29 Major comment added by *U.S. Contribution on ISO/IEC CD 10745: Upper Layers Security Model*, by ASC X3T5, 1 October 1991.

30 One of the objectives of SDNS is to emphasize commercial participation in developing security products.

encryption portion of the Trusted Communications Sublayer (TCS). Northern Telecom's SPX security protocol adds connection-oriented service to SP3. The United Kingdom's End-to-End Security Protocol (EESP) adds connection-oriented services to SP3 and includes integrity and traffic padding. EESP was introduced into SC21/WG1 during May 1990 and has been proposed to the JTC1 as a new work item. EESP may require changes to ISO 8648, *Internal Organization of the Network Layer* [Ref. BSI 1989].

NLSP can operate both in the CO and CL modes and can be implemented in both end systems and intermediate systems. Both modes support address (source/destination) confidentiality. The NLSP protocols makes use of the concept of a security association (for cryptographic keys and associated parameters) and provides security on the basis of the quality of service the Transport Layer demands and the quality of service the domain administration proposes.

The NLSP committee draft ballot ends in April 1992, and NLSP is expected to advance to DIS status in July 1992.

Transport Layer Security Protocol (DIS 10736). TLSP is based on the SDNS SP4 and specifies optional extensions to both the connection-oriented transport protocol (ISO 8073) and connectionless-mode transport protocol data unit (TPDU) transmission (ISO 8602) standards to permit use of cryptographic techniques. Since the proposed protocol operates as an extension only, it does not preclude unprotected communication between transport entities implementing ISO 8073 or ISO 8062. The TLSP has a committee draft keying protocol on *Security Association Establishment* (DIS 10736 PDAM 1) that is expected to reach DIS status in July 1992. This protocol is to be used to exchange security attributes, including encipherment algorithm and traffic key. The standard permits either symmetric or asymmetric algorithms, but the present standard has only a public key (symmetric) algorithm in-band method. Alternatively, an out-of-band method may be specified that is manual or proprietary.

8.2.2.3 Requirements and Approaches for Security

In March 1990 at the Workshop on Distributed Applications in Phoenix, the following observations on security were made [Ref. SC21 N 4526 1990]:

- It is highly desirable to standardize a general approach to providing security in the Application Layer. This can be accomplished by supporting a variety of security methods that involve communication of security information. Examples of such methods could be:
  - Two-way or three-way authentication exchange
  - Privilege attribute certificate transfer
  - Key negotiation sequence.
- A security method would consist of semantics, syntax, and procedural rules relating to the communications aspects of the method.

- There appear to be three possible OSI architectural approaches to supporting security methods:
  - No generic security ASE(s), in which the syntax and procedural rules for any security method are imported into the specification of an application-specific ASE.
  - One generic ASE, in which one ASE is provided that can import into its abstract syntax the syntax of any security method. Possibly, the procedural rules associated with all security methods could be incorporated into the ASE specification.
  - Multiple purpose-specific security ASEs, in which each ASE incorporates the procedural rules and syntax for a particular security method or group of closely related methods (e.g., an ASE to support two-way authentication exchanges).
- Satisfaction of security requirements of TP, Directory, and OSI Management will depend on addressing security modelling issues related to distributed applications. The Upper Layer Security Model includes this in its scope, but the current draft of the model suggests little will be done in this area when it is first released.
- Access control to data resources must address the data model being used by individual applications such as DFR, DTAM, FTAM, IRDS, RDA, SQL, etc. Use of a common data modelling approach provides the potential for use of common access control facilities to such data resources and consequently increases the attractiveness of the common data model approach in order to prevent the need for re-specification of access control facilities for data management applications.

8.2.2.4 FTAM Security

FTAM security appears to be based on passwords. The first password identifies the user (log on) and subsequent passwords are used when protected items (such as records and data) are accessed [Ref. Collela 1992]. Additionally, security may be derived from use of access control lists, such as listing "people" and "groups of people" that are or are not allowed access. JTC1 N 955, *Enhancements to* FTAM *Security Services,* is a new work item proposing amendment (WDAM 4) to several parts of ISO 8571 (FTAM) to deal with authentication and access control in FTAM and suggests some specific forms of access control mechanism [Ref. SC21 N 5757 1991].

8.2.2.5 TP Security

SC21 N 5176, *OSITP Security,* is a new work item for Transaction Processing security. It proposes amendments to DIS 10026 (Parts 1,2, and 3) addressing the formulation and provision of mechanisms to meet a number of security services, including authentication, access control, confidentiality, integrity, non-repudiation, auditing, "management," access right revocation, replay protection, prevention of the denial of service, reliability, and traffic flow confidentiality. This is to deal both with control of access to TP resources and to TP application entities [Ref. SC21 N 5757 1991]. A

Preliminary TP Security Model [Ref. SC21 N 6232] was distributed for comment in May 1991.

8.2.2.6 ODA Security

Changes are being made to ODA, ISO 8613, to improve the security aspects. ODA provides protection for documents as a whole or for parts of a document. Confidentiality, integrity, authentication, and non-repudiation of origin are all supported using encipherment, fingerprints, and seals [Ref. SC21 N 4472 1990].

8.2.2.7 Directory Security

ISO 9594-1 (The Directory) PDAM 1, ISO 9594-2 PDAM 1, ISO 9594-3 PDAM 1, and ISO 9594-4 PDAM 1 develop a model for access control and an access control scheme for general use (in Part 2) and (in Parts 3 and 4) provides "hooks" whereby the access to directory information can be controlled (not to the entities holding the information). These hooks inserted by the amendments to Parts 3 and 4 allow a variety of external access control schemes to be used, not necessarily the basic access control scheme of Part 2 [Ref. SC21 N 5757 1991]. A new work item, *Security Enhancement to Directory*, will extend Part 8, the *Directory Authentication Framework* [SC21 N 6172, July 1991]. PDAM status is expected December 1992.

8.2.2.8 Database Security

SQL2 specifies some security functionality but the standard (ISO 9075) does not address how a secure database should be built. Since the security of the operating system needs to be considered in building a (secure) database, POSIX standards are also relevant to the security of databases.

8.2.2.9 International Standardized Profile (ISP) Security

It has been suggested that the scope of TR 10000 be extended to address the security features in ISPs. An ISP may contain security features if one (or more) of the base standards to which it refers contain security features. In general, the specification of an ISP having security features has two distinct parts, one concerned with security-related functions and one concerned with other functions. This specification is referred to as a security sub-profile. An ISP may contain one (or more) security sub-profiles. The security sub-profile comprises [Ref. Humphreys 1991]:

- A description of the target system environment in which the sub-profile is intended to be used
- An identification of the range of (security) threats that the sub-profile is intended to counter in the target system environment
- A specification of how security functions in base standards should be used to counter the assumed threats

- A specification of the security mechanisms that should be used to provide the necessary security functions (where the base standards provide some freedom of choice)
- A specification of the range of the realizable quality attainable through the use of this sub-profile.

8.2.2.10 Proposed ASE for Security

CCITT SG VII has identified a need to define an ASE capable of providing arbitrarily complex n-way security exchanges, where such exchanges could occur in conjunction with association establishment or after an association has been established. The SG VIII proposal [Ref. SC21 N 3991 1989] identifies such Application Layer exchanges as peer-entity authentication exchanges, exchanges of keying information, and combinations of these. The proposed Security Exchange Service Element would address ACSE shortcomings: peer authentication in ACSE (ISO 8649 DAD1) applies only at the time of association establishment and is limited to a single two-way exchange.

8.2.2.11 Security Exchange Information

A security exchange is the transfer of protocol-control-information, called security exchange information, between open systems as part of the operation of a security mechanism. An ASE that supports the communication of security exchange information is designated a security exchange ASE.

SC21 has adopted a new work item on security exchange ASE that will provide for the transfer of information between a pair of application-entity invocations in support of security services such as authentication, access control, confidentiality, and integrity. The security exchange would be allowed to occur either in conjunction with association establishment or at any time on an established association. Encryption/signature functions could be located in either the Application Layer or the Presentation Layer. A standard method for defining security exchange information using ASN.1 will be defined as part of this work item [Ref. SC21 N 5002 1990]. The Generic Security Exchange ASE standard will comprise four parts, three of which are being recommended for progression to CD status [Ref. SC21 N 5448 1990]:

- *Security Exchange Model and Specification Framework,* [SC21 N 6096] June 1991
- *Security Exchange* ASE *Service Definition,* [SC21 N 6097] June 1991
- *Security Exchange* ASE *Protocol Specification,* [SC21 N 6098] June 1991
- *Security Exchange* ASE *PICS Proforma.*

A NWI developed in SC21/WG6, *Authentication Services for Distributed Applications,* [SC21 N 6099, 1 July 1991] was not accepted by JTC1. It would specify security exchanges to support authentication, suitable for conveyance by the Security

Exchange ASE and describe procedures to be used in conjunction with these security exchanges in order to provide full authentication service. The basis for this work would be the authentication schemes defined in the *Directory Authentication Framework* (ISO 9594-8) (see Section 8.2.2.7), extended as necessary to support the needs of distributed applications in general. SC21 will review the new work item proposal in May 1992 to see if there is adequate support to proceed.

8.2.2.12 Additional Security Standards Work in ISO

JTC1 held a Workshop on Security in London during 5-7 November 1990. JTC1 participants from the Special Working Group (SWG) on Security, SWG-EDI, SC6 (WG2/WG4), SC17(WG4), SC18(WG1/WG4), SC21(WG1), SC22 (POSIX Security), and SC27 attended as well as additional participants from TC68 and TC154. The topics offered for consideration at this workshop were wide ranging and indicate the scope of ongoing work and areas envisioned for standardization in the next 5 or more years [Ref. IST/21:2170 1990]:[31]

- Information security technology
- Information security risk analysis methodology
- Access control to applications and or security objects (e.g., for confidentiality and integrity)
- User authentication
- Indirect access to security objects or delegation mechanisms
- Physical security in such areas as biometrics equipment, TEMPEST equipment, tamper resistance, computer room design, and card access control equipment
- Network security management
- Network access control
- Syntax and data elements for audit trails
- Secure version of OSI protocols (e.g., Data Link Layer, Transport Layer, upper layers)
- Secure versions of EDI
- Secure versions of standards for office documentation
- Standards for secure application design
- Secure versions of databases
- Generic security techniques and mechanisms in such areas as message authentication, digital signatures, peer entity authentication, and key management
- Security of distributed applications
- Security of transaction processing
- Information technology security evaluation criteria
- Integrated circuit cards security.

---

[31] The ISO Member Bodies provided recommendations on priorities for these topics; a summary of these recommendations is given in JTC1 N 1011, "Results of National Body Survey," 10 October 1990.

8.2.3 Security Standards Work in NATO

8.2.3.1 TSGCE SG9 AHWG on Security

The TSGCE SG9 Ad Hoc Working Group (AHWG) on Security is developing the NOSA and SANISI documents (identified in Section 8.2.1 above), whereas the security annexes for the layer STANAGs are the responsibility of TSGCE SG9/WG1 and SG9/WG2. NOSA was developed to give guidance to contractors and procurement managers on the preferred placement of security services within OSI-conformant systems. SANISI provides more detailed rationale on the placement of security services and mechanisms within the NATO OSI Reference Model. The emphasis has been to derive appropriate refinements and augmentations to ISO 7498-2 so that a comprehensive set of security facilities can be defined to satisfy the NATO secure interoperability requirements. SANISI is expected to remain classified for the foreseeable future. Annexes in SANISI are planned to address LANs, security management, and TCS services. There are some terminology differences between NOSA and SANISI; otherwise these documents are considered stable. The AHWG on Security has also developed a classification guide [Ref. NATO 1989a].

The TCS architecture has been broken down into five functional modules. A description of this internal architecture was presented at the SHAPE Technical Centre Military OSI Symposium in June 1990 [Ref. NATO 1990]. Two of the five TCS modules identified so far now have service definitions and protocol specifications in draft form [Ref. NATO 1990a]. *Work is continuing in the AHWG on Security to make the TCS conform to the eventual security protocol agreed by ISO--only the implementation would be unique to NATO.* Further, security issues have been identified by the AHWG on ISDN; when a security architecture is defined for ISDN, that architecture will be assessed to see how it relates to NOSA.

8.2.3.2 NOSA

NOSA identifies OSI security services for the Physical, Network, and Presentation/Application Layers. These are [Ref. NOSA 1988]:

- Physical Layer will provide two services by transparent means without requiring modifications to the Physical Layer protocols:
  - Connection confidentiality, which is capable of dealing with circumstances where the physical communication is intermittent or asymmetric.
  - Traffic flow confidentiality.
- Network Layer security services are provided within subnetwork-dependent roles and within a TCS:
  - Subnetwork-dependent services are peer entity authentication, data origin authentication, access control, connection confidentiality, connectionless confidentiality, traffic flow confidentiality, connection integrity without recovery, and connectionless integrity.

- Security services that can be provided by the NATO TCS are identical to the eight identified above for subnetwork-dependent roles.

• Presentation/Application Layers could provide as many as 14 security services:
  - The eight services identified above for the Network Layer.
  - The following additional six services: selective field confidentiality, connection integrity with recovery, selective field connection integrity, selective field connectionless integrity, non-repudiation with proof of origin, and nonrepudiation with proof of delivery.

8.2.4 Other Security Standards Work

8.2.4.1 Secure Data Network System (SDNS)

The goals of SDNS are to create specifications for end-to-end security; to use the OSI Reference Model; to design an architecture to include electronic mail and end-to-end encryption; to provide transparent key management; and to demonstrate feasibility of techniques. The US National Security Agency (NSA) is supporting the SDNS project [Ref. Tater et al. 1989], which has released to the public domain several standards for security protocols [Refs. NSA 1989; NSA 1989a; NSA 1989b; NSA 1989c; NSA 1989d; NSA 1989e; NSA 1989f; NSA 1989g; NSA 1989h; NSA 1989i; NSA 1989j]. The elements of SDNS are described in Table 16.

The SP3 protocol is comparable to the TCS requirement identified by TSGCE SG9. However, it does not meet all the TCS requirements and it requires CL network services. For example, traffic flow confidentiality is not supported by SDNS. The United Kingdom has recently introduced the EESP, which could address the TCS requirements more fully and support services for CO networks [Ref. Neve 1990]. There is some question as to whether the security models and the mechanisms that provide security services underlying SDNS and the TCS are so different that SDNS can meet the TCS requirements [Ref. Walmsley 1990].[32]

NSA is working with NIST to incorporate the SDNS protocols into US GOSIP. The SDNS protocols will also be introduced into the ANSI by NIST and, if accepted, into the ISO OSI Security Architecture. SP3 and SP4 have already been submitted by ANSI to ISO: SP4 has been accepted as a new work item (part of the Transport Layer Security Protocol), and SP3 was accepted as a new work item after some modifications (part of the Network Layer Security Protocol). Testing of breadboard hardware with the SDNS protocols was conducted in 1989.

---

[32] In a private communication with Clive Walmsley, RSRE, in March 1990, a comment was made that the prospect of interoperability between the two models would be remote.

Table 16. Security Protocols Developed in SDNS

- Security Protocol 3 (SP3). Provides various security services in the Network Layer through the use of cryptographic mechanisms; SP3 is a subnetwork independent convergence protocol (SNICP, ISO 8648) that extends the CLNS (ISO 8348/AD1) with confidentiality (protection against passive monitoring), integrity (protection against modification, replay, addition, or deletion), or both. SP3 is designed to be used at the top of Layer 3 [Ref. NSA 1989].
- Security Protocol 4 (SP4). Specifies optional extensions of the COTS (ISO 8072) and connectionless transport service (ISO 8072/AD1) for the Transport Layer. The extensions permit the use of cryptographic techniques to provide data protection for transport connections for connectionless-mode Transport Protocol Data Unit (TPDU) transmission. SP4 can be used with the CONS or the CLNS. SP4 is designed to be used at the bottom of Layer 4 [Ref. NSA 1989a].
- Message Security Protocol (MSP). Defines additions to the CCITT X.400 (either 1984 or 1988) that permit any type of message (including interpersonal messages) to be sent and received securely. When used with the conventions defined by ANSI for the X.400 Message Transfer System, MSP can be used to exchange EDI messages securely. The MSP provides writer-to-reader confidentiality, access control for message transfer, and request for a signed receipt of the received message. SDN 701 [Ref. NSA 1989c] specifies the MSP, and SDN 702 [Ref. NSA 1989d] defines new attribute types and object classes for inclusion in the X.500 Directory in support of key management functions used by MSP.
- Key Management Protocol. Key management provides for the generation, distribution, and updating of traffic encryption keys (TEKs). The abstract model for a Key Management Application Process (KMAP) consists of two parts: the information processing part that is supported by Management Information Bases (MIBs) for keys and for TEKs, and the communication part, called the Key Management Application Entity (KMAE). The KMAE consists of the Layer 7 ACSE (ISO 8649) and a Key Management Application Service Element (KMASE). The Key Management Protocol provides Layer 7 peer-level services between the KMASEs of two KMAPs. The Key Management Protocol assumes the use of the connection-oriented presentation services (ISO 8822) [Refs. NSA 1989b; NSA 1989h; NSA 1989i; NSA 1989j].
- Access Control. Access control is the prevention of the unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner (ISO 7498-2). SDN 801, SDN 802, and SDN 802/1 [Refs. NSA 1989e; NSA 1989f; NSA 1989g] specify an access control framework based on a four-tiered model and an Access Control Information System (ACIS) that provides a uniform method for encoding access control information that is independent of any particular security policy. The ACIS also provides a standard algorithm for interpreting and comparing access control attributes. The access control framework provides for authentication data and access control checks that will allow communication between different SDNS users/systems when their respective security policies allow it. The framework provides two processes: a Peer Access Approval process for interpreting the data of the four-tiered mode, and the Peer Access Enforcement Process for enforcing access control on a Protocol Data Unit (PDU) basis [Refs. NSA 1989e; NSA 1989f; NSA 1989g].

8.2.4.2 NIST Recommendations

The NIST approach to OSI security standards includes the following features [Ref. DCA 1989a]:

- Security encapsulation standard to provide cryptographic protection of integrity and confidentiality. A common format and processing standard is needed that is independent of the algorithm to be used.
- NLSP based on the SDNS Security Protocol at Layer 3 (SP3). There are four subclasses: N-no routing, A-routing but no fragmenting and reassembly, I-fragmenting and reassembly, and D-fragmenting and reassembly for DoD Internetwork Protocol.
- TLSP based on the SDNS Security Protocol at Layer 4 (SP4).
- Mail handling security system for MHS, to be used between the User Agent and the Transfer Agent to encapsulate the entire message contents; this requires

posted keys and certificates. (One candidate is from X.411; another is the MSP from SDNS.)

- Cryptographic key management, a service to be provided at the Application Layer to support real-time (SP2, SP3, and SP4) as well as posted (MHS) requirements. Current proposals are based on private key (ANSI X9.17) or public key (SDNS) techniques.
- Security labels and labelling. These are planned to be strongly coupled with data.
- Authorization and access control. These features would permit policies to be specified within security domains and would support multiple policies and models (candidates are from ECMA and SDNS).

In addition, NIST is developing standards for digital signature and nonrepudiation where a message and the identity of the sender are cryptographically combined in such a way that any unauthorized change to the message is detectable and the originator cannot deny creating the message. This feature would require trusted notarization and storage. Finally, NIST is developing techniques outside the OSI model for personal identification and authentication. Approaches include knowledge, token, or physical means. Technologies being considered include a smart card and use of passwords. A NIST workshop in September 1990 addressed integrity guidelines, but to date no written results have been forthcoming. The current concentration of NIST is on beginning the development of a new set of Information Security Product Evaluation Criteria, better known as the Federal Criteria.

The NAOIW has a Special Interest Group (SIG) on OSI Security Architecture. The purpose of this group is to develop an overall OSI security architecture that is consistent with the OSI Reference Model and that economically satisfies the primary security needs of both the commercial and Government sectors. The SIG on OSI Security Architecture plans to address key management and security management functions that must be performed between the layers and the peer entities defined in the OSI architecture. Once SP3 and SP4 are adopted as Draft International Standards, the SIG on OSI Security Architecture can consider them for Interim OSI Implementor's Agreements. NIST is in the process of developing a FIPS that would specify the format for a security label for the US GOSIP telling protocol processing entities how to handle unclassified but sensitive data communicated between open systems. An initial draft was issued February 1991.

8.2.4.3 ECMA Recommendations

In December 1989, ECMA issued a standard (ECMA 138) entitled *Security in Open Systems--Data Elements and Service Definition*. It is based on ECMA TR 46, *Security Framework* [Ref. ECMA 1988], which describes a framework for the development of security provisions in the Application Layer. ECMA 138 defines data elements and services for support of a multi-user, multi-vendor, distributed system environment.

8.2.4.4 IEEE Work on Secure Local Area Networks (LANs)

Draft standards are being developed for secure LANs. IEEE P802.10 has released (January 1989) a draft of the Standard for Interoperable LAN Security (SILS) [Ref. SILS 1989]. The draft standard provides different service interfaces for key management, secure data exchange, and security management:

- IEEE P802.10A - *Interoperable LAN Security (SILS) - The Model*
- IEEE P802.10B - *SILS - Secure Data Exchange*
- IEEE P802.10C - *SILS - Key Management*
- IEEE P802.10D - *SILS - Security Management.*

Security management may be expanded to include fault, performance, and configuration management as well. In addition, IEEE P802.2 is considering an optional security sublayer for logical link control [Ref. LLC 1988].

8.2.4.5 BLACKER

On the Defense Integrated Secure Network (DISNET), the Defense Communications Agency (DCA) operates a standard end-to-end encryption (E3) system called BLACKER. A BLACKER front end (BFE) device is installed on each host-to-switch access path of all hosts used by subscribers, including terminal access controllers. The BLACKER system includes key distribution center (KDC) and access control center (ACC) hosts that automatically manage encryption keys via DISNET. BLACKER ensures that no network malfunction can permit or cause an unencrypted packet to be delivered to a host not authorized to receive it [Refs. DCA 1990; Shirey n.d.; DCA 1989b].

BLACKER is designed to satisfy Class A1 of the DoD Trusted Computer System Evaluation Criteria (TCSEC), also known as "the Orange Book," by encrypting the application data in each X.25 packet while leaving header data unencrypted for backbone use. BLACKER makes DISNET multilevel secure in three ways. First, BLACKER separates subscriber security communities from each other, allowing the DISNET communities to share one backbone. Second, on the host side, the BFE recognizes a security label on each packet, allowing DISNET to serve a multilevel secure host through one BFE. Third, BLACKER separates the entire host community on one side of the BFEs from the backbone on the other, allowing the backbone to operate at a lower, less costly security level.

The host interface to the BFE is based on standards defined for the 1983 DDN X.25 interface, and requires that the Internet Protocol (IP) be used as the next layer above X.25. The BFE presents a Data Circuit-Terminating Equipment (DCE) interface to the host. Only DDN "Standard Service" X.25 is offered at the host interface; no provisions for "Basic Service" will be made. The BLACKER interface is, however, neither a pure X.25 interface nor a mere subset of X.25, but rather must be developed from X.25 interfaces.

The BFE conforms to the following Layer 3 specifications [Ref. DCA 1989b]:

- Defense Data Network X.25 Host Interface Specification, DCA, December 1983
- Interface Between Data Terminal Equipment (DTE) and Data Circuit Termination Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks, Recommendation X.25, CCITT, 1980
- WD2512 X.25 Packet Network Interface (LAPB), Western Digital Corporation, 1989.

In the fall of 1989, a multi-Service demonstration that used BLACKER communications security and off-the-shelf gateways and routers was held in the United States. The Integrated Tactical-Strategic Demonstration Network (ITDN) used only non-developmental item components, standard data communications protocols (X.25 with TCP/IP), and existing military communications systems. ITDN interconnected automated systems at multiple echelons at widely dispersed (over 1,000 miles) locations with multiple-security-level interconnected networks.

Work similar to BLACKER is being done in other NATO nations to achieve the same ends.

8.2.4.6 Computer Security (COMPUSEC) Guidance

In order to guarantee secure handling of data and information technology systems, it is necessary to comply with security standards appropriate to the respective risks in differing operational environments. Commonly referenced security standards for COMPUSEC guidance are [Refs. CSC 1985; CSC 1985a; CSC 1985b; CSC 1987; ITSEC 1990]:

- *Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* (Yellow Book), issued by the DoD Computer Security Center (DoDCSC) in June 1985
- *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* (Yellow Book Rationale), issued by DoDCSC in June 1985
- *Department of Defense Trusted Computer System Evaluation Criteria* (Orange Book), issued under the authority and in accordance with DoD Directive 5200.28 in December 1985
- *Trusted Network Interpretation* (Red Book), issued by the National Computer Security Center in July 1987
- *Information Technology Security Evaluation Criteria (ITSEC)--Harmonised Criteria of France, Germany, The Netherlands, and the United Kingdom,* Draft, Version 1, 2 May 1990.

8.3 Status of Standards for OSI Management

Part 4 of the OSI Reference Model, *Management Framework* (ISO 7498-4) identifies three areas of OSI management: systems management, layer management, and application process management. Development of international civil standards for the overall management architecture and for systems management is being coordinated through SC21/WG4 on OSI Management. The United States has developed a draft FIPS, *Government Network Management Profile (GNMP)*, March 1991, based on this management framework.

Figure 14 identifies the classes of OSI management standards and indicates the relationships among these classes. ISO standards are identified where they apply. One standard, CD xxxxx, *Guide to Systems Management*, has not yet been completed. It will be informative, independent of the other standards, and based on the guidelines contained in the early working documents on the five management functional areas: fault, configuration, security, accounting, and performance.

Work is progressing in SC6/WG2 and SC6/WG4 on OSI management in the lower layers. A committee draft specification (CD 10733) of the elements of network layer management information has been developed [SC6 N 6413, December 1990]. SC6 has developed a set of general principles for the definition of lower layer management [SC6 N 5784, January 1990; SC21 N 4630, April 1990]. These principles extend and refine the *Guidelines for the Definition of Managed Objects* (DIS 10165-4).

8.3.1 Development of OSI Management Standards

Network management standards are being developed by SC21/WG4. TSGCE SG9 activities have been directed at identifying issues and positions of concern to military applications and influencing the direction of the work in ISO/IEC. The emphasis of the TSGCE SG9 issues has been in the area of quality of service (QoS).

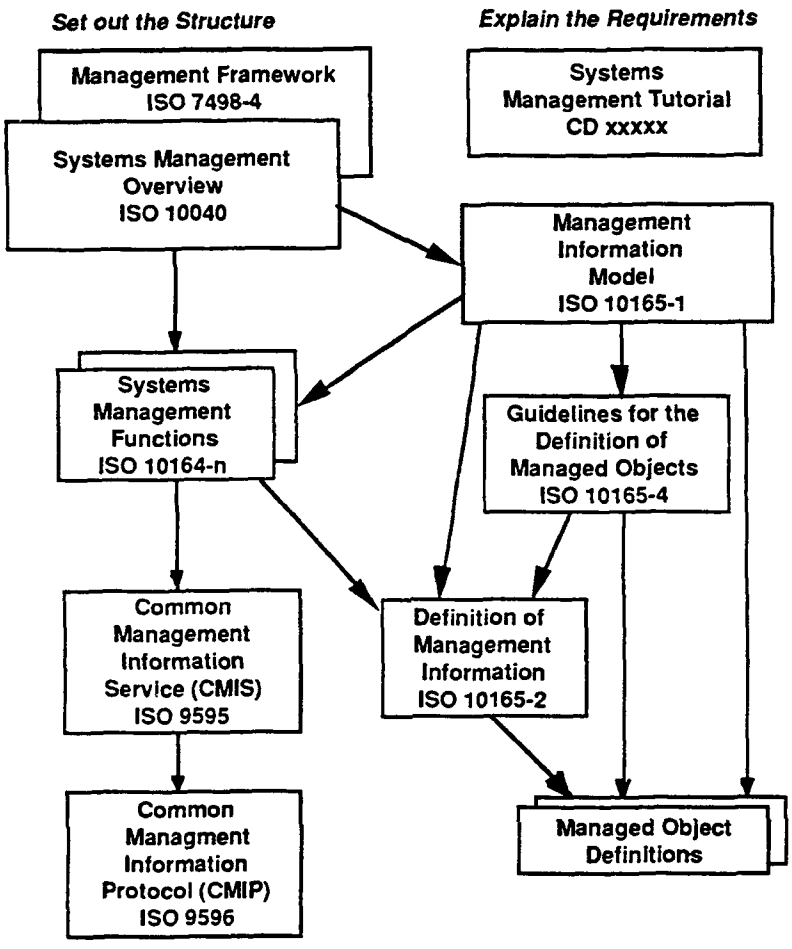
ISO Approach to OSI Management[33]

OSI Management concerns itself with three things: inter-system communications carrying management information, structure of the management information, and management functions to be undertaken by end systems. There are three ways by which management information is communicated:

- Systems Management protocols at the Application Layer
- Layer management protocols at lower layers
- Normal operation of layer protocols.

---

[33] The discussion of the ISO approach to OSI management is taken from a working paper, *Open Distributed Management Standards--The OSI Management Approach*, A. Langsford (British Standards Institute IST21/P4 Chair), July 1989, UNCLASSIFIED.



Source: ISO 10040, *Systems Management Overview*, SC21 N 6353, 4 September 1991.

Figure 14. OSI Management Standards

Systems Management is the preferred method. The others are required only because OSI Management concerns the resources and activities needed to monitor and control the open communications environment. They are not required for management outside OSI Management.

Systems Management uses a Common Management Information Protocol (CMIP) (ISO 9596) to communicate information between systems. This identifies information to be transferred and whether the transfer concerns an event report or an operation. Event reports are generated to notify another system of an asynchronous happening. Operations can monitor data and can exercise control either by assigning data values or initiating actions through a synchronous communication between end-systems.

8.3.2.1 Functional Areas

Establishing the scope of OSI Management is deemed necessary to establishing a consensus concerning the requirements. This led to identifying five functional areas for management: fault management, configuration management, accounting management, performance management, and security management. Although this approach had some advantages in resolving basic elements of functionality, it also exercised a constraining influence over the organization of work. Each functional area became concerned with its narrow perspective. This led to questions concerning the interplay between functional areas, exemplified by the following: "How does one handle standards for reconfiguring a system once a fault has been detected?"

8.3.2.2 Focus on Managed Objects

A clarification came from a shift of emphasis to the data of concern to management. Only when the data have been defined are the functions, which use the data through monitoring or controlling activities, considered. This has resulted in simpler functional standards. Each function can now stand alone rather than being bound into a composite document covering all the functions conceived as belonging to a particular area. It also enabled functions that cross the preconceived functional area boundaries to be handled in a natural manner. The result is that a particular function can be issued as a CD proposal when it is deemed to be technically stable without being unduly delayed by less mature work considered as belonging to the same functional area.

With this shift of emphasis towards data, the aim is now to identify the objects of concern to management, their attributes, and the operations that may be performed upon them. The communication services are thus the vehicles for carrying the values of attributes and a coded field identifying the operation to be carried out on a specific object, not for carrying information specifying a functional area. The approach is very close to (but not quite identical with) object-oriented methods. It has meant that work has concentrated on the management interchanges between systems performing a managing role and systems operating in an agent role manipulating internal managed objects. There has been little investigation of management exchanges between peer, managing entities, or of the management procedures invoked by managers.

The object-oriented approach has enabled OSI Management experts, in collaboration with those developing standards for various OSI layer protocols, to identify classes of managed objects and commonly used attributes. This in turn has promoted the development of a standard naming scheme through which to identify instances of object classes. The naming scheme is based on that used for Directory services. This facilitates the use of directories, conforming to ISO 9494 (CCITT Recommendation X.500), when management makes references to OSI objects.

A March 1991 paper entitled *Proliferation of Managed Objects* [SC21 N 5756] notes that many groups within CCITT and ISO are developing managed object definitions without the benefit of overall coordination. It suggests that this problem can only be solved by taking an overall view of managed object definition activities that requires a global management information authority, capable of influencing the activities of at least all the standards bodies.

8.3.2.3 Distributed Processing Aspects

The shift of emphasis has been further beneficial in bringing into relief the fact that some management has been recognized as a distributed processing activity with its own managed objects. For example, the "event forwarding discriminator" takes management decisions about what should be done to asynchronous notifications flowing from OSI managed objects.

Thus, OSI Management standards are beginning to reveal explicitly what has always been known by management specialists; i.e., management is a distributed processing activity and has much in common with other distributed processing activities. Management's distinguishing feature is that the scope of the distributed application is limited to manipulating the information processing, storage, input/output, and communications environments themselves. Hence, particular attention is paid to controlling the permission to obtain and act upon system information.

8.3.2.4 Results of Work in OSI Management

OSI Management has had a long learning process. The lessons learned have been valuable and appear to be applicable to management in general. The following steps are important in creating new management standards:

- Establish a requirement, since this sets the scope for the standard.
- Identify the objects of concern to management through which that requirement is realized. With identification of the objects goes the identification of their attributes, operations, and of any objects that can be encapsulated within the identified objects.
- Establish a naming scheme for the objects and their attributes.
- Identify management procedures that, through monitoring and controlling activities, meet the requirement. Where a procedure requires inter-system communication, the communication is provided through the use of CMIP.

The Structure of Management Information (SMI) standards for OSI set out rules for specifying managed objects, attributes, and their operations. Although detailed investigations remain to be carried out, first impressions are that these rules are applicable to all aspects of management. However, it could be that further investigation will reveal places where detail may need to be refined.

OSI Management standards identify a number of attributes that are common to many management activities (e.g., counters, gauges, thresholds, status, logs) and many events that have general applicability (e.g., fault reporting, exception handling). Though not yet as well developed, it appears that OSI management procedures for testing, accounting, managing, and accessing logs have the same general applicability. Adopting this work as a basis and providing extensions where required will (a) obviate rework, (b) help limit the unnecessary proliferation of managed standards, and (c) help reduce the diversity of management software that suppliers have to write to support open distributed management.

In communicating related sets of operations to be performed or invoking remote operations, a managing system may wish to assert relative priorities to various tasks. If and how priority should be handled and communicated through CMIP is an open question.

8.3.2.5 Conformance

SC21/WG4 has only begun to describe how conformance statements should be constructed so that they apply meaningfully to OSI Management. The one exception is CMIP for which, being a conventional Application Layer protocol, the task of generating conformance statements is straightforward.

The main problem is that OSI Management is concerned not just with "how" something is communicated (CMIP) but "what" is communicated (SMI) and "why" (management functions and procedures). Whereas conformance and particularly the demonstration of conformance through conformance testing is readily applied to CMIP since the communication is visible and monitorable, the "what" and "why" require that conformance testing be applied to activities taking place within end systems. There is a need to investigate whether the approach of the OSI Conformance Testing Methodology is applicable or whether another method needs to be developed. Any method must recognize the distributed nature of management operations and so would probably be appropriate to other classes of distributed processing enterprise.

Consideration of conformance to management standards, with the wider scope of open distributed processing, could have the beneficial effect of clarifying the conformance requirements, conformance clauses, PICS proformas (or the equivalent), and profiles for OSI Management standards [Ref. Langsford 1989].

8.3.3 ISO Standards for OSI Management

8.3.3.1 Status of OSI Management Standards

The following are the standards documents being developed in ISO by SC21/WG4 for OSI management:

- *OSI Management Framework,* ISO 7498-4, November 1989. The Framework document provides an architectural overview (CCITT X.700).
- *Systems Management Overview,* ISO 10040, August 1991 [SC21 N 6353]. The *Overview* document provides more detailed architectural concepts. It defines the architecture for systems management, which is management using Application Layer protocols for communication, and it sets out the scope of the other systems management standards.
- *Systems Management,* ISO 10164:
  - Part 1: *Object Management Function,* ISO 10164-1:1990 (CCITT X.730).
  - Part 2: *State Management Function,* ISO 10164-2:1990 [SC21 N 4856] (CCITT X.731).
  - Part 3: *Attributes for Representing Relationships,* ISO 10164-3:1990 [SC21 N 4857] (CCITT X.732).
  - Part 4: *Alarm Reporting Function,* ISO 10164-4:1990 [SC21 N 4858] (CCITT X.733).
  - Part 5: *Event Report Management Function,* ISO 10164-5:1990 [SC21 N 4860] (CCITT X.734). Name changed from Management Service Control Function.
  - Part 6: *Log Control Function,* ISO 10164-6:1990 [SC21 N 4862] (CCITT X.735).
  - Part 7: *Security Alarm Reporting Function,* ISO 10164-7:1990 [SC21 N 4874] (CCITT X.736).
  - Part 8: *Security Audit Trail Function,* DIS 10164-8, 8 July 1991 [SC21 N 6283]--IS status in 1992 (CCITT X.740).
  - Part 9: *Objects and Attributes for Access Control,* CD 10164-9.2. 11 October 1991 [SC21 N 6451] (CCITT X.741). Second CD failed ballot (cannot progress to DIS until CD 10181-3 on access control framework is issued).
  - Part 10: *Accounting Meter Function,* CD 10164-10.2, 24 July 1991 [SC21 N 6296] (CCITT X.742). Is status expected early 1993.
  - Part 11: *Workload Monitoring Function,* CD 10164-11.2, 11 October 1991 [SC21 N 6452] (CCITT X.739). Failed second CD ballot.
  - Part 12: *Test Management Function,* CD 10164-12, 31 May 1991 [SC21 N 5517] (CCITT X.745). IS status expected December 1992.
  - Part 13: *Summarization Function,* CD 10164-13, 31 May 1991 [SC21 N 5519] (CCITT X.738). The October 1991 editing meeting recommended re-balloting as a second CD. IS status originally expected December 1992.
- *Structure of Management Information (SMI),* ISO 10165:
  - Part 1: *Management Information Model,* ISO 10165-1, 15 November 1991 [SC21 N 6351] (CCITT X.720).

- Part 2: *Definition of Management Information*, ISO 10165-2, September 1991 [SC21 N 6363] (CCITT X.721).
- Part 3: Cancelled in November 1989 by recommendation of SC21 and incorporated into Part 2.
- Part 4: *Guidelines for the Definition of Managed Objects*, ISO 10165-4, 15 November 1991 [SC21 N 6359] (CCITT X.722).
- Part 5: *Generic Management Information*, ISO 10165-5, August 1991 [SC21 N 6360] (CCITT X.734) (previously entitled *Generic Managed Objects)*.
- Part 6: *Implementation Conformance Statement Proformas*, CD 10165-6, July 1991 [SC21 N 6027]. IS status expected early 1993.
- Part 7: *Management Information Register (MIR) and Registration Procedures*, WD 10165-7 [SC21 N 5687, 14 February 1991]. CD expected July 1992; IS status expected December 1993.

• *Common Management Information Service (CMIS) Definition*, ISO 9595: 1991 (E), 7 January 1991 [SC21 N 5302] and [SC21 N 5582 Rev., 21 January 1991] [CCITT X.710]; CCITT and ISO/IEC are collaborating on CMIS and CMIP. CMIS defines services for acting on an object and includes creation and deletion. Services can apply to values from a set of attribute values; the attribute values can have the structure of a table, so that services can affect entries, entire rows, and entire columns (CCITT X.710).

- DAD 1: *Cancel/Get Service*, February 1990 [SC21 N 3876].
- DAD 2: *Add/Remove Service*, February 1990 [SC21 N 3877].
- CDAM 3: *Support of Allomorphism*,[34] November 1990 [SC21 N 4966].
- DAM 4: *Access Control*, 8 July 1991 [SC21 N 6286]; CMIS has an access control field--the issue is how to use it. IS status expected June 1992.
- WDAM 5: *Enhanced Funtionality*, July 1991 [SC21 N 6039]; PDAM expected in 1993.

• *Common Management Information Protocol (CMIP) Specification*, ISO 9596-1, 7 January 1991 [SC21 N 5303]; CMIP defines peer protocols for layer services between Systems Management entities (CCITT X.711).

- DAD 1: *Cancel/Get Protocol*, February 1990 [SC21 N 3878].
- DAD 2: *Add/Remove Protocol*, February 1990 [SC21 N 3879].
- PDAM 3: *Support of Allomorphism*, July 1990 [SC21 N 4967].
- PDAM 4: *State Tables for CMIP*, January 1990 [SC21 N 4058] (Project cancelled , July 1991).
- WDAM 5: *Enhanced Funtionality*, July 1991 [SC21 N 6039]; PDAM expected in 1993.

• *Common Management Information Protocol (CMIP) Specification*, DIS 9596-2, *PICS Proforma*, 8 July 1991 [SC21 N 6287] (CCITT X.712). IS status expected June 1992.

---

[34] An object in a refined class (i.e., a subclass) of a class definition (e.g., a modem) could behave in certain situations as if it were the parent. This characteristic, called polymorphism or more recently allomorphism, would support backwards compatibility. The way in which an object would respond would depend on how it is addressed. This work will lead to a change in both CMIS and CMIP.

- *Telecommunications and Information Exchange Between Systems - Elements of Management Information Related to OSI Network Layer Standards*, DIS 10733, January 1991 [SC21 N 5560].
- *Specification of the Elements of Management Information Related to OSI Transport Layer Standards* (DIS 10737). IS status expected June 1992. A liaison statement from SC6/WG4 to the ULA group cited DIS 10737 as an example of a layer management specification. SC6/WG4's examination of DIS 10737 discovered two problems with the managed-object structure described in the document that seem to contradict the Reference Model.[35]

As part of the Summarization Function (CD 10164-13) work, the Performance Management (PM) Group of SC21/WG4 was requested to develop a general model for scheduling in management functions. As a result of their work, the PM group has recognized that a general scheduling model has wider applicability than performance management and recommends that this work be progressed independently of the Summarization Function [Ref. SC21 N 5545 1990]. The Performance Management Working Document is currently in its seventh draft [SC21 N 6303, 29 July 1991].

In November 1990, it was agreed that after Version 2 of CMIS and CMIP there will be no further releases (either in the form of addenda or completed standards) that could affect interoperability before 1994 [Ref. SC21 N 5546 1990].

8.3.3.2 New Work Items

Work in SC21/WG4 on OSI management is continuing on several new parts for *Systems Management*, DIS 10164.

- WD 10164-cdt: *Confidence and Diagnostic Test Classes*, June 1991 [SC21 N 6307], second working draft (CD text expected December 1991, DIS late in 1992, and IS late in 1993).
- WD 10164-X: *Software Management Function*, July 1990 [SC21 N 6040], expected to be an addendum to ISO 10165-2 (CD text expected in June 1993).
- WD 10164-A: *Time Management: Representation of Time*, July 1990 [SC21 N 4953] deals with the distribution and synchronization of time in a distributed environment. CD expected June 1993.
- WD 10164-sm: *Systems Management Relationship Model*, August 1990 [SC21 N 4948; JTC1 N 962]--expected to use entity-relationship modelling (CD text expected in December 1992).
- WD 10164-rtm: *Response Time Monitoring*, August 1990 [SC21 N 4949; JTC1 N 963] (CD text expected in December 1993).
- WD 10164-s: *Scheduling Function*, June 1991 [SC21 N 6021]. (CD text expected in June 1992, DIS in early 1993).
- WD 10164-pm: *Performance Management*, 29 July 1991 [SC21 N 6306].

---

[35] *Liaison to SC6/WG4, SC21/WG6, SC21/WG4, and SC21/WG1 on Managed Object Structures*, SC21 N 6006, 24 July 1991.

New work items include:

- *Systems Management Tutorial*, 20 June 1991 [SC21 N 6046; JTC1 N 957] (planned to be a new technical report) (CCITT X.702). CD provisionally expected December 1993. At the May 1991 meeting, some members of WG4 expressed concern that scarce resources will be diverted from other Systems Management work to develop this report. WG4 has therefore asked that National Bodies confirm at its next meeting in May 1992 that there is sufficient support to progress this project. [Ref. SC21 N 6214 1991]
- *Extended Systems Management Architecture*, August 1990 [SC21 N 4943; JTC1 N 958] (planned to be a new part of ISO 10040). CD expected in June 1992. Three NWI proposals are part of this architecture:
  - *Management Domains*, WG4, [SC21 N 6047], June 1991.
  - *Management Knowledge Management*, WG4, [SC21 N 6048], June 1991.
  - *Synchronization*, WG4, [SC21 N 6049], June 1991.
- *Formal Descriptions of CMIP*, July 1990 [SC21 N 4947].
- *Managed Object Conformance Statement (MOCS) Proformas*, 14 February 1991 [SC21 N 5686]--to provide requirements and develop a standard specification technique (template) for MOCS proforma, thus helping to ensure their completeness, consistency, and ease of use. MOCS proformas are analogous to PICS proformas, but apply to managed object definitions as opposed to protocols. Designed to be a new part of DIS 10165-4.
- *Management Information for the OSI Upper Layers* [SC21 N 4108] (approved by JTC1 in May 1990) [Ref. SC21 N 4912 1990]. In May 1991, SC21/WG6 issued a request for comment on requirements for this NWI. [Ref. SC21 N 6067 1991]
- *General Model for Relationship Management*, 20 June 1991--to support DIS 10164-3, which addresses three methods of representing relationships: by name binding, by attributes, and by managed objects [SC21 N 6041]. CD status expected in December 1992 and DIS status late in 1993. This paper proposes a single model of relationships among managed objects within the scope of the OSI management information model.
- *Changeover Function*, WG4 [SC21 N 6024].

WG4 proposed and JTC1 accepted a NWI, *Enhanced Event Management and Log Control* [SC21 N 6035, 1 July 1991] to specify the behavior to be exhibited with a system that may not be able to transmit event reports immediately after being processed by the event forward discriminator, such as when all systems to which event reports are to be sent are not responding. The NWI will also explore possible (optional) mechanisms for managing the storage and deferred delivery of such event reports. It is planned to be part of ISO 10164.

Another NWI from SC21/WG4 is *Development of Enhanced Functionality for CMIS/P* [SC21 N 6039, 1 July 1991]. This NWI would provide enhanced support from CMIS/P for new work on the Extended Systems Management Architecture and the Systems

Management Relation Model. Although the new work item qualified for acceptance in the JTC1 work program, several National Bodies have raised concerns regarding the scope and requirements of the work item. Therefore, SC21 is requested to reevaluate the timeliness of this project and the wording of the scope.

8.3.3.3 Systems Management, DIS 10164

DIS 10164, *Systems Management,* establishes user requirements for each management function, establishes a model that relates the services and generic definitions provided by this function to user requirements, defines the services provided, defines generic notification types and parameters documented in accordance with the guidelines for the definition of managed objects, specifies the protocol necessary to provide the service, specifies the abstract syntax necessary to identify and negotiate the functional units in the protocol (if necessary), defines the relationship between the services and SMI operations and notifications, specifies compliance requirements placed on other standards that make use of these generic definitions, defines relationships with other systems management functions, and specifies conformance requirements. DIS 10164 does not define implementation aspects, specify the manner in which management is accomplished, define interactions that result in the use of management functions, specify services for establishment and normal or abnormal release of a management association, or define managed objects. The major management functions addressed in SMI are defined in Table 17.

DIS 10164 defines particular systems management functions and how these are achieved by use of CMIS. ASN.1 is the notation used to express the abstract syntax of the data elements associated with managed object, attribute, event, and action definitions that shall be carried in CMIP.

Table 17. Definitions of OSI Management Functions From DIS 10164

- Object management--ability to create, delete, examine, and change sets of management information that describe parts of the OSI environment.
- State management--the ability to examine and be notified of changes in state, to monitor overall operability and usage of objects in a consistent manner, and to give or withhold permission for the use of specific objects.
- Relationship management--the ability to examine the relationships among various parts of the system, to see how the operation of one part of the system depends upon is depended upon by other parts.
- Alarm reporting function--reports alarms, errors, and related information. Malfunctions will range in severity from minor, where a minimal impact upon the quality of service to the user occurs, to major, where it is no longer possible to provide the quality of service requested (or promised to) the service user.
- Event report management--the ability to specify conditions to be satisfied by a potential event report relating to a particular managed object or a set of managed objects, in order to be sent to specified destinations.
- Log control--the ability to preserve information about events that may have occurred or operations that may have been performed by or on various objects.
- Security alarm reporting function--provides such capabilities as the means to receive notifications of security-related events, alerts of any misoperations in security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security. The standard provides notifications that include reporting of the clearance of fault conditions.
- Security audit trail--the ability to maintain a record of security-related events that occur in the management domain and to review and analyze these events to detect security breaches, malfunctions, and effectiveness of the security services and mechanisms that are implemented pursuant to the security policy.
- Access control--provides consistent levels of granularity necessary to a homogeneous control policy, preventing management notifications from being sent to unauthorized recipients, preventing initiators from having access to management operations, and protecting management information from unintended disclosure. Various levels of access control will be supported: some users may be given read and write access to specific attributes while other users have only read access or no access; some users may be granted access only to specific managed objects; and some users may not be allowed to establish management communications at all.
- Test management function--remote control of tests involving real open systems and the specification of tests that exercise OSI resources.
- Confidence and diagnostic test classes--defines service in the form of test classes that are required in order to investigate the ability of a resource to perform its allotted function, the ability of the communications mechanism to make a connection between a number of open systems and to transfer data without modification between a number of open systems, the integrity of a protocol, and the effect of increased utilization of a resource.
- Workload monitoring function--may be used by an application process in a centralized or decentralized management environment to interact to satisfy such requirements as:
  - Definition of statistical monitoring tools to derive metrics to characterize performance
  - Definition of a monitoring function that provides metrics of the workload, workload rejected, and resources used
  - Specification of mechanisms to obtain these metrics
  - Specification of notifications to be generated when these metrics exceed threshold values, and the ability to include additional performance information into these notifications
  - Specification of mechanisms to control the operation of this function, for example to initiate and to terminate monitoring
  - Scheduling of metric monitoring over a specified period of time.
- Summarization function--measures throughput, time delays, message round trips, response times, and other measures of congestion and resource utilization for performance monitoring and statistics calculated across managed objects, not over time (see Workload Monitoring Function).

8.3.3.4 Major Remaining Issues for DIS 10164

The following technical issues are not yet addressed by DIS 10164 [Ref. SC21/WG4 1989]:

- Renaming managed objects--requirements for renaming managed objects, including classes to be renamed, conditions under which rename would be permitted, constraints on renaming objects in standardized procedures, and changes that need to be coordinated to make a renaming operation consistent and meaningful.
- Service access control--mechanism to address the need for individual open systems to have the option of protecting themselves against the invocation of services that would forcibly change existing configured relationships among managed objects.
- Startup and shutdown--addressing the requirement to manage the state of an object as regards invoking startup (or initialization) and shutdown.

Specific concerns regarding Part 9 of CD 10164, *Objects and Attributes for Access Control,* are that the document is technically flawed, the technology in the document is already obsolete, and the document contents are inconsistent with its scope. Moreover, Part 9 needs alignment with the *Access Control Framework*, CD 10181-3. [Ref. X3 1991j]

8.3.3.5 Structure of Management Information (SMI) (DIS 10165)

The purpose of DIS 10165-1, *Management Information Model*, is to give structure to the management information conveyed externally by systems management protocols and to model management aspects of the related resources (e.g., an X.25 protocol machine). Managed objects are abstractions of data processing and data communications resources (e.g., protocol state machines, connections, modems) for the purposed of management. It is the attributes, operations, and notifications of managed objects that are visible to management, whereas the internal functioning of the managed object (i.e., the resource it represents) is not otherwise visible to management. DIS 10165-1 describes the model of management information in terms of managed objects and the set of operations that may be performed upon them and notifications that they may generate. It also defines, using object-oriented principles, key concepts such as inheritance, allomorphism, containment, and naming as they relate to managed objects.

ISO 10165-2 defines the generic object classes, support managed object classes, abstract attribute types, attributes types, notifications types, action types, parameter types, and associated abstract syntaxes that may be applicable to a number of different standards. It also specifies compliance requirements placed on other standards that make use of these definitions.

ISO 10165-4 defines the management information that is to be transferred or manipulated by means of the OSI management protocol and the managed objects to which that information relates. DIS 10165-4 provides developers of managed object class

definitions with the information and documentation tools that are required in order to produce complete managed object class definitions.

ISO 10165-5, *Generic Management Information*, provides developers of OSI specifications that contain managed object definitions with generic definitions of managed object classes that will:

- Provide common superclass definitions from which layer- or resource-specific object class definitions may be derived
- Assist with the development of common elements of object class definitions across multiple layers or components of layers
- Reduce duplication of effort in other working groups by identifying commonly useful definitions.

WD 10165-7, *Management Information Register (MIR)*, defines a mechanism for registering system management information and procedures for maintaining the register. It would contain information describing:

- Support managed object classes
- Generic managed object classes
- Definitions of attribute types, support objects, system management notifications, system management actions, name bindings, and management information parameters.

While it was agreed that progression of this project is of the highest priority in Systems Management, SC21/WG4 was unable to resolve the National Bodies' comments on the scope of the project at its meeting in May 1991 [Ref. SC21 N 6215 1991]. The German National Body has suggested using the Directory system (ISO 9594) as the MIR [SC21 N 5891].

8.3.4 Telecommunication Management Network (TMN)

The Telecommunication Management Network (TMN) is a concept developed by CCITT (Recommendation M.30) to manage a telecommunication network (e.g., the public telephone network or an ISDN). A TMN is conceptually a separate network that interfaces a telecommunications network at several different points to receive information from it and to control its operations. A TMN may use parts of the telecommunications network to provide for its own communications.

Architecturally, the TMN functions are divided into three blocks:

- Operation System Function (OSF) that processes the information related to telecommunication management to support or control the realization of various telecommunication management functions.
- Mediation Function (MF) that acts on information passing between Network Element Functions (see below) and OSFs to achieve smooth and efficient communication. The main MFs are communication control, protocol

conversion, data handling, communication of primitives, processing involving decision making, and data storage.

- Data Communication Function (DCF) that provides the means to transport information related to telecommunication management between functional blocks.

The three functional blocks can communicate with two external blocks. One is the Network Element Function (NEF) that communicates with a TMN for the purpose of being monitored and/or controlled. The other is the Workstation Function (WSF) that provides the means for communications between function blocks (OSF, MF, DCF, and NEF) and the user. The current draft of the *NATO C3 Architecture Communications Subsystem* (July 1989) indicates that the management of the NATO ISDN (see Section 15.3.6) will be based on the TMN concept [Ref. Man 1990]. The NATO Tactical Communications Architecture proposed by TSGCE SG11/PG6 is also based on TMN (see Section 4.4).

8.3.5 Military Concerns in Network Management

Some concerns in the OSI management area involve the direction and support of work being done by ISO for Quality of Service (QoS) and multipeer/multiaddressing. Both of these areas were reassessed in 1989 due to lack of support from the nations. Specifically, a formal question[36] has been raised and put to a ballot on the need for a framework for quality of service within the ISO standards. Since these areas have been found to be priority items for achieving military requirements, it is important for the Nations individually and collectively to express their support for additional work in these standards areas.

The Ad Hoc Working Group on OSI Management (AHWG-OM) of TSGCE SG9 has been formed to address OSI management issues for NATO.[37] The major standing document of the AHWG-OM is *NATO Requirements for Open Systems Management* [Ref. AHWG 1990]; some key elements are the following:

- Part 1: *Rationale and Objective* (of which Section 7 is Military Features and Their Impact on OSI Management and Annex A.2 is the Work Plan), 28 June 1990
- Annex H: *Notes Concerning the Quality of Service Issue*, Third Draft, 9 February 1990
- Appendix 4, *Requirements for a Network Management Broadcast Facility*, 1 May 1990.

---

[36] ISO/IEC JTC1/SC21/WG1 Question 62: "Is Quality of Service an architectural issue which needs overall guidance and consistent approach across all layers?" Balloting closed in May 1989.

[37] The work TSGCE SG9 working groups is discussed in Section 15.3. The AHWG-OM is addressed in Section 15.3.5.

8.3.6 Quality of Service (QoS)

In the framework of OSI, QoS provides the capability to measure the service level provided by the communications service provider and the means to request a target service from the communications service provider. QoS parameters now used in ISO standards[38] include transit delay and priority.

SC21/WG1 posed Question 62 (Q62) in 1989 to query whether a QoS Architecture was necessary since such an architecture would require modification to the OSI Reference Model. The first step to developing such an architecture would be defining the components of a QoS Framework. A concern of several national bodies in WG1 is that a new QoS Architecture would destabilize the existing standards. At the May 1990 SC21 Plenary in Seoul, WG1 did not progress the QoS Framework as a new work item. In May 1991, WG1 reported to SC21 the final answer to Q62, saying that there was indeed a need for a QoS framework [Ref. SC21 N 6158 1991]. In June 1991, it was again proposed as a new work item. [Ref. SC21 N 6159 1991]

The AHWG-OM (see Section 15.3.5) has identified [Refs. WG/1 1990; AHWG 1989] the following deficiencies and requirements relative to QoS:

- Only static QoS parameters have been defined--the relationship of various QoS parameters to each other and actions to take upon dynamic change in QoS are not yet supported.
- A tight coupling between QoS and communications services is needed to support applications in areas such as military and real-time process control and high assurance of message delivery. Specifically, this means that applications need:
  - Capability to clearly express the QoS requirement to the underlying communications service
  - Notification of changes in QoS
  - Close monitoring of the QoS
  - Assurance that QoS is maintained in a deterministic manner.
- While QoS's need of the layer services have led to protocol definitions that include parameters for specifying QoS, no syntax or semantic meaning of those parameters has been defined.

Further, the AHWG-OM has recommended that:

- An overall framework for OSI QoS be developed and, specifically, ISO/IEC SC21/WG1 raise the priority of QoS discussions in this area.
- QoS be expanded to provide five functions: establishment, monitoring, maintenance, notification of change, and negotiation.
- The definition of QoS be modified to include the following four classes of QoS parameters:

---

[38] ISO/IEC references to QoS are in Layer 3 (ISO 8438), Layer 4 (ISO 8072, 8073), Layer 5 (ISO 8326), Layer 6 (ISO 8822), and Layer 7 (ISO 8649, 8650, 8571-3).

- Quality of addressing--the correct assignment of addresses to the originator and the recipient.
- Quality of message--the reliability of message delivery against data loss, data corruption or insertion, misdelivery, duplicate delivery, or out-of-sequence delivery.
- Quality of timeliness--the delay of transferring information across a communications service, including specification of requirements on time limits for delivery of a message. The latter may be in terms of the time after which the message is no longer valid, allowable delay in the transfer, and the action to take on failure to meet the criteria.
- Quality of confidentiality--the ability of the system to protect its resources from unauthorized use and to prevent unauthorized interception of information relative to the transfer of a message. Clearly this quality overlaps security requirements.

The AHWG-OM in its meeting in June 1990 recommended three steps for progressing work on QoS: (1) establish an ad hoc working group on QoS in TSGCE SG9 to define QoS requirements and a QoS Framework; (2) apply the QoS Framework in other SG9 working groups; and (3) provide additional information to ISO and other standards bodies on the need for QoS. AHWG-OM recommended that the proposed framework consider the application QoS parameters, the application actions (procedures used by applications in processing QoS information), and QoS facilities for establishment, monitoring, maintenance, notification, and negotiation of QoS [Ref. AHWG 1990a].

A key background paper for QoS is *Management Requirements Arising from a NATO Study of Quality of Service* [Ref. Kennedy et al. 1989]. This paper identifies QoS requirements in such areas as specification, establishment, application actions, monitoring, maintenance, notification, negotiation, information flow, and applicability. It also addresses the QoS framework, information model, and interaction model. Four QoS parameters are identified: addressing, message, timeliness, and confidentiality. The June 1990 recommendations of the AHWG-OM to SG9 were based, in part, on material described in this paper.

At the Arles meeting of SC21 in May 1991, a new work item on QoS Framework was approved. The UK has suggested [Ref. TSGCE 1991] in the September 1991 meeting of TSGCE SG9/WG2 that a technical re be prepared and noted that NATO is a major source of work in this area. There is clearly interest in SG9 for QoS but apathy in SC21. The UK recommendation was that a Type 2 technical report be drafted; such a document applies to a particular standard and can be referenced in other documents, including full standards. It could simply be a guide or could itself become a standard, if necessary, subject to normal balloting procedures.

The UK MOD/Industry Workshop on Quality of Service has been exploring QoS issues in the military context and their impact on OSI standards. The workshop aims to provide technical advice and backup to NATO efforts in promoting the recognition of QoS issues in OSI and to feed military requirements directly into OSI via the British Standards Institute (BSI). The workshop is chaired by Ian White, the Chairman of SG9, and is

therefore in an excellent position to channel NATO interests into OSI. At the September 1991 meeting of the workshop, it was agreed to appoint an editor for a QoS technical report, the first draft of which will consist of a fusion of ideas and concepts explored in earlier submissions to the workshop. Two working groups have been established, one of framework and structure and one on rationalization of QoS parameters.

8.3.7 Special Interest Groups for OSI Management

A number of special interest groups have been formed to promote standardization of OSI management. These include [Ref. AHWG 1990b]:

- Network Management Experts Group--formed within EWOS with plans to meet four times per year
- Network Management Forum (NMForum)--developing specifications that will be demonstrated in September 1990 during the first Network Management Showcase
- NIST Network Management Special Interest Group (NMSIG)--developing specifications for the *Stable Implementor's Workshop Agreements* with a target date of December 1990. The 1990 version will define, in coordination with EWOS and the NMForum, managed objects for LANs including FDDI, X.25, and ISDN. Additional managed objects would be defined in 1991 for Layer 3-7 protocols and routers and in 1992 for applications, operating systems, and database management systems.

8.3.8 ECMA Model for Management

In January 1987 the European Computer Manufacturers Association (ECMA) established [Ref. ECMA 1987] an abstract model for the management aspects of OSI. The framework provided by ECMA is designed to form the basis for the definition and specification of services and protocols that enable the planning, organizing, supervising, and controlling of the communication service that forms a part of a distributed information processing system. In this context, OSI management is defined as the collection and interchange of information necessary for the management of those aspects of open systems that are relevant to Open Systems Interconnection. The abstract model addresses standardization in two areas:

- Semantics of the management information transferred or extracted from the management information base (where the structure of the information within the management information base is viewed as a local matter and not subject to management standardization)
- Services and associated protocols for the transfer of management information between open systems; this requires that both the syntax and semantics of the information transferred be specified.

ISO standards for OSI network management are being developed by SC21/WG4; they are discussed in Section 8.3.3.

8.4 Standards for Conformance Testing

Conformance testing is crucial to the achievement of OSI to ensure comparability of test procedures and results by different test centres. Conformance testing is defined by the United Kingdom's National Centre for Information Technology as:

> the testing of a product against a published standard in order to determine the degree of conformance with that standard [Ref. Pink et al. 1991].

Standardization of conformance test suites needs to be based on a standard testing methodology and approach to test suite specification, which is reflected in ISO 9646, *OSI Conformance Testing Methodology and Framework (CTMF)*. Work has already begun in standardizing test suites based on ISO 9646 for X.25 terminals, the connection-oriented transport protocol (ISO 8073), MHS, FTAM, ACSEs, session, and presentation protocols. A detailed description of OSI conformance testing is provided in [Ref. Rayner 1987]. ISO/IEC work in conformance testing is done by SC21/WG1.

ISO 9646 is being developed in seven parts, five of which have achieved IS status. The seven parts, together with the current annex and amendment, are as follows:

- ISO 9646-1, Part 1: *General Model,* May 1991 [SC21 N 5865] (CCITT X.290)--merged text incorporating PDAM 1 and PDAM 2 awaited.
- ISO 9646-2, Part 2: *Abstract Test Suite Specification,* May 1991 [SC21 N 5867] (CCITT X.291)--merged text incorporating PDAM 1 and PDAM 2 awaited.
- Annex to ISO 9646-2: *Guidelines for PICS Proformas* [SC 6 N 6243, 23 October 1990] is also under development (see 8.4.1)
- ISO 9646-3, Part 3: *The Tree and Tabular Combined Notation (TTCN),* October 1991 (CCITT X.292)
- ISO 9646-3 PDAM 1, *Amendment on Extensions to TTCN Including Parallel Tree,* March 1990 [SC21 N 4219, December 1989] (PDAM expected November 1991; DAM expected June 1992; AM expected June 1993)
- ISO 9646-4, Part 4: *Test Realization,* May 1991 [SC21 N 5869] (CCITT X.293)--merged text incorporating PDAM 1 and PDAM 2 awaited.
- ISO 9646-5, Part 5: *Requirements on Test Laboratories and Clients for the Conformance Assessment Process,* May 1991 [SC21 N 5871] (CCITT X.294)--merged text incorporating PDAM 1 and PDAM 2 awaited.
- CD 9646-6, Part 6: *Protocol Profile Testing Specification,* June 1991 [SC21 N 6177] (DIS expected March 1992; IS in December 1992)
- WD 9646-7, Part 7: *Requirements and Guidelines on Implementation Conformance Statement (ICS) and ICS Proformas,* June 1991 (SC21 N 6196) (CD expected May 1992).

The primary areas for standardization of conformance testing in the near future are: multi-protocol (profile) testing, multi-party test methods, additional features in TTCN and

multi-test case tables, the nature of profile conformance testing and configurability, and implementation conformance statements. Specifically,

- *Protocol Profile Conformance Testing Methodology* (PPTM) was a proposal for a new work item, January 1990 [SC21 N 4217; SGFS N 9]. It is now its second working draft [SC21 N 5075, June 1991]. It will extend the OSI conformance testing methodology and framework (DIS 9646) to make it applicable to OSI protocol profiles as well as base protocols. This standard will supersede TR 10000-1 as far as conformance aspects are concerned. In addition to Part 6 of ISO 9646, PDAMs to parts 1,2, 4, and 5 of ISO 9646 on PPTM were issued in June 1991.
- *Multi-party test methods* addenda to parts of DIS 9646 [SC21 N 4218, January 1990] will define the main requirements concerning MPTM and a multi-party test architectural model. The model will be used to map abstract test methods on which to base the development of abstract test suites and means of testing for the various multi-party protocols and multi-party testing configurations using more than one protocol or more than one channel. A joint meeting with CCITT SG VII was held February 1991 from which a WD emerged [SC21 N 5076], and PDAMs to parts 1, 2, 4, and 5 of ISO 9646 were issued in June 1991. Also in June 1991, WG1 circulated a document entitled *Multi-Party Testing for Connectionless Relay and Routing Protocols* for study and comment. [Ref. SC21 N 6202 1991]
- Work on *TTCN extensions* has already begun. As an addendum to DIS 9646-3, *TTCN Extensions* introduces the notion of parallelism in order to ease the writing of test cases, provide a language means to describe explicitly the cooperation of (distributed) components of a test architecture, and to make TTCN a test notation that covers the aspects of a multiparty test methodology. WD text was distributed for comment in March 1990, and CD text was issued in June 1991.
- *Formal Methods in Conformance Testing (FMCT)* is a proposal for a new work item, January 1990 [SC21 N 4215]. A WD was issued in July 1991 and CD text is expected in June 1994. A joint meeting with CCITT was held in October 1991 to progress the WD focussing on terminology, consistency between FMCT and CTMF concepts, relationship between specification, implementation and testing, FMCT concepts interpretation with FDTs, test generation methods, and specification style for testability. [Ref. SC21 N 6423 1991]

Additional topics to be addressed for conformance testing in 1991-1992 are ISDN and multimedia concerns, application of formal methods, and protocols for test support.

SC21/WG1 has noted concerns [Ref. SC21 N 4187 1989] about the available resources and direction of work on upper layer conformance testing. Work has slipped 2 years on abstract test suites for FTAM and 3 years for embedded test suites for ACSE, Presentation Layer, and Session Layer. There is an imbalance between work on the basic methodology and that applied to the actual conformance tests, specifically on abstract test suites.

The status of Abstract Test Suite (ATS) work as of June 1991 is as follows:

- SC21 N 3665, *Specific Partial ATS for Responder Tests*, submitted by NCC (UK). This test suite will be aligned with the international standard version of TTCN. Additional contributions are expected in October 1991. CD text is expected in October 1992; DIS text expected October 1993; and IS text expected October 1994.
- SC21 N 7018, *Common Partial Embedded ATS*. CD text is anticipated May/June 1992.
- SC21 N 5903, *Presentation Connection-Oriented ATS, Common Partial ATS*. At its meeting in May 1991, WG6 decided not to produce a WD until the IS text of TTCN is produced [Ref. SC21 N 6115 1991]. CD expected June 1992; DIS expected June 1993; IS expected June 1994.
- SC21 N 6116, *Annex to the WD Embedded Abstract Test Suite for the Presentation Protocol* [SC21 N 5903], 16 August 1991.
- SC21 N 7016, *Presentation Connection-Oriented ATS, Specific Partial ATS*.
- SC21 N 3666, *ATS for CS Test Method*, submitted by AFNOR. WD expected June 1992; CD October 1992; DIS October 1993; IS October 1994.

EWOS has agreed [ITSTC 1989] to convene an activity to study and investigate OSI Conformance Testing Methodology. This work would examine central aspects of OSI testing methodology that are necessary to support standardization of test specifications. CEN has been assigned leadership of the work.

TTCN is a unique, informal notation that was developed by ISO and CCITT for specifying generic and abstract test cases [Ref. ISO 4642-2 1987]. Other formal description techniques in use for this purpose are the Language of Temporal Ordering of Specification (LOTOS) and Estelle--both accepted in the *NTIS Transition Strategy*--and the System Development Language (SDL), developed by CCITT (Recommendation Z.100). Both Estelle and SDL are Pascal-based notations. These formal description techniques (FDTs) are described in detail in Section 8.4.2.

TTCN provides a notation in which generic and abstract test cases can be expressed in test suite standards, which is independent of test methods, layers, and protocols, and which reflects the abstract testing methodology of DIS 9646. TTCN provides a naming structure to reflect the position of test cases in the abstract test suite hierarchy (complete test suite, test groups, test cases, test steps, and test events). TTCN also provides the means of structuring test cases as a hierarchy of test steps culminating in test events.

Many organizations have been formed to address OSI conformance testing. These include Corporation for Open System (COS), OSINET, SPAG, European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC), NIST, Industrial Technology Institute (ITI), World Federation of Manufacturing Automation Protocol (MAP) and Technical and Office Protocol (TOP) User Groups, Conformance Testing Services-Wide Area Network (CTS-WAN), National

Computing Centre (NCC), and EurOSInet. TSGCE SG9 is addressing [Ref. CA 1989] military requirements in this area and whether NATO-specific activities need to be supported. The following are areas in which existing civil organizations may be expected to contribute to conformance testing to support military requirements [Ref. Cardonna 1988]:

- Developing standards and conformance certification criteria: ISO, CCITT
- Developing abstract test suites for OSI upper layers: ISO
- Developing test profiles and provisioning testing under military requirements: COS, SPAG
- Developing site accreditation criteria: Industrial Technology Institute (ITI)
- Implementing site accreditation and testing tools, and specifying test control and maintenance procedures: NIST
- Developing standards and test methodologies: CEN/CENELEC, ANSI.

COS [Ref. COS 1989] and SPAG have now completed formal agreement to combine their conformance test products within a single integrated tool set (ITS). In addition, COS, POSI, and SPAG have completed (June 1989) an Initial Strategic Technical Cooperation Agreement that commits the organizations to a strategic cooperative arrangement designed to provide a common technical solution to conformance testing, building upon the ITS. The agreement is also known as "CPS" (both for Conformance Promotion Strategy and for COS-POSI-SPAG).

OSINET, a 55-member United States-based interoperability testing organization, has voted to reorganize under the auspices of COS. OSINET was formed in 1984 under the auspices of NIST to work in three specific areas:

- Research and development of test scripts used in OSI interoperability testing
- Interoperability testing and registration of announced OSI products
- Demonstration and promotion of OSI technology [Ref. OSN 1991h].

There is a need to harmonize testing and certification schemes to enable mutual recognition of results of testing internationally. In 1985, the Conformance Test Service (CTS) was set up under the CEN/CENELEC to support the development of test tools and provision of test services. In Phase I (1985-1986), it addressed the following topics: OSI protocols, software quality, programming languages, and GKS. In Phase II (1987-1988), it continued to address OSI protocols as well as SGML, ODA, POSIX, and the programming language C. Memorandum M-IT-03 defines a framework for testing and certification in Europe which aims to enable mutual recognition of results of testing. The European Committee for IT Testing and Certification (ECITC) is implementing M-IT-03 by setting up mechanisms for mutual recognition of test reports and certificates These include abstract test suites and recognition of test tools, services, and tested products. The Open Systems Testing Consortium (OSTC) was formed in 1989 on completion of the CTS project to ensure continued harmonization [Ref. Pink et al. 1991].

8.4.1 PICS Proformas

An approach used in conformance testing (and in other applications) to specify interoperability parameters for an implementation profile (or a functional profile) is called a protocol implementation conformance statement (PICS). A PICS specifies all the parameters and options required to show how a particular implementation meets static conformance requirements. As such, it is the first tool in conformance testing. A PICS proforma is a PICS template developed and standardized in conjunction with a protocol standard. In the future, a PICS proforma can be expected to be required as part of the functional profile guidelines being developed by NIST, EWOS, AOW, NATO, and other standards bodies.

Since there are so many projects involving the development of PICS proformas, SC21/WG1 is developing an Annex of ISO 9646-2, *Guidelines for PICS Proformas*. SC21 has further developed a document entitled, Guidelines for PICS Proformas in SC6, to amplify some parts of the Annex for SC6 purposes [SC6 N 6243, September 1990]. In order to harmonize their use, SC21/WG1 has also set up as a standing document a *Catalogue of PICS Proforma Notations* [SC21 N 6160, 13 August 1991] to be updated as required.

8.4.2 Formal Description Techniques (FDTs)

FDTs are used to produce unambiguous descriptions of OSI services and protocols in a more precise and comprehensive way than natural language descriptions. Further, FDTs provide a foundation for analysis and verification of a description. The objectives of FDTs are to provide:

- Unambiguous, clear, and concise specifications
- Basis for determining completeness of specifications
- Foundation for analyzing specifications for correctness, efficiency, etc.
- Basis for determining consistency of specifications relative to each other
- Basis for implementation support.

There are three international standard FDTs that range from abstract to implementation-oriented: Estelle, LOTOS, and SDL. Since emerging standards are being written in one or more of these FDTs, the following sections are provided to give some technical information together with the basis, derivation, and character, for these description techniques [Ref. PDTR 10167 1989]. TR 10167, *Guidelines for the Application of Estelle, LOTOS, and SDL*, July 1991, provides guidelines for applying these three FTs. A fourth FDT--TTCN--was described in Section 8.4.

SC21/WG1 developed a working draft for *Architectural Semantics for FDTs* [SC21 N 4231, April 1990]. This work was planned to assist development of formal descriptions of standards for data communications, networking, and distributed computing. The draft defines and catalogues a set of selected elementary concepts, which act as a bridge between

the architectural concepts and structures and the semantic models of the FDTs (Estelle, LOTOS, and SDL). SC21 approved the May 1990 recommendations developed by a reassessment of the work associated with the *Architectural Semantics for FDTs*. The current work in SC21/WG1 will be terminated and a subproject initiated in SC21/WG7 in the area of ODP architectural semantics [Ref. SC21 N 4655 1990].

8.4.2.1 Estelle

Estelle (ISO 9074, *Estelle, A Formal Description Technique Based on an Extended State Transition Model,* July 1989) is a formally-defined specification language for describing distributed or concurrent processing systems, in particular those that implement OSI services and protocols. The language is based on widely used and accepted concepts of communicating non-deterministic state machines (automata). An Estelle specification defines a system of hierarchically-structured state machines. The machines communicate by exchanging messages through bidirectional channels connecting their communications ports. These messages are queued at either end of the channel. The actions of machines are specified in (extended) Pascal; hence, familiarity with Pascal makes Estelle specifications easily readable. Estelle uses Pascal data types in its data descriptions.

Estelle is based on an extended state transition model, i.e., a model of a nondeterministic communicating automaton extended by the addition of the Pascal language. Estelle may be viewed as a set of extensions to Level 0 of ISO 7185 (*Programming Language - Pascal*) that models a specified system as a hierarchical structure of communicating automata that may run in parallel and may communicate by exchanging messages and by sharing, in a restricted way, some variables. As in Pascal, all manipulated objects are strongly typed, which enables static detection (e.g., during compilation) of specification inconsistencies.

Estelle language mechanisms allow modelling of synchronous and asynchronous parallelism between state machines of a specified system. They also permit dynamic development of the system configuration. Estelle specifications can be prepared at different levels of abstraction, from abstract to quite implementation-oriented. The latter may be derived from the former with the aid of supporting tools. An Estelle tutorial has been developed and is intended to become Annex D (informative) of the Estelle base standard (ISO 9074 DAM 1, *Estelle Tutorial,* SC21 N 5710, 23 May 1991).

8.4.2.2 LOTOS

LOTOS (ISO 8807, *LOTOS, A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour,* February 1989) is a mathematically-defined FDT, developed from a large, well-established body of theory based on three mathematical techniques: Calculus of Communicating Systems (CCS), Communicating Sequential Processes (CSP), and ACT ONE. Having a well-defined mathematical foundation, it provides a solid basis for both analysis and development of reliable tools,

including simulation, compilation, and test sequence derivation. The basic constructs of LOTOS allow modelling of sequencing, choice, concurrency, and nondeterminism in an entirely unambiguous way. In addition, LOTOS permits modelling of both synchronous and asynchronous communication. LOTOS, like SDL, uses abstract data types in its data descriptions.

LOTOS may be applied to produce a specification of the allowed behaviours of a system, i.e., the set of all behaviours that may be observed of a conforming implementation. Furthermore, LOTOS permits the description of allowed behaviours without describing how this may be achieved or by describing particular mechanisms that achieve the required behaviour.

Formal descriptions of the session service and protocol using LOTOS have been developed:

- TR 9571, *LOTOS Description of the Session Service,* September 1989
- TR 9572, *LOTOS Description of the Session Protocol,* September 1989.

A new work item (SC21 N 6126) has been proposed for a CCR LOTOS description. In addition, WG1 has proposed a new sub-question on LOTOS enhancements to redress limitations identified by experience to date with the language. These limitations include:

- A notation for data abstractions which is not sufficiently user-friendly,
- Inability to compose a specification from pre-existing modules,
- Inability to specify explicit time.

This sub-question may lead to a proposed NWI on extension to ISO 8807 and possibly amendment to, or interpretation of, the existing standard. [Ref. SC21 N 6161 1991]

8.4.2.3 SDL

SDL is based (CCITT Z.100-Series recommendations) on the extended finite state machine model supplemented by capabilities for abstract data types based on the initial algebra model (the same one used in the ACT ONE part of LOTOS). This combination is supported by well-defined formal semantics. SDL provides constructs to present structures, behaviours, interfaces, and communications links. In addition, it provides constructs for abstraction, module encapsulation, and refinement. All of these constructs were designed to assist the representation of a variety of telecommunications systems specifications, including aspects of protocols and services.

8.4.2.4 G-LOTOS

Text for a standard for a graphical syntax, G-LOTOS, has been submitted [ISO 8807/PDAM 1 1989] that provides an extension to LOTOS (ISO 8807 DAM 1) to facilitate production and enhance clarity and readability of formal descriptions, simplify

teaching and learning the language, favour the development of advanced user-friendly software tools, and promote the diffusion and application of the language [Ref. G-LOTOS 1988].[39] AM status is expected in December 1992.

8.4.2.5 Z

Z is an abstract specification language; however, there is no current standard for Z. Z is based on the mathematics of set theory and predicate calculus. Systems are described by introducing fixed sets and variables and specifying the relationship between them. Current applications of Z include safety- and security-critical systems [Ref. Spivey 1989]. ISO/CCITT Joint Modelling Group has suggested Z be considered as a candidate FDT for use in ODP [SC21 N 6088, 31 May 1991].

8.4.3 Conformance Test Suites

Before conformance testing can be conducted, conformance test suites must be specified for each standard to be addressed. The standards for conformance test suites typically have two parts: *Test Suite Structure and Test Purposes* and *Abstract Test Suite.* These form the basis for developing a conformance test and verifying its accuracy. Examples of standards for conformance testing are ISO 8882 (X.25), ISO 9594 (Parts X and Y for Directory), DIS 10025 (Transport Protocol), DIS 10168 (Session Protocol), ISO 10169 (ACSE Protocol), ISO 10170 (FTAM), CD xxxx (Transaction Processing Protocol), DIS 10729 (Presentation Protocol), and DIS 10739-1 (Virtual Terminal).

In 1989, NIST conducted an analysis of the OSI testing situation and concluded that unless it acted, no credible means of substantiating GOSIP compliance would be available in time to support the US Government OSI mandate beginning August 1990. Abstract Test Suites, where they existed, were fragmented and not publicly available. Although multiple suppliers of Means of Testing (MOTs) existed, no credible mechanism existed to assess MOTs against GOSIP requirements; no means existed for finding one MOT acceptable and another not. Moreover, no program of evaluating and accrediting commercial GOSIP testing laboratories was planned. From April through November 1989, NIST defined a GOSIP Testing Program and on November 13 issued a proposed *GOSIP Conformance and Interoperation Testing and Registration FIPS* for public comment [Ref. Favreau et al. 1990]. On September 30, 1990, NIST published the initial set of registers (*Register of Abstract Test Suites* and *Register of Assessed Means of Testing*). The *Register of Accredited Testing Laboratories* appeared May 1, 1991 [Ref. Martin 1991]. Section 7.2.1.1 addresses the POSIX Conformance Test Suite.

---

[39] New work item [JTC1 N 485] for G-LOTOS was not accepted, but work is proceeding nevertheless (January 1991).

8.5 Standards for Registration Authorities

Registration provides unambiguous identification of instances of certain types of information objects within the OSI environment. Examples of these instances are an application process, an application entity, and the definition of a class of information such as a file format. Registration is the assignment of an unambiguous name to an instance of a type of information object in a way that makes the assignment available to interested parties. It is carried out by a registration agent that may be either a standard or an organization.

SC21 and CCITT SGVII have agreed to collaborate in work on registration authorities. The groups have concurred that "the establishment and operation of registration is critical to communications in a distributed environment and that, without procedures for the operation of registration, interoperability between applications is unlikely" [Ref. SC21 N 5014 1990]. An area of disagreement is the presence of the Name Form in DIS 9834-1, included to support the specification of procedures to ensure the assignment of unambiguous names for registration purposes.

SC21/WG1has developed[40] a standard (ISO 9834, *Procedures for the Operation of OSI Registration Authorities*) for the operation of OSI registration authorities. The status and structure of this standard is as follows:

- ISO 9834-1 (Part 1): *General Procedures*, March 1990 [SC21 N 4352] (July 1991 editing meeting recommended progression to IS status)
- ISO 9834-2 (Part 2): *Registration Procedures for Document Types*, June 1991 [SC21 N 6268]
- ISO 9834-3 (Part 3): *Registration of Object Identifier Component Values for Joint ISO/CCITT Use*, July 1990 [SC21 N 4718, April 1990]
- ISO 9834-4 (Part 4): *Registration of VTE Profiles*, July 1991 [SC21 N 4325]
- ISO 9834-5 (Part 5): *Registration of VT Control Objects*, July 1991 [SC21 N 4322]
- DIS 9834-6 (Part 6): *Registration of AP Titles and AE Titles*, September 1990 [SC21 N 5218]; did not progress to IS status, vote failed 13:5 [SC21 N 5910, 25 April 1991]
- *Register of Object Identifier Components Allocated to Areas for Joint ISO-CCITT Work* [SC21 N 5506, November 1990], maintained as an internal SC21 document.

Work on registration authorities (SC21/WG1) is ongoing in one additional area--registration of system titles, but this will probably be incorporated in the management standards. Prior work on authentication mechanisms, application context names, abstract

[40] Work on Registration Authorities beginning in November 1989 was transferred to SC21/WG6.

syntaxes, and transfer syntaxes (WD 9834-B, C, D, E, F) is now considered as not required.

8.6 Assessment

Quality of Service and security are not well addressed by OSI and other open systems standards. Both of these sets of services require review and possible modification of the basic reference models for open systems. They therefore could lead to disruption of some of the standards that have already become stable under the existing reference models.

Both sets of services may be supported in a wide range of ways, and several approaches of these may be required in CCISs to meet operational requirements. For example, quality of service affects all the layers of the OSI Reference Model, and the associated protocols, managed objects, and parameters of the protocol data units may all have to be extended to meet military requirements. Security can be expected to impact at least the Physical, Network, and Applications Layers of the OSI Reference Model (the NATO position) and other layers as well (SDNS also provides a protocol for the Transport Layer).

Work has already begun on OSI services and protocols in the management area. Support for access control and authentication is already being incorporated into a number of OSI standards. Many other aspects of security, such as key management, still must be standardized to ensure interoperability and to avoid building the same functions many times in similar systems (e.g., function-specific CCISs) and in the applications of a single system, such as a CCIS.

Management issues can be expected to differ for each of the technologies being considered for CCISs. For example, security aspects of local area networks differ from those associated with broadcast radio and packet-switched point-to-point links.

Some issues and findings in security and OSI management are:

- Standards for OSI security are evolving, but the evolution is slow. OSI standards may not be satisfactory in some areas (e.g., OSI services) in and of themselves for military applications. They may need to be supplemented by application-level services outside the OSI model.
- An adequate treatment of management services may require modification to the OSI Basic Reference Model and thereby impact many stable OSI standards.
- Some management standards are now stable (e.g., ISO 9595, ISO 9596; ISO 10040, ISO 10164, DIS 10165), but there is standardization required in many additional areas.

9. DATA INTERCHANGE SERVICE STANDARDS

Data interchange services transfer data that represent abstract objects such as military orders, reports, research documents, graphical items (e.g., maps and overlays, symbolic graphical data that might be produced by a simulation), and raw video (e.g., television images). Data interchange services also address product descriptions. An overview of the status of standards for data interchange services is given in Table 18.

Quick Reference	
Topic	Page
Assessment	225
Audio Data Exchange	224
CEDD	219
CGI	213
CGM	212
Comp Graph Ref Model	212
Data Compression	221
DCW	220
DFR	207
DIGEST	216
DOAM	204
DTAM	206
EDI	205
NATO Geog Conference	220
ODA	198
ODIF	198
RDT	208
SDTS	220
SGML	201
SIMNET	218
Video Data Exchange	223
VPS	220

9.1 Document Exchange

This section summarizes standards for office document interchange architectures and formats. It addresses CCIS requirements for both formatted and unformatted documents. These requirements include [Ref. IDA 1991, 137 and 142]:

- Existing use of formatted messages in CCISs
- Reduced reliance on formatted messages in favor of direct database exchanges
- Interoperability and closer coordination with systems not traditionally used directly by commanders and their staffs
- Production and maintenance of unformatted documents on the same computers that will be used for command and control
- Electronic dissemination of unformatted documents both for review and final distribution.

Table 18. Status Overview of Key Data Interchange Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
ODA/ODIF/ODL	●		●		○		○
SGML	●		○	●	●		●
CGM	●	●	●	●	●	●	●
IGES	●	●		○	●	●	●
STEP			●				

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

ISO, CCITT, and ECMA have developed several standards for the transfer of files and d standards efforts is one of the main topics for the Technical Study Group (TSG-1) on Interfaces for A and their relationships are discussed in the sections that follow.

9.1.1 Office Document Architecture (ODA) and Interchange Format (ODIF)

ODA is one of two standards used for describing documents in preparation for electronic interchange; the other is SGML. ODA (ISO 8613) was originally designed for the interchange of office documents between different word processors. The equivalent CCITT Recommendations are the T.410 series (see end of Appendix E). ODA describes a document in terms of its logical structure or its layout structure or both together. The ODA standard is divided into several parts:

- ISO 8613-1, *Part 1: Introduction and General Principles* and *ISO 8613-1 AM 1 Amendment 1: Document Application Profile Proforma and Notation and AM 2 Amendment 2: Conformance Testing Methodology*
- ISO 8613-2, *Part 2: Document Structures*
- WD 8613-3, *Part 3: Document Processing Reference Model* [WITHDRAWN]
- ISO 8613-4, *Part 4: Document Profile*
- ISO 8613-5, *Part 5: Office Document Interchange Format (ODIF)*
- ISO 8613-6, *Part 6: Character Content Architectures*
- ISO 8613-7, *Part 7: Raster Graphics Content Architectures*
  - *AD1: Tiled Raster Graphics*
  - *AM 2: Color*
  - *AD 3: Alternative Representation*
  - *AD 4: Security*
  - *AD 5: Streams*
  - *AD 6: Styles*
- ISO 8613-8, *Part 8: Geometric Graphics Content Architectures*
- WD 8613-9, *Part 9: Audio Content Architectures*--CD expected in 1992 (1Q), DIS in 1992 (4Q), and IS in 1993 (3Q)
- ISO 8613-10, *Part 10: Formal Specifications* and *ISO 8613-10 AM 1 Amendment 1: Formal Specification of the Document Profile and AM 2 Amendment 2: Formal Specification of the Raster Graphics Content Architectures.*

ISO 8613-3 was withdrawn, but is now being developed by SC18/WG1, User Requirements and Reference Model, as a two part standard. Part 1 will be the *Basic Reference Model* and Part 2 will be the *Technical Reference Model*. CD is expected in 1991 (4Q), DIS in 1992 (3Q), and IS in 1993 (3Q). [Ref. OSN 1991k]

Part 5 of ODA specifies a second method of representation and interchange, using the Office Document Language (ODL) and the SGML Document Interchange Format

(SDIF). ODL is an application of the Standard Generalized Markup Language (SGML), and may be used to represent a document structure in accordance with ODA in SGML.

ISO 8613 is being adopted as an American National Standard as well. ASC Committee ANSI X3V1 - Text: Office and Publishing Systems plans to produce multiple part addenda that will provide extensions to an ANSI standard that will remain consistent with the ISO 8613 standard [Ref. X3 1991]. Table 19 shows some of the planned extensions and their estimated dates of completion [Ref. OSN 1991b].

Table 19. Future Work on Office Document Architecture (ODA, ISO 8613)

Revision Accountancy	1993
Annotations	1992
Automatic content generation	1992
Business charting	1994
Data in documents, spreadsheets	1992
Hypermedia support	1992
Hyper ODA	1991 (WD)

The following describes this new work [Ref. OSN 1991k]:

- Revision accountancy consists of a collection of several revisions of a document, possible including some additional information as to the status and rational for a revision and its author.
- Annotations may or may not form a permanent part of a document, but they may use any content type.
- Automatic content generation refers to generated listings including table of contents, tables of figures, illustrations, etc., indexes, glossaries; cross references; and copying of body material into executive summaries and outlines.
- ODA business charting includes the ability to derive a business graphic from tabular, spreadsheet or other data in the document or referenced by the document; derive part of a document from an external business graphic; and include a business graphic in a document in such a way that the business graphic specific processing can be performed by the recipient.
- Data in documents is to be part of Part 8. It refers to support for incorporating external material by reference, for example: both the structure and content of an external document, document in a database, or font information.
- Hypermedia structures allow an originator to be able to pass to a recipient the intention that the recipient can follow one or more routes through the logical structure with associated control of the presentation of an ODA document.
- The ODA audio content architecture (Part 9) will define a content architecture for voice and other audio information. It will use pre-existing or developing coding standards for audio. Audio content, which may be used for annotation or other purposes within a document, has a close relationship with time

synchronization and annotation extensions for the ODA document processing work.

The Profile Alignment Group for ODA (PAGODA) has been formed from the three special interest groups (SIGs) and expert groups (EGs) from the three regional OSI workshops (see also Section 6.4.1): Asia/Oceania Workshop (AOW) ODA SIG, EWOS ODA EG, and the NIST ODA SIG. PAGODA is developing ODA profiles based on ISO 8613, *Office Document Architecture (ODA) and Interchange Format (ODIF)*. The Office Document Format (FOD) provides for two types of structure in its proposed taxonomy [Ref. SGFS 1989]:

- Hierarchically related based on increasing complexity and functionality (simple, enhanced, and extended document structures). The simple document structure is intended to address the general requirements of current word processing applications. The enhanced document structure is intended to address the general requirements of emerging word processing applications that have been enhanced over current applications. The extended document structure would address the general requirements of emerging personal publishing and document processing applications.
- Content architectures for various combinations of character, raster graphics, and geometric graphics content architectures.

FODs currently under development as proposed draft International Standardization Profiles (pDISPs) (see Section 6.4.2) include the following [Ref. OSN 1991c]:

- FOD11-1 (pDISP), *Office Document Format Profile for the Interchange of Basic Functional Character Content Documents in Processable and Formatted Forms - Part 1: Document Application Profile (DAP)*
- FOD26-1 (pDISP), *Office Document Format Profile for the Interchange of Enhanced Function Mixed Content Documents in Processable and Formatted Forms - Part 1: Document Application Profile (DAP)*
- FOD36-1 (pDISP), *Office Document Format Profile for the Interchange of Extended Function Mixed Content Documents in Processable and Formatted Forms - Part 1: Document Application Profile (DAP).*

Although there is no strong user demand for ODA products currently, predictions are that over the next 5 years ODA has the potential to satisfy growing demand for standards-based document management, particularly interchange. Three types of ODA products are available:

1. ODA toolkits -- intended to enable ODA conversion facilities to be built into products and systems with minimum effort
2. Converters -- extensions to existing products to allow them to take part in ODA document interchange
3. Native products -- applications that implement document processing functions that conform to ODA standards.

Six major international computer companies recently formed the Open Document Architecture Consortium (ODAC) to develop a toolkit of software that conforms to the ISO ODA standard. The companies are Digital, ICL, Siemens Nixdorf Information Systeme, Groupe Bull, IBM, and Unisys. The toolkit is expected to be available in 1993 [Ref. OSN 1991b]. In addition, Apple Europe has made available an ODA toolkit called WOPODA.

Bull, Siemens-Nixdorf and Xerox offer ODA converters as part of their more comprehensive office systems products. Beta test versions of word processor converters and native ODA editors are in use on personal computers and Apple Macintosh's.

ODA has been the subject of visible interworking demonstrations both in Japan and Europe. Cooperative activity in Europe has included the PODA (piloting ODA) project which, in 1990, as one of its products demonstrated the interchange of integrated text and graphics documents between participants systems using X.400 electronic messaging. Moreover, IBM recently announced that it will adopt the ODA standard instead of the revised form of its own Mixed Object Document Content Architecture (MO:DCA). Microsoft has also just declared its intention to support ODA and have an ODA Manager based around its Microsoft Word product [Ref. OSN 1991d].

9.1.2 Standard Generalized Markup Language (SGML)

SGML formalizes document markup, making the document system and processing independent. It is an architecture-free and application-free language for managing structures and is designed for full multi-media database publishing. SGML is a meta-language, providing the rules for designing and applying a system of markup tags rather than the specific set of tags. As noted above, ODL is a set of rules in ODA for using SGML to represent documents. The SGML standards are:

- ISO 8879, *Standard Generalized Markup Language (SGML)*
- TR 9573, *SGML Support Facilities--Techniques for Using SGML*
- ISO 9069, *SGML Support Facilities--SGML Document Interchange Format*
- ISO 9070, *SGML Support Facilities--Registration Procedures for Public Text Owner Identifiers*
- TR 10037, *SGML and Text-Entry Systems--Guidelines for SGML Syntax-Directed Editing Systems.*

Accredited Standard Committee ANSI X3 recently announced the second public review of X3.190-199X, *Conformance Testing for SGML.* The draft standard addresses the construction and use of test suites for verifying conformance of SGML systems (see also Section 9.4). Its provisions assist those who build test suites, those who build SGML systems to be evaluated by such suites, and those who examine an SGML system's performance on a test suite as part of the process of selecting an SGML tool [Ref. X3 1991a].

Three standards related to SGML are:

- CD 10179, *Document Style Segmentation and Specification Language (DSSSL)*
- CD 10180, *Standard Page Description Language (SPDL)*
- MIL-M-28001A, *Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text,* 20 July 1990 (CALS application of SGML). Revision B is expected to be complete in late 1992.

Some people believe that these standards, when used with SGML and viewed as a group, will comprise a much more comprehensive information management architecture than that envisioned by ODA [Ref. Terrell 1990]. SGML is also being extended to deal with hypermedia/time-based document interchange. The HyTime standard, *Hypermedia/Time-based Structuring Language (HyTime),* under development by ANSI X3V1.8M (Project 749-D) and ISO (CD 10744), is a notation to describe hypermedia. HyTime is a collection of abstract semantic constructs associated with syntactic conventions. It allows hyperdocument interoperability to the maximum extent possible (1) without standardizing multimedia objects, their notations, their modifiers, the effects of those modifiers on them, and the semantics of link types; and (2) without requiring existing documents to be recast in order to make their contents linkable to HyTime documents. HyTime-compliant documents can allow HyTime-cognizant software to browse, render, format, and query them even if that software is not able to understand or render its multimedia objects. If the notation of an object is uninterpretable because no interpreting system is locally available for it, the render can still incorporate some form of blankness, e.g., darkness, silence, or an appropriate error message, so that the space and time relationships of the rendered and unrenderable objects is preserved [Ref. Newcomb c1991]. Object-oriented methods are at the heart of another similar standards effort, run by the Multimedia and Hypermedia information coding Experts Group (MHEG) [Ref. Fox 1991].

SGML has been chosen by the DoD as the documentation standard for its Computer Acquisition Logistics Support (CALS) strategy. This strategy is designed to take defense information from its current paper form to a totally electronic mode over the next decade. MIL-M-28001A establishes the requirements for the digital data form of technical publications. Data prepared in conformance to these requirements will facilitate the automated preparation, storage, retrieval, exchange, and processing of technical documents from heterogeneous data sources. The requirements set forth by this specification include:

- Procedures and symbology for markup of unformatted text in accordance with this specific application of SGML
- SGML-compatible codes that will conform a technical publication to specific format requirements
- Output control codes that will conform automated document processing functions to a uniform structure.

MIL-M-28001A establishes the requirements for the digital forms of all US DoD technical publications using SGML. Data files satisfying the requirements of this specification will be one of two types: Type I - MIL-M-38784B conforming technical manuals and Type II - technical manuals conforming to other military specifications. Documents prepared in accordance with MIL-M-38784B and MIL-M-28001A must conform to the document type definition (DTD) defined in Appendix A and the output specification in Appendix C of MIL-M-28001A. The DTD and output specification for a MIL-M-38784B conforming manual do not have to be delivered with the tagged text. Technical manuals conforming to other military specifications may develop their own DTD but must use only those tags in the baseline tag set defined in Appendix B of MIL-M-28001A. In this case, the DTD must be delivered with the publication along with a compatible output specification.

MIL-M-28001A addresses the five steps in the publication preparation process:

(1) Creating a DTD for publication control

(2) Authoring the publication and inserting SGML markup tags

(3) Verifying the syntax according to the rules of SGML

(4) Using the output specification to compose the document so that produced copy corresponds to the proper formal and style

(5) Generating a text presentation metafile in SPDL to drive the display device.

The heart of MIL-M-28001A is found in its appendices. Appendix A specifies the role played by the DTD in an SGML implementation; a general description of DTD structure and content; the specific DTDs available for use in authoring, validating, and verifying an SGML-tagged technical document; and procedures for DTD development. The appendix introduction provides an overview of the concepts behind the SGML standard, a brief tutorial on reading an SGML DTD, guidelines for using SGML tags, and DoD's SGML declaration. Two DTDs are also presented in Appendix A. This first DTD is for use when preparing a document that conforms with MIL-M-38784B. The second uses the same elements as the first DTD with the addition of more subordinate paragraphs and steps. This DTD may be used for MIL-M-38784B non-conforming documents or as a model for the development of a more appropriate DTD. Both DTDs allow for four types of non-SGML data: IGES data, CGM data, CCITT Group 4 data, and system-generated data.

Appendix B of MIL-M-28001A contains an alphabetical listing of all elements contained in the DTDs presented in Appendix A. Appendix C is a stand-alone document. It includes a document output specification (format and style guide) to be used for all applications of this specification. Although the format default values are set according to MIL-M-38784B, the values may be tailored to satisfy other format requirements. The appendix also provides an example of an SGML-coded source file and the composed sample document produced from the marked up file.

CALS, since it is an application-specific architecture oriented to technical weapons systems support documentation, may not be applicable to all of the other types of information that a generic CCIS comprises.

There is an incorrect perception that ODA and SGML are competing standards. In fact, ODA is a generic interchange architecture that uses SGML as one of its interchange formats. The other interchange format, ODIF, is specifically of use in an OSI environment because it uses ASN.1. However, both standards exist in the application layer of the OSI. Although CALS has selected SGML, it has left the door open to ODIF as well. The NIST assessment is that both ODA/ODIF and SGML enjoy an average level of consensus, and neither has much product availability or *de facto* usage. However, it evaluates ODA/ODIF as being more complete than SGML, but rates SGML as being significantly more stable and mature than ODA/ODIF [Ref. APP 1991, 35].

9.1.3 Distributed Office Applications Model (DOAM)

The Distributed Office Application Model (DOAM), ISO 10031, was established to provide a set of common principles to which all Distributed Office Application (DOA) standards must adhere. The two parts of this standard, General Model and Referenced Data Transfer, do not contain any implementable protocols; they are limited to the description of models and tools to be used by DOA standards developers.

An important feature of the DOAM is the client-server model, which allows one part of an application to be implemented in a "client" machine and another part to be implemented in a "server" machine. This possibility of splitting an application allows certain central resources, such as a large database or an expensive laser printer to be shared among a number of users from their workstations.

DOA consists of the DOA model (DOAM) and two specific DOAs: Document Filing and Retrieval (DFR, ISO 10166) and Document Printing Application (DPA) (DP xxxxx). The DOAM (ISO 10031) addresses the general model, design guidelines for the peer-to-peer (Application Layer) protocol, and Referenced Data Transfer (RDT). Use of ROSE is mandatory in DOAM. The DOAM guidelines are used to define DOA objects (e.g., documents), together with object attributes and criteria for filtering those objects. The DOAM guidelines identify a set of abstract operations such as List, Read, Write, Modify, Copy, Move, Search, Create, Delete, Reserve, Unreserve, Notify, and Abandon. RDT is the mechanism used to perform transfer of objects. RDT was developed to permit "small" systems (e.g., workstations) to handle "large" objects, such as moving an object from a document store to a print service. DFR defines the structure of a document store and an associated access protocol. DPA defines an access protocol for print services. DOA is being developed by SC18/WG1 [Ref. SC21 N 3930 1989]. SC18 recently merged the DOA and messaging work into one working group (WG4) to produce better cooperation between the two areas. [Ref. OSN 1991k]

9.1.4 Electronic Data Interchange (EDI)

EDI provides for a standardized exchange of data between systems by a wide range of means, including exchange of magnetic tapes and the transmission of data by Telex. EDI is a standard for the data, and as such, is outside OSI (OSI standards are for the means of moving that data). EDI is intended to enable data to be interchanged without networking and is used mainly for interorganization communication where internetworking may be undesirable (internetworking is a primary feature of OSI).

Prior to 1985, there were two world-wide EDI standards, UN-TDI/GTDI in Europe and ANSI X12 (*An Introduction to EDI*, July 1987) in North America.[41] At that time, the United Nations tried to produce a single standard for both communities. This standard was the EDI for Administration, Commerce, and Transport (EDIFACT). The syntax for EDIFACT is now an ISO standard (ISO 9735). EDIFACT is based on ISO 646 encoding (7 bits per character--ASN.1 Basic Encoding Rules use the full range of 8 bits in each octet). A large number of standard messages have been developed based on EDIFACT, and the EDIFACT has been endorsed by many standards bodies and user groups. However, another standard, TRADACOMS, has been developed for use in the United Kingdom, based on the UN-GTDI syntax. TRADACOMS is now in wide use in the United Kingdom and currently enjoys the status of *de facto* UK standard. However, a recent notice [Ref. CCTA 1991a] issued by the CCTA in the United Kingdom states that "departments should refrain from its (TRADACOMS') use" and invites departments and agencies to adopt EDIFACT as the EDI standard. CCTA's UK GOSIP Version 4 provides up-to-date guidance on the use of EDIFACT.

EDIFACT provides data structure and content standards for developing messages for use by importers, exporters, transportation firms, financial institutions, ports, customs, and other business and administrative activities (e.g., insurance, tourism, construction). EDIFACT was developed by the UN working party on Facilitation of International Trade Procedures to ensure there is only one worldwide standard for EDI. EDIFACT is ISO 9735 and uses the international standard Trade Data Element Directory (ISO 7372) [Ref. SC21 N 3885 1989]. ANSI X12 guides, stimulates, and promotes the development and use of the EDIFACT standards in the United States and Canada, but EDIFACT is still not aligned with ANSI X12. The ANSI X12 Secretariat has noted that differences in syntax control segments, data segments, and data elements continue to exist between EDIFACT and the X12 standard for EDI [Ref. DISA 1990]. X12 plans to align with EDIFACT by the time of publication of Version 4 of the X12 standards in 1994 [Ref. Kornfeld 1990].

---

[41] The number of companies currently using EDI has been estimated at 15,000. Up to 13,000 of these are in the U.S. and about 1,600 in the U.K. The number of users is reported to be doubling every year. Source: International Network Services, Limited [OSN 1989c].

CCITT is preparing a fast-track recommendation in 1990 for electronic data interchange over X.400 (CCITT X.425). This standard will use a new User Agent protocol called PEDI that will include security services necessary to support nonrepudiation. The CCITT EDI user agent will allow CALS formats (e.g., US MIL-STD-1840B, *CALS Originator File Sets and Transfer*) to be supported as body parts.

The CALS initiative is the largest and best known of the EDI proponents. CALS requires full compliance to EDI standards for digital delivery of technical information and interoperability among DoD systems beginning in January 1990. Major applications areas are automation of technical manuals, computer-assisted design, and spares acquisition. CALS standards include EDI for data interchange file management, IGES for engineering drawings, Standard Generalized Markup Language (SGML) for automated publishing, and CGM for technical manual illustrations. The standard currently being used for raster graphics representation is US DoD-unique (MIL-R-28002A, 30 November 1990).

ISO/IEC JTC1 has a special working group (SWG) on EDI whose purpose is to further global interoperability among EDI application areas and use of various Information Technology standards. It has published an interim draft report on a conceptual model for EDI standards and services (ISO/IEC JTC1 SWG-EDI N 1770). The proposed "open-EDI" model intends: (1) to describe "business" relationships among participants in EDI in a formal way, and (2) to be able to develop standards and tools supporting this description. The proposals for standardization work include [SC21 N 5635, *Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI)*, 23 January 1991]:

- The methods to be followed for the description of open-EDI scenarios, and indications on the formal description techniques to be used
- The description of the functional requirements supporting the execution of the scenarios
- The abstract definition of the services needed to meet these functional requirements.

In May 1991, SC21/WG5 proposed an EDIFACT/FTAM Document Type (see also Section 6.3.3) in an attempt to merge existing FTAM implementations with existing EDI systems with a minimum of change. [Ref. SC21 N 6224 1991]

9.1.5 Document Transfer and Manipulation (DTAM)

DTAM is being developed by CCITT SG/VIII. The DTAM protocols are designed to support interactive as well as store-to-store real-time end-to-end communications. They are also suitable for multi-media applications. Telematic applications are currently defined within the integrated, modular approach based on ODA (see Section 9.1.1), DTAM, and Document Architecture Operations (DAO, CCITT SG VIII). The telematic applications are Group 4 Facsimile, mixed mode, processable mode, and videotext internetworking. Each

telematic application consists of equipment characteristics, document characteristics (selected from ODA), operational characteristics (optional, selected from DAO), and communications characteristics (selected from DTAM).

DTAM differs from FTAM in that the standards address different environments. FTAM satisfies requirements for the transfer of files between different file systems, including retention of generic filing information. DTAM, on the other hand, provides facilities for the storage, management, and retrieval of documents in an integrated office application environment.

Two types of telematic and office environment applications for DTAM are being developed by CCITT SG VIII and ISO JTC1 SC18: conference type and remote document handling. A service called Remote Open Document Editing (RODE) is being proposed for the telematic environment to provide real-time remote editing for content manipulation through use of ODA/DTAM. RODE is expected to fulfill such user requirements as observing changing documents; maintaining identical documents between partners, even when partners have different presentations; providing speedy manipulations; and potentially supporting participation of more than three partners. Services are being defined to enable RODE to support a desk top conference application using DFR as well as RODE [Ref. SC21 N 4342 1990].

9.1.6 Document File and Retrieval (DFR)

DFR (ISO 10166) is the responsibility of ISO/IEC JTC1 SC18/WG4. DFR is one of the office application standards defined by the DOAM (see Section 9.1.1) and shares common mechanisms with directory services and MOTIS. These mechanisms include attribute definition and filtering facilities, and they use service elements for remote operations (ROSE) and reliable transfer.

DFR also supports a "version management" mechanism. This mechanism allows a document to be declared as a new version of an existing document. When this is done, a "previous-version" attribute points to the previous version of the document, and the previous version correspondingly receives a "next-version" attribute, thus retaining the complete evolution of a given document. All versions of a document contain a "version-root" attribute indicating the first version of the document.

DFR is defined by two standards:

- ISO 10166-1, *DFR - Part 1: Abstract Service Definition and Procedures,* 1989
- ISO 10166-2, *DFR - Part 2: Protocol Specification,* 1989.

DFR and DTAM both handle primarily ODA documents. They differ in that DFR is not concerned with the inner content of a document, whereas DTAM is concerned with both the whole document and the inner content of the document. Further, DFR provides

for filing and retrieval of (whole) documents, whereas this capability is not supported by DTAM.

DFR differs from FTAM in that filing and retrieval of documents is DFR's single specific office application. An important difference between these two standards is the manner in which a document or file is identified. DFR uses a "Unique Permanent Identifier" that remains with the object for its lifetime. FTAM uniquely identifies its objects by its pathname from the root through the directories leading to it. In FTAM, if the contents of a file are moved to another directory, the pathname will change. Also, there is no analogy in FTAM of DFR's version control mechanism.

A joint meeting between SC21/WG5 (FTAM) and SC18/WG4 (DFR) in Stockholm in May 1989 concluded that, due to the different user requirements being met by the two standards, a general-store model could not be progressed [Ref. OSN 1989a].

9.1.7 Referenced Data Transfer (RDT)

RDT standards have been under development within ECMA TC32-TG5 and ISO/IEC JTC1 SC18/WG4. The abstract service definition is Part 2 of the DOAM (ISO 10031-2). The RDT protocol duplicates functionality provided by FTAM, specifically the simple, efficient transfer of unstructured data (this is provided by FTAM-3 and the FTAM Transfer Service Class). However, a minimal implementation of FTAM would not provide all the apparent RDT requirements, such as security, single/multiple use of reference, finite life of reference, and use over a single association along with the RTSE.

9.1.8 DoD Document Exchange Standards

DoD has developed the following standards for document exchange:

- DoD-STD-7935, *Automated Data Systems (ADS) Documentation,* 15 February 1983
- MIL-M-38784B, *Manuals, Technical: General Style and Format Requirements,* February 1991
- MIL-STD-1840B, *Automated Interchange of Technical Information,* March 1991
- DoD-STD-2167A, *Defense System Software Development,* 29 February 1988.

DoD-STD-7935 provides guidelines for the development and revision of the documentation for Automated Data Systems (ADS) of applications computer programs, and prescribes the standards and descriptions for each of the technical documents to be produced during the life cycle of an ADS. ADS is defined as "an assembly of procedures, processes, methods, routines, or techniques (including, but not limited to, computer programs) united by some form of regulated interaction to form an organized whole, specifically designed to make use of automatic data processing equipment." The objective of the standard is to provide managers of ADS projects with documentation of uniform

format and content for review to assure the meeting of significant development milestones. It also provides ADS technicians with a standard record of technical information as a basis for coordination of later ADS development or use modification. There are eleven technical documents described in the standard: Functional Description, System/Subsystem Specification, Data Base Specification, Computer Operational Manual, Test Plan, Implementation Procedures, Data Requirements Document, Program Specification, Users Manual, Program Maintenance Manual, and Test Analysis Report. A proposed outline and text format for each document type is provided in Section 3.0 of the standard.

MIL-M-38784B is a military specification approved by the DoD for use in developing technical manuals. Technical manuals are publications that contain instructions for the installation, operation, maintenance, training, and support of weapon systems, weapon system components, and support equipment. Manuals prepared in accordance with this specification are intended for use in the operation and maintenance of equipment or for accomplishment of assigned missions. It covers the general style and format requirements for the preparation of manuscripts and reproducible copy for standard technical manuals and changes to those manuals. The only decision left to the author of a technical manual is the actual technical content of the manual; even the style of writing is specified (US Government Printing Office Style Manual).

The major section of MIL-M-38784B, Section 3.2, is dedicated to format issues. The specification covers everything from the size of the paper to capitalization to suggested type styles and sizes. The specification identifies the structure of a technical manual. It specifies what will be included in the manual outline and publication divisions (volumes, parts, chapters, section and paragraphs). Paragraphs are divided into primary and subordinate paragraphs. The last sections of the specification discuss how to make changes to a technical manual, quality assurance provisions (readability, etc.) and preparation for delivery (packaging).

The purpose of MIL-STD-1840B is to standardize the digital interface between organizations or systems exchanging digital forms of technical information necessary for the logistic support of weapon systems throughout their life cycle. This standard addresses technical information and product definition data. It standardizes the format and information structures of digital data files used for the transfer and archival storage of digital technical information. The format, information structures, and transfer procedures are applicable in all cases where the information can be prepared and received in the form of American Standard Code for Information Exchange (ASCII) text files, product definition data files, raster image files, or graphics files.

Technical publications addressed by MIL-STD-1840B consist of text and associated illustrations. The files of a technical publication consist of a declaration file, text files (in ASCII) tagged to the contract (may use MIL-M-28001A), illustration files (in Initial Graphics Exchange Specification (IGES), Computer Graphics Metafile (CGM), or raster

format), files in Page Description Language (PDL) form, and other files (output specification file, special word file, etc.). The standard dictates very detailed requirements for the structure, content, and order of information. For example, the declaration file must precede the data files and provide information about the identifications, source, destination, and classification of the document. The standard also specifies the file header records for textual data, CGM data, document type definition, program descriptive language (PDL) data, IGES data, gray scale, raster data, special word, and output specification data.

DoD-STD-2167A provides the means for establishing, evaluating, and maintaining quality in software developed for weapon systems and its associated documentation. The contract agency is responsible for tailoring the software management process to meet the needs of a particular project. The data item descriptors (DIDs) associated with this standard describe a set of documents for recording information required by the management process. The standard encourages the production of deliverable data using automated techniques.

9.2 Graphical Data Exchange

Existing military CCISs support the generation and display of graphics, a capability that will continue to be required in the future. The problem is that graphics are generally not distributed. Instead the data are distributed and the graphics are regenerated at each location where they are needed. This process tends to be slow, unreliable, and expensive [Ref. IDA 1991, 152]. What is needed is a common standard intermediate form to transmit graphics such as exists in other areas of publishing [Ref. Carlson 1991]. Moreover, there is growing interest in using graphics for simulation purposes [Ref. IDA 1991, 152].

Section 9.2.1 describes two standards for exchange of graphical information products: Initial Graphics Exchange Specification (IGES) and the Standard for the Exchange of Product Model Data (STEP, formerly PDES). Standards for graphics interchange services (e.g., Computer Graphics Metafile) and Computer Graphics Interface (CGI) are addressed in Section 9.2.2. Two graphics standards are treated separately in Chapter 11: the Graphics Kernel System (GKS) and the Programmer's Hierarchical Interactive Graphics System (PHIGS).

9.2.1 Graphical Information Product Exchange

The IGES, Version 4.0, is an ANSI standard (*Digital Representation for Communication of Product Definition Data*, Y14.26M-1989) developed by the American Society for Mechanical Engineers (ASME). It is based on the work of the IGES/PDES Organization that is chaired by NIST. This group establishes information structures to be used for the (1) digital representation and communication of product definition data and (2) representation and transfer of vector graphics data used by various Computer Aided Design and Computer Aided Manufacturing (CAD/CAM) systems. ASME is currently working on Version 5.0.

MIL-D-28000, *Digital Representation for Communication of Product Data:* IGES *Application Subsets*, December 1988, identifies the requirements to be met when product definition data is delivered in the digital format of IGES as specified by ANSI standard Y14.26M. MIL-D-28000 is designed to be incorporated into a contract to define the technical requirements to be met when purchasing product definition data or product data in digital form. Product definition data is defined in MIL-D-28000 as:

> . . . the totality of data elements required to completely define a product. Product definition data includes geometry, topology, relationship, tolerances, attributes and features necessary to completely define a component part or an assembly of parts for the purpose of design, analysis, manufacture, test, and inspection.

The specification defines product data as "all data elements necessary to define the geometry, the function, and the behavior of a piece part or an assembly of parts over its entire life span."

MIL-D-28000 defines the technical requirements for the exchange of digital product data in specific application subsets. These subsets are technical illustrations, engineering drawings, and electrical/electronic applications. The technical illustration subset addresses entities that support the exchange of figures and illustrations normally found in a technical publication. The emphasis is on visual clarity for human interpretation. The engineering drawings subset is used to encode product data being acquired in accordance with DoD-D-1000 (*Engineering Drawings and Associate Lists*) for delivery in digital form. Exchange emphasis is on completeness, visual equivalency for human interpretation, and functionality of the received drawing model. The electrical/electronic applications subset addresses the representation and exchange of electrical and electronic products including printed wiring boards, printed wiring assemblies, hybrid micro-assemblies, cables, and wiring harnesses. Emphasis is on component and circuit element descriptions, their placement, their connectivity, and the routing of electrical paths.

MIL-D-28000 is currently undergoing revision. In addition to eliminating inconsistencies and redundancies, all references to ANSI 14.26M (based on IGES 3.0) have been updated to ASME Y14.26M (based on IGES 4.0). Moreover, references to DoD-D-1000 have been replaced with the document that supersedes it, MIL-T-31000, *Technical Data Packages, General Specifications for* [Ref. DSPO 1991].

An alternative to IGES for product data interchange is STEP, which is being developed by ISO (DP 10303). STEP was previously known as PDES, but the name was changed to differentiate it from the IGES/PDES Organization. STEP is in the draft stage and may undergo revision at any time. Many of the component specifications have not been defined, but early 1992 is projected as the goal for most of the component specifications to be ready [Ref. APP 1991, 39-40].

9.2.2 Standards for Graphics Services

This section reviews the Computer Graphics Reference Model, Computer Graphics Metafile (CGM), and Computer Graphics Interface (CGI). Chapter 11 reviews other graphics service standards, including the Graphical Kernel System (GKS) (see Section 11.2) and the Programmer's Hierarchical Interactive Graphics System (PHIGS) (see Section 11.3).

9.2.2.1 Computer Graphics Reference Model

The Reference Model for Computer Graphics[42] defines a basic architecture and consistent terminology for computer graphics. It addresses environment; primitives; geometry, attributes, and aspects of primitives; pictures; collections; metafiles; and archives. There are four environments: application (to which an application interfaces), virtual, logical, and physical (to which the user interfaces) [Ref. RM 1989].

9.2.2.2 Computer Graphics Metafile (CGM)

CGM standards provide a file format suitable for the storage and retrieval of picture information. The file format consists of a set of elements that can be used to describe pictures in a way that is compatible between systems of different architectures and devices of differing capabilities and design. ISO 8632 is a standard for producing a CGM in order to:

- Allow picture information to be stored in an organized way on a graphical software system
- Facilitate transfer of picture information between different graphical software systems
- Enable picture information to be transferred between graphical devices
- Enable picture information to be transferred between different computer graphics installations.

The CGM standards are:

- ISO 8632-1, *Functional Specification*
- ISO 8632-2, *Character Encoding*
- ISO 8632-3, *Binary Encoding*
- ISO 8632-4, *Clear Text Encoding*.

Vendors commonly use CGM as an exchange format for the storage, interchange, or output of a wide range of graphical pictures and numerous CGM implementations exist for use in federal procurements. Virtually all major microcomputer software products can generate and/or interpret CGM files. Moreover, most CGM implementations conform to

---

42 This model does not appear to have been published as an ISO standard.

the CALS Application Profile. CGM is considered to be mature and stable [Ref. APP 1991, 37-38].

A CGM test service was launched by NIST in May 1991. The service, which is a one-year trial program, will analyze a CGM file to see if it meets requirements that allow the transfer of pictures among different graphical software systems, graphical devices, and computer graphics installation. The two requirements used are FIPS 128, *Computer Graphics Metafile*, and MIL-D-28003, *CALS Application Profile*, December 1988.

9.2.2.3 Computer Graphics Interface (CGI)

ISO and ANSI have drafted a standard called the CGI , formerly the Computer Graphics Virtual Device Interface (CG-VDI). This provides a standard specification of the control and data interchange between device-independent graphics software and one or more device drivers by defining an interface to a virtual graphics device. Device dependencies are allowed in limited circumstances, such as when dealing with raster entities (this is the first graphics standard to contain explicit operations dealing with raster graphics displays). It is designed as a system level interface to provide efficient device-independent access to graphics devices and processes, but provides little error checking or error handling. Character, binary, and clear-text codings are provided. This functional specification is also supported by language bindings that specify the exact name for each operation, its parameter sequence, and data types for the parameters.

The ISO/IEC approach to defining a CGI is provided in DIS 9637, *Interfacing Techniques for Dialogues with Graphical Devices* - CGI *Data Stream Encoding*. The standard comprises 3 parts, part 1 of which is currently undergoing review:

- Part 1: *Character Encoding* (review period ends 19 November 1991)
- Part 2: *Binary Encoding*
- Part 3: *Clear Text Encoding*.

The governing CGI standard is DIS 9636, which has the following parts:

- Part 1: *Overview, Profiles, and Conformance*
- Part 2: *Control, Negotiation, and Errors*
- Part 3: *Output and Attributes*
- Part 4: *Segmentation*
- Part 5: *Input and Echoing*
- Part 6: *Raster*
- Part 8: *FORTRAN Language Binding of* CGI *(working draft)*
- Part 11: C *Language Binding of* CGI *(working draft)*.

DIS 9638 comprises the language bindings for CGI . Its parts are as follows:

- Part 1: *FORTRAN*

- Part 2: *Pascal*
- Part 3: Ada
- Part 4: *C*.

Although CGI is expected to be published in the final quarter of 1991, early versions of CGI implemented by IBM and AT&T have yielded workstation managers that are already becoming the industry's *de facto* standards [Ref. Wexelblat et al. 1991].

9.3 Geographical Data Exchange

This section covers the US military and government, foreign, and commercial standards and standardization activities in geographic information exchange. Digital cartographic and geographic information systems have existed for several years; however, their widespread use has been impeded by difficulties in data collection and the need for information sharing standards. Perhaps the most fundamental distinction between the digital representation of cartographic data and the conventional printed graphic is the need to explicitly and unambiguously code the attributes and spatial relationships among the various data elements. Because of the massive amounts of information that must be stored, data compression is a related topic of interest (see Section 9.4).

Specific CCIS requirements for the processing and interchange of maps and geographical information include the abilities to:

- Display and transfer a working color map between two or more headquarters
- Change map features, post symbols, and have zoom capability
- Received, store, process, display, and integrate all environmental data [Ref. IDA 1991, 157].

Requirements for use of geographic information systems (GISs) for command and control are being treated in several international forums. In October 1989, a symposium on GISs was held at the SHAPE Technical Centre in The Hague. This symposium addressed requirements, standards, and implementation aspects of GISs for military application. Examples of digital data that may be required for military use of GISs are [Ref. Baybrook et al. 1990]:

- Electronic maps and tactical terrain data.
- Intelligent spatial data, to include maintaining topological relationships interactively, presenting a feature-based view of the data in which attributes can be easily requested interactively, supporting high-speed interactive queries (for which parallel processors and rule-based software may be required), and maintaining prioritized feature symbolization during creating and editing of feature data.
- Topologically structured vector data to support exchange and display of electronic maps, tactical terrain data, and user-generated queries. Features and attributes of the features are associated with points, lines, and areas. Each

geographic element is captured and stored only once, together with attributes and relationships to other elements.

- Intelligence collection, data fusion, and intelligence preparation of the battlefield.
- Battle management, mission planning, tactical maneuver, and interdiction.
- Fire support and close air support.
- Antisubmarine warfare.

Digital cartographic and geographic standards generally address (1) encoding or (2) exchange. Typically they reference one another. Currently, all exchange standards are designed for removable media as opposed to establishing communication protocols for exchanging cartographic and geographic information.

There are four basic types of digital cartographic and geographic data:

(1) Digital elevation data

(2) Digital planimetric data

(3) Digital land use and land cover data, and

(4) Digital geographic names data.

Several United States Geological Survey (USGS) circulars cover these types of data:

- FIPS PUB 70-1, *Specifications for Representation of Geographic Point Location for Information Interchange,* 1986 [USGS Circular 878-B]
- FIPS PUB 103, *Codes for Identification of Hydrologic Units in the United States and the Caribbean Areas,* 1983 [USGS Circular 878-A]
- USGS Circular 895-B, *Digital Elevation Models*
- USGS Circular 895-C, *Digital Line Graphs from 1:24,000 Scale Maps*
- USGS Circular 895-D, *Digital Line Graphs from 1:2,000,000 Scale Maps*
- USGS Circular 895-E, *Land Use and Land Cover Digital Data*
- USGS Circular 895-F, *Geographic Names Information System.*

FIPS PUB 70-1 specifies a uniform format for representing geographic point location data in digital form for purposes of information interchange among data systems. It applies only to the three coordinate systems most widely used in the United States to define the position of a point that may be on, above, or below the earth's surface.

FIPS PUB 103 adopts the set of codes used to identify hydrologic units published in Geological Survey Circular 878-A. These codes identify a hydrologic system that divides the United States and Caribbean outlying areas into 21 major regions. These regions are further subdivided into approximately 2,150 units that delineate river basins having drainage areas usually greater than 700 square miles. The codes provide a standardized base for use by water-resources organizations.

In response to a special study chartered by the US Joint Requirements Oversight Council (JROC), the Defense Mapping Agency (DMA) established a program of standardization on 6 August 1990, the goal of which is to develop a comprehensive suite of standards for exchanging, manipulating, and displaying digital Mapping, Charting, and Geodesy (MC&G) data. The Mapping, Charting and Geodesy Technology (MCGT), standardization area will provide for the compatibility and interoperability of digital MC&G databases supporting a wide variety of simulators, command and control, and weapons systems. [Ref. DMA c1990]

Several US military specifications cover digital geographic information exchange:

- MIL-D-89000, *Digital Terrain Elevation Data (DTED)*, 26 February 1990
- MIL-D-89005, *Digital Feature Analysis Data*
- MIL-A-89007, *Arc Digitized Raster Graphics.*

The first of these, MIL-D-89000, defines the requirements within the DMA's DTED database, which supports various weapon and training systems. The purpose of MIL-D-89000 is to assure uniform treatment among all mapping and charting elements engaged in coordinated production and maintenance of this type of data. The U.K. MoD has related standards, *Digital Terrain Elevation Data* and *Digital Feature Analysis Data.*

The NATO STANAGs relevant to this area include:

- STANAG 3809, *Digital Terrain Elevation Data Exchange Format*
- STANAG 3985, *Preferred Magnetic Tape Standards for the Exchange of Digital Geographic Information*
- STANAG 3986, *Digital Data File Transmittal Form for Geographic Information.*

9.3.1 Digital Geographic Information Exchange Standard (DIGEST)

The 11-nation[43] Digital Geographical Information Working Group (DGIWG) is working on DIGEST. DIGEST may be submitted to ISO, but no definite plan for this has been identified. The present concern is for magnetic tape exchanges, with electronic communications exchanges possible in the future.

DIGEST is intended for standardizing exchanges of digital geographic data and making compatible the digital data products of the participating nations; the final draft of the standard was produced in October 1989. This draft was developed to accommodate the exchange of multiple data sets of different data structures using a single format. DIGEST has two parts. The Generic Standard is supplemented by the Minimum Standards Specifications, which are single-data-structure oriented subsets of the Generic Standard. Whereas the generic standard contains the necessary file, record, field, and subfield

[43] The seven member nations are France, Germany, Italy, the Netherlands, Norway, the United Kingdom, and the United States. The four active observers are Belgium, Canada, Denmark, and Spain.

definition and implementation details to exchange all data structures supported by the standard, each minimum standard specification is geared towards one particular data structure and serves as the basis for the exchange of data only in that structure. The current standard supports the following [Ref. Schneider 1990]:

- Vector topologically structured data, which includes association of features with individual nodes (e.g., water tower), edges (e.g., two-lane highway with an asphalt surface), faces (e.g., forest of deciduous trees), and collections of features associated to nodes, edges, and faces (e.g., Route 1 for a series of line features or city for a collection of three types of features).
- Color-coded and red-green-blue (RGB) coded raster data:
  - An RGB raster image is a collection of red, green, and blue color bands, which when combined for display purposes form the original color of the source graphic.
  - A color-coded image represents each unique color of a scanned graphic as a series of pixels which represent the information on the original source graphic that utilized that color.
  - The raster structure supports use of subsets and merged sets.
  - The raster structure also supports user-defined parameters to indicate scan direction and row and pixel sequencing, which are required for exchanging data derived from scanners that have different capture methods.
- Feature Attribute Coding Catalog (FACC) for feature identification:
  - Features are associated with spatial coordinates or sets of coordinates.
  - Attributes may be associated with features and may serve to designate width, length, material composition, etc.
  - The initial version of the FACC has 300 feature codes and 125 attribute types with associated values. The FACC includes a recommended attribute set for each feature code.
- Transmittal Header File to describe characteristics of the entire transmittal (e.g., originator, edition of the exchange specification used, number of data sets in the transmittal, and security and release information for the transmittal).
- Header information files to describe global characteristics of each data set being exchanged [e.g., quality (currency, accuracy, and completeness), source, projection type, coordinates of the geographic limits of the data set, data structure type]. Qualities can be associated with features and attributes as well as with data sets.
- ISO media standards [using ISO 9660 for Compact Disk-Read Only Memory (CD-ROM) and ISO 1001 for magnetic tapes].
- Security labeling.
- Format implementation compliant with ISO 8211, *Specification for a Data Descriptive File for Information Interchange*. ISO 8211 is being updated to (1) provide support for compound arrays (concatenated regular data structures); support for extended (multi-byte) character sets; better-specified support for simple binary data, and support for fixed point, floating point, and complex binary data; and (2) support recursive tree structures in level 3. The revision is at the working draft stage [SC21 N 6128, 14 June 1991], but CD status is

expected in December 1991. The statement of work for the revision is SC21 N 6129.

Standards for two other data structures are being developed for the 1990 version of DIGEST: matrix (to support exchange of elevation data) and spaghetti vector (to support exchange of non-topological vector data).

DGIWG's position is that DIGEST data should be exchanged between map-producing agencies, such as the Defense Mapping Agency (DMA), and not between operational units. Standards governing exchanges between field systems are the responsibility of the system development organization. This is a traditional view in military systems development organizations and leads to substantial interoperability problems, particularly intra-national. The official position notwithstanding, the DGIWG is encouraging the distribution of DIGEST by its member nations to the widest possible audience, including the military services and civilian users.

9.3.2 Geographic Document Architectures

The Directorate of Cartography at the Canadian National Defence Headquarters has proposed that geographic exchange standards be built on a document architecture similar in scope to ODA (see Section 9.1.1). This architecture would address, as does DIGEST, a range of physical media such as magnetic tape and CD-ROM. It would also address exchange of partial data sets and geographic "document" organizations. Unlike DIGEST, the architecture would not attempt to define the sets of feature codes and attributes, which are seen as dependent on political jurisdiction and intended use. For example, Canada must incorporate more geographic ice feature types in hydrographic charts than many other countries. The proposed architectural concept views the architecture as a vessel that carries various properly labeled containers of information. Specification of the channels for transporting the vessel are left, as with ODA, to OSI or other means outside the scope of the architecture. Encapsulation of data for telecommunications would use ASN.1 (ISO 8824 and 8825) and for physical media interchange by ISO 8211. Coding of the information would use such presentation standards as ASCII or ISO 646 for basic text; ISO 6937, *Supplementary Characters*, for accents to the text, other alphabets (e.g., ISO 2375, *Non-Latin Alphabets*), and ISO 9292, *Picture Coding*, for pictorial information [Ref. McKellar 1990].

9.3.3 SIMNET Common Geographic Data Model

The US SIMNET program has developed a geographic data model to integrate such heterogeneous data types as digital terrain models, traditional maps, and satellite and aerial imagery and such specialized tools as digital imagery workstations, GISs, relational DBMSs, and high-performance graphics workstations. The data model was defined using ASN.1, which provides a concise, unambiguous means of specifying abstract data types. The current specification, SIMNET Database Interchange Specification [Ref. Lang et al.

1989], recasts the specification of the data model into a relational data framework in order to take advantage of relational database management and query capability.

The data model represents features in spatial and non-spatial components that can be further subdivided for separate handling and also reassembled to recover the complete feature description. Entities in SIMNET (and many other GIS applications) are represented as objects. For example, networks are represented as collections of line segments, landcover is represented by polygons, terrain is represented by a triangulated mesh, and modeled objects as collections of points, line segments, and triangles. Classes of these object types (such as a class of tree representations) are generated for use in SIMNET data model. Further, the data model permits the enlargement of classes and addition of new classes of objects. For example, several classes of trees are required for simulation: sets of individual trees, collections of irregular groups of trees, lines of trees, uniformly wooded areas, and generalized surface vegetation.

The spatial model represents the physical aspects, including their visual appearance and the intervisibility of pairs of objects (one hides a part of the other). The spatial model encompasses the geometric description, the location, and the orientation of an object within some spatial frame of reference. The spatial model includes aspects that are expected to change only rarely (e.g., the underlying coordinate system) and the modifications are generally only to enhance the fidelity of the representation or the performance (e.g., through data compression). As in DIGEST, the spatial model is based on points, line segments, and triangles. It also includes tetrahedrons for three-dimensional objects, as well as a standard technique from algebraic topology called simplicial complexes to relate the various geometric elements. In this technique, triangles are 2-simplexes, line segments are 1-simplexes, and the three line segments that make up a triangle are functions of the vertices of the triangle.

The non-spatial aspects for simulation may change during execution of a simulation and are therefore expected to be dynamic. These aspects are treated as attributes of objects as a whole or to a component. Examples of non-spatial attributes are color, weight, power, and composition [Ref. Lang et al. 1990].

9.3.4 IHO Committee for the Exchange of Digital Data (CEDD)

The International Hydrographic Organization (IHO) is developing standards for the exchange of digital hydrographic information. The work is being done by the CEDD. No world-wide standards have yet emerged from this work. One effort of IHO, called the North Sea Project, is establishing an electronic chart database, testing the contents of this database for electronic chart display systems, and evaluating methods of electronic navigational chart updating [Ref. Stene 1990].

9.3.5 NATO Geographic Conference

The NATO Geographic Conference meets annually (usually in June) to manage and coordinate digital geographic information production in support of NATO plans. The primary tasks are to [Ref. Matthews 1990]:

- Identify common national and NATO requirements for digital geographic information
- Recommend priorities for international cooperative production
- Recommend outline production responsibilities for national agreement
- Recommend outline rules and procedures for operational geographic support and its coordination.

9.3.6 Digital Chart of the World (DCW)

The DCW is a research and development project of the US DMA to develop, refine, and establish a suite of standards that enable the exchange of spatial data on a variety of exploitation systems. The DCW will employ a topologically based vector structure and provide digital representation of land surface information on 30-40 CD-ROMs. The coverage will be world wide and the major source will be the 270 maps of the 1:1,000,000-scale Operational Navigation Chart series. The DCW will be the forerunner for deployed digital databases derived from DMA's Digital Production System (DPS), which is scheduled to produce 31 standard products in 1991. A Map, Chart, and Geodesy Feature Data Exchange structure is being defined to archive and exchange DPS products.

9.3.7 Vector Product Standard (VPS)

This standard is currently in a prototype stage, but nearing finalization. A military standard was expected to have been issued in early 1991. Although the draft standard is being distributed to the civilian community, there are currently no plans to offer VPS as a civilian standard.

9.3.8 Spatial Data Transfer Specification (SDTS)

The United States National Committee for Digital Cartographic Standards, a multi-agency working group headed by the USGS which is responsible for most of the US non-military geographic information exchange standards has issued SDTS. The DMA was an original participant in the development of this standard, but dropped out in favor of its own activities. On July 26, 1990 SDTS was submitted to NIST for approval as a FIPS. A revised version was resubmitted to NIST on April 8, 1991. Following approval as a FIPS, the USGS is prepared to submit the SDTS to ANSI for promotion as an ANSI standard and then to ISO for promotion as an ISO standard.

The SDTS include definitions of terminology, a spatial data transfer specification, methods for reporting digital cartographic data quality, and topographic and hydrographic

entity terms and definitions. The standard will allow users to transfer digital spatial data sets in a variety of formats between dissimilar computing systems. To support the SDTS, the USGS will coordinate the development of a suite of software tools to assist users in interfacing with the standard. These tools will include the capability to encode and decode the standard from user-specified data models and formats and to encode and decode SDTS data sets to ISO 8211 *(Specification for a Data Descriptive File for Information Interchange)* [Ref. McDermott 1991].

Other standards under development by USGS include:

- Aquifer names and geologic unit codes
- Classification of wetlands and wildlife services
- EPA (Environmental Protection Agency) parameter codes
- Codes for taxonomic identification of flora and fauna
- Land use and land cover codes
- Public land survey codes
- Cartographic attribute/feature codes.

9.3.9 British Standard Specification for Geographic Information

Draft British Standard BRDF, *British Standard Specification for Geographic Information--National Transfer Format (NTF),* is a standard for the exchange of digital map data between organizations. The NTF is designed for all types of raster/grid and vector map data. The specification defines media-independent file and data record descriptions for information exchange; description of data elements, vectors, and arrays containing character strings and numeric forms; relationships between data elements; and volume and header information that enables data interchange to occur with minimal specific external description. BSI 91/65602, dated 24 July 1991, is in Release 1.2. It is being developed by the British Standards Institute Technical Committee 36, a new committee on geographic information that was set up in 1991 within the Association of Geographic Information which is acting as Secretariat.

9.4 Data Compression

An area closely related to map and geographic information is data compression since maps require large quantities of data. For example, at a scale of 1:1,000,000 a digitized map of the world requires 30 CD-ROMS. The Army wants maps that are 1:250,000 and 1:50,000. The use of data compression is not limited to maps however, as the use of complex computer graphics proliferates in areas such as desktop publishing, engineering, and industrial design. Currently, individual manufacturers, software developers, and computer services have adopted their own internal storage formats and data compression algorithms. What is needed is a unifying standard [Ref. Carlson 1991].

Some of the available image storage standards and commercial software implementations of data compression schemes include [Ref. Carlson 1991]:

- Utah RLE (Run Length Encoding) - University of Utah
- TIFF (Tag Image File Format) - Aldus and Microsoft
- PICT Version 2 (Macintosh) - Apple
- IFF (Interchange File Format) - Electronic Arts
- GIF (Graphics Interchange Format) - CompuServe
- TGA (Targa Image Format) - Truevision, Inc.
- Sun Rasterfile - Sun
- GKS (treated separately as a graphics standard; see Section 11.3)
- CGI (see Section 9.2.2.3)
- CCITT Recommendation T.4 (Fax).

These are several emerging data compression activities that may become standards:

- Joint Photographic Experts Group (JPEG). The JPEG, a joint project of IEC/ISO and CCITT, has issued a proposed standard currently referred to as the JPEG standard (CD 10918). The JPEG standard was originally conceived as a companion standard to Group 3 and 4 facsimile standards covering compression and decompression of still-frame, continuous-tone, photographic (gray scale or color) digitized images. The current JPEG Draft Specification (JPEG-8-R5 dated 1/2/90) is in its fifth revision [Ref. Haber 1991]. It comprises two parts. The first part specifies four modes of operation, the different codecs specified for those modes, and the interchange format. It also contains implementation guidelines. It began the CD ballot process in February 1991 as CD 10918-1. Part 2 specifies compliance tests and began CD ballot in June 1991 as CD 10918-2 [Ref. Wallace 1991]. Several vendors have already introduced JPEG-compatible products [Ref. Haber 1991]. A second standard that deals with still pictures, JBIG (Joint Bi-Level Imaging Group) is also under development.
- JBIG will be used to compress bi-level images such as black-and-white photos or pages of text. While pixels can be eliminated without the loss being perceived in the continuous-tone images that JPEG deals with, JBIG deals with simpler images where there can be no image distortion. A final version of the JBIG standard is about 18 to 24 months away. Currently, there are no available JBIG implementations [Ref. Haber 1991]. A third proposal for video compression is under development by the Moving Picture Experts Group (MPEG).
- ISO/IEC/JTC1/SC2/WG11 committee work on MPEG (CD 11172, December 1990) began in 1988 with the goal of achieving a standard by 1990. MPEG-Video is addressing compression of video signals at 1.5 Mbits. MPEG-Audio is addressing compression of digital audio signals at rates of 64, 128, and 192 kbit/s per channel. MPEG-System is addressing the issue of synchronization and multiplexing of multiple compressed audio and video bit streams. Products are expected as early as 1992 [Ref. LeGall 1991].

- Digital Video Interactive (DVI). DVI uses a proprietary compression scheme that is backed by Intel Corporation, IBM, and AT&T. IBM and Intel are already marketing DVI products for personal computers and it has the potential to become a *de facto* standard.

JPEG's interest in data compression stems from a desire to transmit digital representations of photographs by facsimile. To achieve the desired levels of quality for both color and black and white requires large amounts of data and transmission time. The MPEG is looking at data compression techniques for motion pictures, reducing the data needed to represent each frame and taking advantage of the redundancy from one frame to the next.

ASC ANSI X3 recently announced the approval of a new project on *Data Compression, Adaptive Coding with Sliding Window for Information Interchange* under the auspices of Technical Committee ANSI X3B5, *Digital Magnetic Tape*. This standard will represent the minimum requirements for the generation of a compressed encoding of data for the interchange of information between systems and provide an effective encoding which results in the compression of data typical to information processing systems. [Ref. X3 1991k]

9.5 Video Data Exchange

Future CCIS will depend on video technology for multimedia information exchanges, training, and intelligence gathering. CCIS may need to store and transmit such video images to analysts at distributed locations [Ref. IDA 1991, 162].

Most of the standards in this area appear to have come from the television industry, specifically, in the United States, the Society of Motion Picture and Television Engineers (SMPTE). The International Radio Consultative Committee's (CCIR) Recommendation 601, *Encoding Parameters of Digital Televisions for Studios* was published in 1982.

CCITT Recommendation H.261, *Video Codec for Audiovisual Services at px64 kbit/s* (commonly referred to as the px64 standard) is a video coding standard that was approved in December 1990 A slightly modified version is under development by ANSI T1.64, *Digital Processing of Video Signals - Video Coder/Decoder for Audiovisual Services at 56 to 1,536 kbit/s*. A draft was issued in October 1990 [Ref. Liou 1991].

The real-time simulation community is currently faced with a tradeoff between standards or high-speed performance since available computing power is inadequate to support standards. MIL-STD-1379D, *Military Training Programs*, also addresses video, as does Multi-Media Extensions to Microsoft's Windows (*de facto*).

In addition, High Definition Television (HDTV) will require studio, exchange, mission, and display standards. For none of these does a single international standard seem likely. In the United States, the FCC intends to issue HDTV standards in the spring

of 1993. Six alternatives are under consideration. Evaluation of alternatives is expected to be completed in 1992 [Ref. IDA 1991, 165].

9.6 Audio Exchange Standards

Integrated voice technology is another future CCIS requirement. Some possible applications include:

- Voice mail
- Multimedia documents for training and maintenance
- Computer-generated speech for "eyes-on" situations [Ref. IDA 1991, 166].

In March 1991, ASC X3 announced the approval of two new standards projects on Voice Messaging:

1. *Voice Messaging over MOTIS ISO 10021* is being developed by Task Group ANSI X3V1.4 as a standard protocol for voice messaging to permit the interchange of information objects effectively between various vendors' message systems.
2. *Standard User Interface to Voice Messaging* is being developed by Task Group ANSI X3V1.9 to provide users of voice messaging systems with a consistent mode of interaction in a way that is independent of underlying system implementation. The standard will apply only to Touch Tone telephones. Alternative interface technologies such as speech recognition or screen-based interfaces are not included.

The CCITT I Series of Recommendations for Integrated Services Digital Network (ISDN) (see Section 6.3.8.3 and 9.3.4) seeks to combine audio, video, and data transmission on a single system. Currently, the service is limited to a number of disconnected areas since most of the long distance trunk service has not been converted [Ref. IDA 1991, 166].

Future versions of MIL-STD-1379D (see Section 9.5) are expected to include standards for digital audio. The Interactive Multimedia Association is currently working on this. The ODA (see Section 9.1.1) is also designed to allow for extensions including additional types of content such as sound. In addition, CCITT G.721 is a standard audio encoding method.

A larger issue is that of integrating all these nascent standards efforts by developing a framework or reference model for digital multimedia. This problem has only recently been considered by ISO/IEC/JTC1. In addition to algorithms, bit streams, encoders, and decoders, both users and application programmers will need complete systems and environments. Open systems are required, each with an Interactive Multimedia Application Development/Utilization Environment including some or all of the following [Ref. Fox 1991]:

- Multimedia data capture tools
- Multimedia data editors/synthesizers
- Multimedia scripting language tools
- Multimedia data integrator/sequencer tools
- Multimedia database and storage/retrieval layout tools
- User interface development tools
- Simulation, testing, and publishing assistance tools
- Archiving, versioning, backup, and recovery tools
- Project management tools
- Run-time support environment for application use.

Developing a framework is but one suggestion of the ISO/IEC JTC1 Ad Hoc Technical Study Group on Multimedia and Hypermedia. Other tasks include:

- Discussing and recording a procedural plan for establishing multimedia and hypermedia requirements and a procedure for communicating these requirements among the relevant groups within JTC1
- Preparing a report on the general concepts and definitions related to multimedia and hypermedia and trying to reach agreement on general concepts.

SC18 has been given the responsibility for developing the framework. SC 18 will work closely with the Multimedia/Hypermedia Experts Group (MHEG) (JTC1 SC2/WG12) in developing the Audio Visual Interactive (AVI) Scriptware work item (JTC 1 N 809) as a two part standard:

- Part 1: *Functional definition,* being the responsibility of SC 18
- Part 2: *Encoding,* being the responsibility of SC29 [Ref. JTC1 N 1161 1991].

9.7 Assessment of Coverage by Standards

In the area of document exchange, standards exist that would fulfill a CCIS's requirements. There is evidence that these standards are stabilizing as Document Application Profiles (DAPs) begin to appear. A decision that a CCIS may need to make is whether to adopt the ODL or SGML for its interchange format. While both can be used with ODA and information can be transferred between the two formats, there are some advantages to using SGML. Not only does CALS use SGML, but more commercial products are available for it than for ODL. Moreover, it is human-readable, preserves user file divisions, and is extensible to other architectures. Finally it possesses a broader information processing orientation than does ODL, which is concerned solely with document processing. An argument against using the CALS standard as a model is that it is oriented to technical weapons systems support documentation which may not be appropriate to a CCIS.

The status of technology in the area of data interchange is such that standards do not yet manage information as a database where content is encoded and structure and form attached.

US EDI standards are not entirely aligned with international EDI standards, which poses potential interoperability problems.

Graphics services standards all appear to be stable and mature with a high level of consensus and product availability. However, none address the question of distributed graphics. A common intermediate standard is needed to exchange graphics data stored on different platforms.

The remaining data interchange standards areas (geographic, data compression, video, and audio) are far less stable and mature. A lack of standards has impeded the widespread use of digital cartographic and geographic information systems. For example, standards establishing communications protocols for exchanging cartographic and geographic information do not exist. Harmonization of the emerging efforts is another potential problem. A CCIS proponent will need to monitor standards developments in these areas as well as in the area of multimedia standards where standards are generally lacking. For example, one promising technology that has been crippled by a lack of standards is multimedia mail [Ref. Borenstein 1991].

10. USER INTERFACE SERVICE STANDARDS

10.1 Requirements for User Interface Services

Quick Reference	
Topic	Page
Assessment	237
HCI Stds Organizations	228
OPEN LOOK	236
MOTIF	236
Reference Models	235
Requirements	227
Terminal Mgmt (TM)	232
Virtual Terminal (VT)	230
Visual Disp Term (VDT)	229
X-Windows	233

User interface services specify the human-computer interface (HCI), terminal management services, and interactions with virtual terminals. Such standard interfaces are needed to ensure a high degree of application portability and to provide a consistent look and feel across multiple implementations. An overview of standards for user interfaces is given in Table 20.

The user interface services provide a consistent way for applications programs, operating systems, and various system utilities to gain access to the people who develop, administer, and use a system. A CCIS architecture addresses not only the technical features of the user interface but also the human engineering considerations. User interface services address client-server operations, object definition and management, window management, and dialog support.

10.2 Standards for User Interface Services

Human-computer interfaces comprise two levels of standardization. One level is the specification of how computer system elements shall interface to display terminals, workstations, and other output devices for which there is capability for human interaction. The second level is the look, feel, and layout of the display screens, keyboards, and other elements of the workstation that would define the way information is displayed and how the user interacts with the information provided. For CCISs, the recommended technical approach is to standardize the interfaces. This is distinct from the military necessity of standardizing information formats and presentations at workstations for operational reasons.

Table 20. Status Overview of Key User Interface Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
X Window Sys.	●	○	○	●	●	●	
XVT		○	○				

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

10.2.1 HCI Standards Organizations

The standards work in ISO/IEC covers both levels of HCI. These standards activities seek to:

- Provide consistency--in screen and keyboard layout, terminology, semantics, user action, and syntax--across and within manufacturers, systems, and applications
- Enhance comfort and well-being
- Enhance usability[44]
- Assist in product procurement and evaluation.

Specifically, ISO/IEC JTC1 SC18 (Text and Office Systems) has a working group, SC18/WG9 (User System Interfaces and Symbols), that is developing standards to support keyboard layout, user interfaces, cursor control, and icons (e.g., symbols) to be displayed. In addition, the Ergonomics Technical Committee (TC159) of ISO is addressing, through SC4 (Signals and Controls) and WG5 (Software Ergonomics and Man-Machine Dialogue), standards for dialogue interface, coding, formatting, menus, and usability assurance. Other areas of standardization related to the user interface to information systems being addressed by ISO are [Ref. Bevan 1989]:

- Documentation (JTC1 SC7/WG2)
- Software quality characteristics (JTC1 SC7/WG3)
- Text interchange (JTC1 SC18/WG4)
- Terminal management (JTC1 SC21/WG4)
- Form Interface Management System (FIMS) (JTC1 SC22)
- POSIX (JTC1 SC22/WG15)
- Commands for interactive text searching (TC46/SC4)
- Software quality assurance (TC176 SC2/WG5).

Other groups working on HCI standards include:

- CCITT Study Group X, Working Party 1, Man-Machine Language
- Human Factors Society, Human Computer Interaction Committee
- ANSI X3V1.9, User System Interfaces and Symbols
- IEEE Steering Committee on User Interface
- IEEE Project 1201, Window Interface for User and Application Portability
- Open Software Foundation (OSF)'s MOTIF Graphical User Interface (GUI)
- Unix International (UI) OPEN LOOK GUI [Ref. SUN 1990]

---

[44] As used in SC18/WG5, usability of a product is defined as the degree to which specific users can achieve specified goals in a particular environment effectively, efficiently, comfortably, and in an acceptable manner.

- Information Industry Association
  - Voice Messaging User Interface Forum (VMUIF)
  - Voice/Fax User Interface Forum (VFUIF) [Ref. Reed et al. 1991].

10.2.2 Visual Display Terminal (VDT)

Although work has been underway for several years on the hardware user interface standards, now known and approved as Human Factors Society (HFS)/ANSI 100-1988, Human Factors Engineering of Video Display Terminal Workstation Standard, little work has begun on software user interface standards. The HFS Technical Standards Common Human-Computer Interaction was formed in 1985 to evaluate the feasibility of software user interface standards. It has submitted a fully-reviewed document on menu-based dialogue design to the ISO Working Group on Software Ergonomics (TC159/SC4/WG5) [Ref. Reed et al. 1991].

SC18/WG9 seeks to develop a User Interface Standard that would address names of basic objects and actions, user guidance, dialogue interaction, and graphical symbols used on screens. The standard is CD 9995: *Information Technology - Keyboard Layouts for Text and Office Systems*. The current parts represent a recombination of material that was formerly presented in 21 parts. The seven parts, six of which have been distributed for balloting at the CD level are:

- CD 9995-1, *General Principles Governing Keyboard Layouts*
- CD 9995-2, *Alphanumeric Section*
- CD 9995-3, *Common Secondary Layout of Alphanumeric Zone of Alphanumeric Section*
- DP 9995-4, *Principles Governing the Placement of Characters and Symbols on Keys*
- CD 9995-5, *Editing Section*
- CD 9995-6, *Functional Section*
- CD 9995-7, *Symbols Used to Represent Functions*.

WG9 has also distributed working drafts of two components of an as-yet unnumbered standard for icons used on screens. The standard is intended to apply to systems implementing the desktop metaphor, although icon system suitable for other application fields may be future subjects of standardization [Ref. Billingsley 1990]. ANSI X3V1.9 is the US Technical Advisory Group to WG9.

TC159/SC4/WG5 is developing a standard (ISO 9241) for VDTs that addresses office task requirements, visual requirements, keyboard ergonomics, work place design and environment, surfaces and filters, use of color and graphics, non-keyboard input devices, usability, coding, formatting, and terminology. The status of the standards in ISO 9241, *Ergonomic Requirements for Office Work with Visual Display Terminals*, is as follows:

- ISO 9241-1, *Introduction*
- ISO 9241-2, *Task Requirements*
- DIS 9241-3, *Visual Display Requirements*
- DIS 9241-4, *Keyboard Requirements*
- CD 9241-5, *Workstation Layout and Postural Requirements*
- CD 9241-6, *Environmental Requirements*
- CD 9241-7, *Display Requirements with Reflections*
- CD 9241-8, *Requirements for Displayed Colors*
- CD 9241-9, *Requirements for Non-Keyboard Input Devices*
- WD 9241-10, *Dialogue Principles*
- CD 9241-11, *Usability Statements*
- CD 9241-12, *Presentation of Information*
- WD 9241-13, *User Guidance*
- CD 9241-14, *Menu Dialogues*
- WD 9241-15, *Command Dialogues*
- WD 9241-16, *Direct Manipulation Dialogues*
- WD 9241-17, *Form-Filling Dialogues*
- XX 9241-18, *Question and Answer Dialogues* (not yet started)
- XX 9241-19, *Natural Language Dialogues* (not yet started).

10.2.3 Virtual Terminal (VT)

VT standards (ISO 9040 and 9041) define a communications protocol between a terminal and its host in terms of a conceptual terminal, where the mapping from the conceptual terminal to the physical device is an implementation issue outside the standard. Several classes of display and data manipulation capabilities will eventually be addressed by VT standards [Ref. OSN 1989b]:

- Basic class, for textual data in a rectangular array of character boxes
- Forms class, similar to the basic class, but with the ability to define fields with control over data entry
- Graphics class, for geometric data such as lines and circles (as defined, for example, in GKS)
- Text class, for structured data such as provided by ODA data streams
- Image class, for bit-mapped displays.

The initial VT standards address the basic class of capabilities. They will contain addenda that provide extensions (AD1, *Extended Facility Set*) to the basic class for enhanced access rules, structured control objects, blocks, fields, and reference information objects. These enhancements will be incorporated into the base text before the standards are submitted for ballot as international standards. Three additional extensions are being

developed [SC21 N 3366 and N 3367, December 1988] for VT: ripple, to provide facilities to undertake simple text editing by the addition of control objects and operations; exception reporting for non-fatal errors; and context retention for multiple VT sessions. These extensions have been progressed as Amendment 2 (AM 2, *Additional Functional Units*) to both ISO 9040 and 9041.

DIS 9041-2, *VT PICS Proforma*, 25 April 1991 [SC21 N 5702; IST/21:2745], is being developed. An editing meeting was scheduled for November 1991. SC21/WG5 expects to reach IS status for the PICS Proforma in February 1992. In addition, registration authority procedures have been developed for the Virtual Terminal Environment (VTE) and VT Control Objects: ISO 9834-4 and ISO 9834-5, respectively. Finally, a guide to VT standards has been developed by SC21/WG5 [SC21 N 3365, December 1988]. A draft international standard *Conformance Test Suite for the VT Protocol* (DIS 10739-1) has also been developed. This is expected to become a standard in July 1992.

Amendment 2 [SC21 N 6270 and N 6271, 12 June 1991] for ISO 9040/9041 enhances the capability of the VTE by use of the Association Establishment or Negotiation functions, extends the set of objects and operations provided by the Data Transfer function, and enhances error handling capabilities of the service provider. Amendment 2 provides additional functionality for ripple mode editing (insertion, deletion, and copy operations for a Display Object), exception reporting (provides mechanisms by which non-fatal exception conditions may be reported by the VT service provider to both VT users), and retention of VT context across Negotiation (retention of the information stored in selected VT Objects--Display Object and Control Objects--to be retained between successive VT environments within the life time of a VT association).

VT profiles are being developed by two regional workshops: the EWOS and the NIST OSI Implementor's Workshop. EWOS is working on synchronous-mode profiles that are based on a two-way exchange with a single display object requiring the exchange of an access token. EWOS profiles include Forms, Page, Enhanced, and Enhanced Page. The NAOIW is developing asynchronous-mode profiles. These are based on a character-by-character interworking, in which there are two display objects, but the user at each end is allowed to update only one of the objects. NAOIW profiles include TELNET, Transparent, Forms, Scroll, Page, and X29 (of which the first three are in the Stable Agreements).

In May 1991, SC21/WG5 generated an output document for study and comment on the possibility of supporting interactive access to ODA data structures through an extension of the VT protocol. [Ref. SC21 N 6227 1991]

10.2.4 Terminal Management (TM)

SC21/WG5 is working on a program for developing standards for TM, directed at support for multi-function workstations. The role of TM is to support the control and

manipulation of logical devices typically associated with workstations. Logical devices are defined in TM to provide a mapping between transferred data such as ODA documents and the physical devices such as a workstation screen, taking into account control information such as synchronization and the use policy of a particular application. TM is related to Document Transfer and Manipulation (DTAM, CCITT), user interface standards (SC18), Forms Interface Management System (FIMS, SC22), and window management (SC24). The TM standard consists of three parts: *TM Model* (CD 10184-1.2), *TM Service* (WD 10184-2), and *TM Protocol* (WD 10184-3). The first, *TM Model*, progressed to second CD status in June 1991 and is expected to progress to DIS in July 1992 and IS in July 1993. CD status for the other two is expected in December 1992.

TM provides a general framework for defining interactive processes that support in a systematic way such diverse features as: (1) combining different data types (e.g., presenting diagrams with a telephone conversation); (2) handling multiple simultaneous dialogues from a single terminal; and (3) interacting with several levels of processes in a single session, in which low-level functions such as echoing and simple checking are done locally, and responses to more demanding operations such as database access are generated by a remote system. The TM draft standards address the following requirements [Ref. SC21 N 4176 1989]:

- Presenting data from several sources on a single display, for example using a window system.
- Moving data between windows presented together.
- Supporting multiple users and displays attached to one application.
- Handling the same data at several different levels of abstraction; for example, a graphics image may need to be manipulated at the level of a display list, at the level of various geometric objects, or at the bit-map level.
- Controlling how the logical structure of dialogues is mapped onto real resources, such as open systems and OSI application associations.

TM permits the establishment of a general network of processes with dialogues between them. The dialogues may be of a variety of types, such as VT, bit-map graphics, or ODA. TM does not itself define the operation of an individual process, nor does TM define the data stream for a particular dialogue type--these are specified by other standards. Where a process has input parameters that may be adjusted, such as the specification of the positions and priorities of the various windows in a window system, these are provided by TM. The TM model addresses the following:

- Model for Terminal Management Application Service Elements (ASEs) in two or more open systems that collectively are defined as a Terminal Management Domain (TMD)
- Model for the information flows between ASEs within a TMD
- Model for the shared use of interactive resources within a TMD
- Mechanisms for the representation of information in a window environment

- Relationships between the Terminal Management ASE and other ASEs within a Single Association Control Function
- Relationship between the Terminal Management ASEs and other ASEs within the Multiple Association Control Function.

A User Descriptor Object (UDO) is defined in TM; the UDO is updated and maintained by a TM control process within a TM domain. The UDO supports the following mechanisms and requirements:

- End-user specific libraries
- User Interface Management System (UIMS) tool kits
- Local system characteristics such as devices supported, window management system information in support of specific menus and icons, peripherals to be supported during a given instance of communication, and a user clipboard for the storage of miscellaneous information
- Application-specific information (known to the user)
- Window management system and user interface dependencies, such as sizing a user interface to fit window instructions
- State information for devices supported, UIMS in general, and active and deactivated applications.

TM contains a User Window Manager Interface onto which users may interface their own window manager. If a user-supplied window manager is in place, all user requests are first sent to the user window manager. In cases where the user window manager makes decisions in conflict with the TM domain user policy, these are resolved within the TM process.

10.2.5 Status of X-Windows

The X-Windows standard effort, a UNIX-based user interface standard, began as a *de facto* standard developed at the Massachusetts Institute of Technology (MIT). It was developed by Project Athena and the Laboratory for Computer Science at MIT with funding and participation by Digital Equipment Corporation (DEC) and IBM [Ref. McCartney 1987]. Currently in Version 11 (Release 5), X-Windows sets a standard to provide portability of information across different hardware and operating systems. In contrast to the kernel-based architecture of traditional windowing systems, it has a network-based architecture. *User Interface* is based on this standard as is *DEC windows* software from DEC [Refs. Stoffel 1989; Oldenburg 1989].

The strategic direction in ISO for OSI support of windowing environments is Terminal Management. However, there is a rapidly growing demand for the use of the X-Windows system. This demand is being satisfied by the use of X-Windows clients and servers co-located in the same machine or over LANs using protocols such as TCP/IP. Some large user communities are now trying to run X-Windows over WANs and in some

cases may plan to install TCP/IP networks in competition with the emerging OSI networks based on ISO protocols [Ref. SC21 N 4189 1989].

An efficient OSI compatible way of supporting the X-Windows System in an OSI environment is needed. While it would be preferable from the standards point of view to rewrite X-Windows completely, removing the session and presentation functionality it concurrently contains, would require developmental effort and dedicated expertise that does not appear to be available. Further, by the time any such standard becomes complete, it would likely be too late to gain acceptance. Instead, on April 21, 1991, X3 announced the approval of a new project on X Window System Data Stream Definition, Part IV: Mapping onto Open Systems Interconnection (OSI) Services. This draft standard, under development by Technical Committee ANSI X3H3, Computer Graphics, represents the development of the Version 11 of X-Windows (X11) mapping onto OSI services. This mapping entails the use of the OSI Application Layer, employing the ACSE for association establishment and release and P-Data from the Presentation Layer for transmission of the X data stream encoding. OSI Application Layer naming and addressing conventions will be used [Ref. X3 1991i]. This is expected to be submitted to ISO for fast-track balloting in 1992 by SC21. The other three parts of the X-Windows standard that ANSI expects to ratify will be submitted to ISO for fast-track balloting by SC24.

Because X11 has limited two-dimensional (2D) graphics capabilities, a consortium of organizations under the auspices of MIT has developed X3D-PEX, an extension to the X11 standard that supports the Programmers' Hierarchical Interactive Graphics System (PHIGS) and the three-dimensional version of the Graphical Kernel System (GKS-3D) [Ref. Clifford et al. 1988]. PHIGS and GKSare discussed in Section 4.2.2.

Despite competition from other UNIX-based windowing systems like Sun Microsystems' *News*, *Silicon Graphics*, *4Sight*, and Carnegie-Mellon's *Andrew* [Ref. Greco 1988], X-Windows has received rapid and overwhelming acceptance as an industry standard [Ref. Anderson 1989].

FIPS-158, *X-Window User Interface,* was approved in May 1990 as a US mandatory standard. It is based on Release 3 of Version 11 of the MIT X-Windows *de facto* standard and is compatible with Release 4 which is currently available from most vendors. Since the *de facto* standard is now in Release 5, NIST plans to issue FIPS 158-1 by the 4th quarter 1992. It is anticipated that Release 5 will be available from most vendors by mid-1992. [Ref. Kuhn 1991]

10.2.6 User Interface Reference Models

FIPS-158 comprises the first three layers (Layers 0-2) of the User Interface Reference Model developed by NIST [Ref. Kuhn 1990]. The NIST Model consists of:

- Layer 0: Data Stream Encoding
- Layer 1: Data Stream Interface (Xlib)

- Layer 2: Subroutine Foundation (Xt Intrinsics)
- Layer 3: Toolkit
- Layer 4: Dialogue
- Layer 5: Presentation
- Layer 6: Application.

Layer 0 is an X- Protocol for messages between client and server. It equates with ANSI X3H3.6 (Window Management) Project 0672-D, "X Data-Stream Encoding for Window Management X Window System VII Data Stream Definition." The target date for completion of this standard is the second quarter of 1991. Layer 1 is a library interface that provides a C language interface to the X-Protocol. Layer 2 consists of basic functions for controlling windows and acts as a tool kit for building tool kits [Ref. Kuhn 1990].

An IEEE P1201 Reference Model, which is built on the NIST Reference Model, relates X, 1201 work, and other systems. IEEE Project P1201.4, "X Library" is Layer 1 of the NIST Model. Xt Intrinsics (Layer 2 from the NIST Model above) may be taken on by IEEE P1201, but a formal proposal has not yet been made for this work.

NIST Reference Model Layers 3 through 5, while not part of FIPS-158, are the subject of IEEE projects. Layer 3 is equivalent to IEEE Project 1201.1, "Toolkit--High-Level Windowing Applications Program Interface." IEEE P1201.1 is also developing a framework for interfaces for user and application portability. The toolkit layer is implemented using a collection of widgets. Several different widget sets may be used. Some of the earliest were released by MIT's Project Athena (where X was originally developed), Hewlett-Packard, and DEC. Today, the most popular widget sets are OSF's MOTIF and AT&T's OPEN LOOK. By definition, the widget layer not only provides an API, but also presents a certain look and feel to users that varies among widget sets. Much of the work of the P1201 API group thus far has been devoted to deciding whether the working draft of the API standard should be based on OPEN LOOK or MOTIF, or whether a combined approach should be taken [Ref. Mehta 1990].

Layers 4 and 5 are addressed respectively by the User Interface Language and UIMS work of IEEE Project 1201.3 and are still in the research stage. IEEE has formed a study group, but not a working group, for this work.

The GUI is part of the IEEE P1201 Reference Model but is not included in the NIST Reference Model. The GUI is the subject of IEEE Project 1201.2, "Drivability Guide," which provides a recommended practice for minimal commonality for window systems (see Section 3.4.3.3). It uses the analogy of controls for driving a car [Ref. Kuhn 1991]. A pre-draft was issued in March 1991; the standard is expected to go to ballot in the last quarter of 1992 [Ref. Martin 1990a].

10.2.7 OSF/MOTIF

The OSF/MOTIF GUI is the result of OSF's RFT process which solicited input from the worldwide computer industry for GUI technology. OSF/Motif was first released in July 1989 and incorporates technologies from Digital Equipment Corporation, Hewlett-Packard, and Microsoft. It is currently in Release 1.1.

OSF/MOTIF offers user-oriented PC-style behavior and screen appearance for applications running on any system which can support X-Windows System, Version 11, Release 3 or 4. It comprises an API consisting of a toolkit and User Interface Language (UIL). In addition, its window manager offers a standard environment for manipulating application windows. The OSF/MOTIF environment provides Native Language Support (NLS) consistent with the NLS solution proposed in the X/OPEN XPG3. The UIL can fully support display of 16-bit and compound strings, including all character sets standardized by the X Consortium, to provide localization in Asian and European languages [Ref. OSF 1990a].

In addition to being under consideration by P1201 as the basis for an API standard, the DoD CIM standards office is also considering OSF/MOTIF as an interim DoD GUI standard.

10.2.8 OPEN LOOK

OPEN LOOK, jointly developed by Sun Microsystems and AT&T is another implementation-independent GUI specification. Three toolkits can be used with OPEN LOOK:

- News Development Environment (NDE) (Sun) is an emulated PostScript interpreter modified to suspect a windowing system
- XView (Sun) implements OPEN LOOK on top of the Xlib level of the X-Window System
- Xtt (AT&T) is built upon the intrinsics level of the X-Window System.

The choice of toolkit depends, in part, on the target platform to be used: NDE and XView for the Sun, XView for DEC VAX, and Xtt for AT&T platforms. These toolkits are proprietary to Sun and AT&T, unlike the OSF/Motif toolkit. Also, unlike OSF/Motif, OPEN LOOK implementations are currently limited to eight-byte character sets and are English-based. OPEN LOOK presently receives less industry support than OSF/Motif.

10.2.9 Form Interface Management System (FIMS)[45]

Form Interface Management System (FIMS) is being developed by SC22/WG18. FIMS is a high level user interface tool that builds on top of the windowing and menu features in GUI tool kits, but at a higher level of abstraction. The distinctive features of a form are its record level interface, validation, and built-in dialog management model.

FIMS achieves a high degree of program/device independence by allowing a form to be customized for a device, taking advantage of its special features, rather than being limited to a least common denominator. It is possible to create a form that looks natural on block-mode terminals, workstations, and laser printers.

FIMS is optimized for operation in a network, where the user interface often sits on a font-end node. Dialog management facilities allow efficient user interaction. Since the API is at the record level, network traffic is minimized.

10.3 Assessment

Of all the service groups, standards for the user interface services are the least mature. This area suffers from a general lack of standards for toolkits and UIMS and at the API level itself. API directions likely to be taken over the next 5-10 years are uncertain. GUIs remain in the research stage. Standards for window management are only emerging. Neither Terminal Management (TM) nor X-Windows has reached the stage of becoming an international standard. TM has the support of ISO but its progress is slow. X-Windows has wide support in the United States and elsewhere, but the implementations are not standardized. Some issues are:

- Is there a requirement to establish a common look and feel for user interfaces? Does such a requirement come from the functional requirements, the training requirements, or from the users as a separate operational requirement?
- Is it appropriate to adopt a *de facto* standard, such as one set of X-Window interfaces? The user interface services area may be one case in which *de facto* standards must be used in lieu of international standardization.

---

[45] Discussion for this section taken from "The Standards Reporter," in *Open Systems Standards Tracking Report*, Volume 1, Number 1, October 1991, p.2.

(This page intentionally left blank.)

11. GRAPHICS SERVICE STANDARDS

This chapter reviews standards being developed for computer graphics. These include the Computer Graphics Reference Model, the Graphical Kernel System (GKS), and Programmer's Hierarchical Interactive Graphics System (PHIGS). The Computer Graphics Interface (CGI) and Computer Graphics Metafile (CGM) are discussed in Sections 9.2.2.2 and 9.2.2.3, respectively. An overview of the status of key standards for graphics services is given in Table 21.

Quick Reference	
Topic	Page
Assessment	241
GKS	239
PHIGS	240
Ref Mod Comp Graphics	239

11.1 Reference Model for Computer Graphics

The Reference Model for Computer Graphics[46] defines a basic architecture and consistent terminology for computer graphics. It addresses environment; primitives; geometry, attributes, and aspects of primitives; pictures; collections; metafiles; and archives. There are four environments: application (to which an application interfaces), virtual, logical, and physical (to which the user interfaces) [Ref. RM 1989].

11.2 Graphical Kernel System (GKS)

The GKSstandard, ISO 7942, specifies a language-independent nucleus of a graphics system. For integration into a specific programming language, GKSis embedded in a language-dependent layer obeying the particular conventions of that language. This layer (technically referenced as a "binding") has been defined for the programming language Ada in ISO 8651-3, based on the Ada *Programming Language* (ISO 8652). It has also been defined for the programming languages FORTRAN (ISO 8651-1), Pascal (ISO 8651-2), and C (DIS 8651-4).

Table 21. Status Overview of Key Graphics Service Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
GKS	●	●	●	●	●	●	●
PHIGS	●	●	●	○	●	●	●

Key: ● High Evaluation ○ Average Evaluation Blank Low Evaluation

Source: NIST, April 1991.

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

[46] This model does not appear to have been published as an ISO standard.

GKS is considered to be a mature and stable standard. A full range of products and automated tools based on GKShas been available for various vendors for 5 or more years. However, it is limited to two-dimensional graphics [Ref. APP 1991, 41].

A 3D version of GKSis being developed in ISO. The purpose of GKS-3D is to specify extensions to GKSfor defining and viewing 3D wire-frame objects. As such, the GKS-3D documents only describe additions to be made to GKS. The GKS-3D portions of the GKSstandards are:

- ISO 8805, GKS*for Three Dimensions (GKS-3D) Functional Description*, October 1988, and ISO 8805/WDAD 1, Addendum 1: *Name Set Addendum*, April 1987
- DIS 8806-1, *GKS-3D Language Bindings - Part 1: FORTRAN*, November 1988
- DIS 8806-3, *GKS-3D Language Bindings - Part 3:* Ada, 1989
- DIS 8806-4, *GKS-3D Language Bindings - Part 4: C*, 1989
- ANSI X3.122.5, *GKS-3D Language Bindings - LISP*.

One of the major design goals in ISO is compatibility between GKS-3D and GKS. The 2D primitives of GKScan be seen as a subset of the 3D primitives obtainable via GKS-3D. This allows a GKS-3D program to read both 2D and 3D metafiles (by forcing 2D primitives to the z=0 plane); however, GKSis unable to use 3D metafiles. Thus, upwards, but not downwards, compatibility has been achieved.

11.3 Programmer's Hierarchical Interactive Graphics System (PHIGS)

The following are the standards for PHIGS, defining language bindings for graphics interfaces:

- ISO 9592-1, *PHIGS - Part 1: Functional Description* and ISO 9592-1 AD 1 Amendment 1: *PHIGS Plus Support*
- ISO 9592-2, *PHIGS - Part 2: Archive File Format* and ISO 9592-2 AD 1 Amendment 1: *PHIGS Plus Support*
- ISO 9592-3, *PHIGS - Part 3: Clear-Text Encoding of Archive File* and ISO 9592-3 AD 1 Amendment 1: *PHIGS Plus Support*
- ISO 9592-4, *PHIGS - Part 4: PHIGS Plus*
- ISO 9593-1, *PHIGS Language Bindings - Part 1: FORTRAN Binding*
- DIS 9593-2, *PHIGS Language Bindings - Part 2: Extended Pascal*
- ISO 9593-3, *PHIGS Language Bindings - Part 3:* Ada
- DIS 9593-4, *PHIGS Language Bindings - Part 4: C*.

PHIGS is a full-functioned specification for the development of interactive two- and three-dimensional graphics applications that manage hierarchical database structures containing graphics data. Numerous PHIGS implementations are available for various hardware/software platforms. PHIGS is mature and relatively stable. No changes are

planned in the next 1 to 3 years. Bindings for FORTRAN and Ada have been adopted. Bindings for C and Pascal are under development. A new standard, PHIGS Plus (ISO 9592-4) has been developed, which adds shading, lighting, and other advanced graphics programming capabilities that were not included in PHIGS. Conforming PHIGS programs will be able to execute under PHIGS Plus with no change [Ref. APP 1991, 42].

11.4 Assessment of Coverage by Standards

Graphics services standards all appear to be stable and mature with a high level of consensus and product availability. However, none address the question of distributed graphics. A common intermediate standard is needed to exchange graphics data stored on different platforms.

(This page intentionally left blank.)

12. PROGRAMMING SERVICE STANDARDS

This chapter identifies programming languages, software development environments, tool sets, process models, and methodologies, and other programming service standards. It needs be expanded to address specific tools such as compilers, syntax (e.g., ASN.1) analyzers, and other support tools. An overview of the status of key standards for programming services is given in Table 22.

Quick Reference

Topic	Page
Ada	244
Assessment	256
BASIC	248
Bindings	248
APSE	244
C	246
CAIS	244
COBOL	247
FORTRAN	247
KBSs	253
LISP	247
Pascal	245
Process Models	254
Requirements	243
Software Engineering	250
Software Reuse	254

12.1 Requirements

Programming language services address the sets of tools that support requirements definition, system development, testing, maintenance, and administration. They also address CASE, software development environments and tools, and library support.

In order to satisfy the overall CCIS requirement for using COTS/NDI hardware and software, software must be both portable and interoperable. Moreover, a multitude of applications ranging from data analysis to word processing will need to be integrated. Requirements for the efficient production of effective software dictate the use of software development environments and tools as well as reuse libraries. As the technology evolves, needs for expert system support in the software production process will arise.

Table 22. Status Overview of Key Programming Service Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
Ada	●	●	●	●	○	○	○
C	●	●	●	●	●	●	●
COBOL	●	●	●	●	●	●	●
FORTRAN	●	●	●	●	●	●	●
PASCAL	●	○		●	●		
ECMA PCTE	○			○			
SCCS		○					

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1991.

12.2 Programming Languages

12.2.1 Ada Programming Language

Ada is a programming language agreed to be used within NATO and the U.S. DoD[47] as a standard general-purpose high-level programming language. It was introduced in 1979 after the U.S. DoD became concerned about the proliferation of computer languages it was using and determined that none of these languages was suitable for writing DoD software. Ada uses the latest ideas in language design and a standard programming support environment is suggested. In 1983 it was adopted as a standard by ANSI and as a U.S. Military Standard (MIL-STD-1815A). It was adopted as a Federal Information Processing Standard (FIPS 119) on 8 November 1985. In 1987 ISO endorsed it as an ISO standard (ISO 8652).

In 1988, the Ada 9X project was undertaken to revise ANSI/MIL-STD-1815A through a three step process: (1) requirements development, (2) revision of the Ada Language Reference Manual, and (3) implementation demonstrations. In May 1990 the requirements process culminated in the publication of the Ada *9X Project Report:* Ada *9X Revision Issues*, Release 2 [Ref. Ada 9X 1990]. Whether or not Ada will be fully upwardly compatible with Ada 9X is currently unknown. However, revisions to Ada will be subjected to public review and comment before becoming part of the revised standard. It is expected that most changes will be upward compatible with existing compilers and tools.

12.2.1.1 Ada Programming Support Environment (APSE)

An APSE is an environment for developing software systems written in Ada. At its core is a kernel APSE (KAPSE), which represents general operating system services such as file management services and process and device control services, as well as object management services. It is at this level, as opposed to the outer layers, the MAPSE (Minimal APSE) and APSE, that a common set of interfaces is required. The MAPSE consists of software tools that minimally support software development, such as compilers, editors, and linkers, while the APSE provides project-specific tools and services.

12.2.1.2 Common APSE Interface Set (CAIS)

CAIS provides a common set of interfaces to the KAPSE. The CAIS standard (U.S. DoD MIL-STD-1838A, 1989) defines a set of interfaces that allows APSE tools to use common operating services and facilities in a standardized fashion. The original plan for the designing of CAIS in the U.S. called for one set of interfaces to be produced at the

---

[47] DoD Directive 3405.1 states that Ada is the preferred computer programming language for all DoD applications except when the use of another higher order language is most cost effective over the

end of 4 years' work (the original target was 1987). As pressure mounted for an earlier release, the Ada Joint Program Office (AJPO) decided that a limited capability version should be provided before the full CAIS was complete.

The first version of CAIS (U.S. DoD MIL-STD-1838) was published in October 1986. It comprised only those interfaces common to two different APSEs being developed by the U.S. Army and the U.S. Air Force: the Ada Language System (ALS, for the Army) and the Ada Integrated Environment (AIE, for the Air Force). Because of divergent approaches at the KAPSE interface level taken by the ALS and AIE contractors, the KAPSE Interface Team (KIT) and the KAPSE Interface Team from Industry and Academia (KITIA) were formed. Together, the KIT/KITIA produced the first version of the CAIS.

In parallel, the Requirements and Design Criteria Working Group (RACWG), composed of KIT and KITIA members, was established in July 1983 for the purpose of defining a set of requirements and criteria for the design of a second version of the CAIS. In 1985, a contract was awarded to SofTech, Inc., to continue development of this second version of CAIS (CAIS-A). CAIS-A was reviewed publicly in 1987 and was published as a military standard (MIL-STD-1838A) on April 6, 1989 [Ref. AJPO 1989].

There are no plans, nor is a mechanism currently in place, to update CAIS-A. While at least two implementations of CAIS-A now exist, one by SofTech for the VAX/VMS environment and one by UNISYS for the Sun/UNIX environment, the effort is generally suffering due to a lack of commercial support.

However, there are plans to merge CAIS-A with a similar European standards effort, the PCTE+ (Portable Common Tool Environment), over the next several years. The result of this merger will be the Portable Common Interface Set (PCIS). PCTE is an effort of the European Strategic Programme of Research and Development in Information Technology (ESPRIT) (see Section 12.3.2). Meetings to discuss PCIS are scheduled to begin in 1991 and the specification of PCIS is expected to be ready by 1994.

12.2.2 Pascal Programming Language

Pascal is a computer programming language originally designed to satisfy two principal aims. The first was to provide a language suitable for teaching programming as a systematic discipline based on certain fundamental concepts clearly and naturally reflected by the language. The second aim was to define a language whose implementations could be reliable and efficient on then-available computers. A Pascal standard was adopted in 1983 as ANSI X3.97 and IEEE 770.

---

application's life cycle. DoD Directive 3405.2 mandates the use of Ada in all computers integral to weapons systems (embedded systems).

At the same time that the ANSI/IEEE Pascal standard was being developed, the British Standards Institution (BSI) sponsored an ISO draft proposal for Pascal. In 1983, ISO adopted Pascal as a standard (ISO 7185), endorsing British Standard (BS) 6192-1982. While the ISO and ANSI/IEEE Pascal standards are compatible, there are some differences in technical substance as well as some errors in the ISO standard.

In January 1985 the U.S. Federal Government adopted the ANSI/IEEE standard as FIPS 109. The implementation of FIPS Pascal involves three areas of consideration:

- Acquisition of Pascal processors
- Interpretation of FIPS Pascal
- Validation of Pascal processors.

On 10 April 1990, ANSI X3 and the IEEE approved the Extended Programming Language Pascal standard as IEEE 770 and ANSI X3.160.

12.2.3 C Programming Language

C originated in the late 1970s as the programming language of the UNIX operating system. It is a general-purpose programming language that features economy of expression, modern flow control and data structures, and a rich set of operators.

C is not a very "high level" language, nor a complex one. Its particular area of application is systems programming (e.g., software for an operating system). Although it was originally implemented on a DEC PDP-11, it is now widely used [Ref. Kernighan et al. 1988].

Its growing popularity, changes in the language over the years, and the creation of compilers by groups not involved in its design raised the need for a standard in the early 1980s [Ref. Kernighan et al. 1988]. In 1989, ANSI promulgated X3.159, Programming Language C. In 1990, this standard was adopted by ISO (ISO/IEC 9899). It was also recently approved by the US Federal Government as FIPS-160.

There is also an ASC X3 project (0743-D) to promulgate a standard for Programming Language C++, a higher-level update of C. There is no draft standard yet, but estimated completion is 1994.

Technical Committee ANSI X3J11 of ASC X3 is developing a technical report for numerical C extensions. The objective of the report is to outline the technical issues involved in adding more support for numerical programming in Programming Language C. The issues that have been identified are [Ref. X3 1991h]:

- Optimization of potentially aliased variables
- Support for vector hardware
- Complex arithmetic
- Variability dimensioned arrays

- IEEE issues including infinity and NaN handling
- Exception handling
- Support for parallel processing
- Syntax for array/matrix operations.

ASC X3 recently announced the approval of a new project for Programming Language C Information Bulletins under the auspices of Technical Committee X3J11, Programming Language C. ANSI X3J11 has compiled numerous requests for interpretation or clarification of ANSI X3.159-1989, and the Bulletin will provide a means of making those interpretations available to the public. [Ref. X3 1991m]

12.2.4 COBOL Programming Language

This programming language, which is primarily used for business applications, is an ANSI (X3.23-1985) standard that was also adopted in 1985 by ISO (ISO 1989). On 18 March 1986, it was adopted by the United States as FIPS 21-2. A revision of ANSI X3.23 is currently in the planning stages. Public review began in 1990 with approval expected about 1999. An addendum to ANSI X3.23 for intrinsic functions (ANSI X3.23A-1989) was recently approved, and a Correction Addendum to ISO 1989 (*Programming Language COBOL*) is currently out for public review. The ANSI X3J4 Accredited Standards Committee on COBOLhas recently received approval to work on an Addendum for Multi-Octet Character Sets that are necessary for Asian languages. It is also working on a COBOLInterface to the Forms Interface Management System (FIMS) (ANSI Project 0676-D). Object-oriented extensions to COBOLare also under consideration by the committee. Despite standardization, non-standard versions of COBOLexist which can pose interoperability problems.

12.2.5 FORTRAN Programming Language

In 1978, ANSI promulgated a standard for FORTRAN (ANSI X3.9), a programming language for scientific numerical computation that has wide use and many variations. In 1980 this standard was endorsed by ISO (ISO 1539). FIPS 69 adopted X3.9-1978 on 4 September 1980 as a U.S. standard to promote portability of FORTRAN programs for use on a variety of data processing systems. The most recent FIPS (FIPS 69-1) was issued on 24 December 1985; a revised ANSI standard was issued in 1989. An ANSI X3J3 project X3.198 (DIS 1539.2) is underway to produce an extended version of FORTRAN. Like COBOL, non-standard versions of FORTRAN exist, posing potential interoperability problems.

12.2.6 LISP Programming Language

LISP is currently the most popular computer language used in artificial intelligence (AI) programming in the United States, although Prolog standardization efforts are underway in the United Kingdom. LISP is designed for supporting symbolic manipulation

and the interactive, trial-and-error style of programming employed by many AI researchers. It was invented in 1958 and has many dialects. The dialects tend to fall into one of two main camps: INTERLISP and MACLISP. In the interest of standardization, Common LISP was developed [Ref. Steele 1984]. It is not yet an official standard, but was created at the initiative of many vendors and is increasingly becoming the preferred version. Common LISP compilers exist for several mainframe computers [Ref. Schutzer 1987], minicomputers, and microcomputers. The Standards Committee ANSI X3J13 is working on an ANSI standard for Common LISP. Currently, a full draft is under review by the X3J13 committee, and a public review is expected by the end of 1991. Except for efforts to standardize Scheme (IEEE 1178, which was approved on December 6, 1990) and the AI programming language Prolog, there are currently no other standards for knowledge-based specifications or notations.

12.2.7 BASIC Programming Language

BASIC is distinguished from other programming languages in its concern for the unsophisticated or novice user. While BASIC is a general-purpose programming language, it is designed primarily to be easy to learn, easy to use, and easy to remember. It is oriented toward, but not restricted to, interactive use. Its constructions are kept simple and special rules are kept to a minimum. The ANSI standard for Minimal BASIC (X3.60) was promulgated by ANSI in 1978 and adopted as FIPS 68 in 1980. It was subsequently adopted by ISO in 1984 (ISO 6373). In 1987, ANSI withdrew X3.60-1978 and superseded it with a standard for Full BASIC (X3.113-1987), which was adopted as FIPS 68-2 on 28 August 1987. This revision reflects major changes, improvements, and additions to the BASIC specification. In December 1989 ANSI issued the standard ANSI X3.113A, *Addendum to Programming Language Full BASIC, Modules, and Individual Character Input.*

12.3 Standards for Software Environments

12.3.1 Bindings

In addition to programming language standards, several standards provide interfaces or connectivity between programming languages and applications. Such "bindings" as they are called exist or are being proposed for the POSIX (IEEE P1003), GKS(ISO 7942), GKS-3D (ISO 8805), PHIGS (ISO 9592), and CGI (ISO 9636) standards.

POSIX bindings are planned for Ada, C, and FORTRAN. The PAR for IEEE project P1003.5, Ada *Bindings for POSIX*, was approved in December 1987, but a target date has not been established. The PAR for the FORTRAN binding (P1003.9) was approved in February 1989. A PAR has not yet been approved for the C binding (P1003.X).

ANSI and ISO have approved standards for FORTRAN, Pascal, and Ada bindings for GKS. The C binding is currently in the working draft stage. They are:

- ISO 8651-1, *FORTRAN Binding* (ANSI X3.124.1-1985), October 1988
- ISO 8651-2, *Pascal Binding* (ANSI X3.124.2-1985), October 1988
- ISO 8651-3, Ada *Binding* (ANSI X3.124.3-1985), October 1988
- DIS 8651-4, C *Binding* (ANSI X3.124.4-199x).

ISO draft standards have been developed for GKS-3D bindings for FORTRAN, Ada, and C. Pascal and LISP bindings are under development. They are:

- DIS 8806-1, *FORTRAN Binding*
- DIS 8806-3, Ada *Binding*
- DIS 8806-4, C *Binding*
- *Pascal Binding* [SC24 N 190] (ANS Project 0545-I)
- *LISP Binding* (ANS Project X3.122.5-199x, estimated completion 1991).

There are ISO standards for Ada and FORTRAN bindings to PHIGS. The Pascal and C bindings are awaiting balloting. All are draft ANSI standards. They are:

- ISO 9593-1, *FORTRAN Binding* (ASC X3.144.1-199x), October 1988
- DIS 9593-2, *Pascal Binding* (ASC X3.144.2-199x)
- ISO 9593-3, Ada *Binding* (ASC X3.144.3-199x), March 1990
- DIS 9593-4, C *Binding* (ASC X3.144.4-199x).

The FORTRAN and C bindings to CGI are currently ISO working documents and ANSI projects:

- WD 9636-8, *FORTRAN Binding* (ANS 0560-D)
- WD 9636-11, C *Binding* (ANS 0559-D).

ISO/IEC JTC1/SC22/WG11, *Binding Techniques for Languages* has several projects underway, some of which are broader in scope than the name of the WG suggests The following work items have been assigned to SC22/WG11 [Ref. SC21 N 5682 1991]:

- PDTR 10182, *Binding Techniques for Programming Languages* [SC22/WG11 N 754]. The scope of this technical report is to classify language binding methods, report on particular instances in detail, and produce suggested guidelines for future language binding standards.
- *Specification for a Model for Common Language-Independent Procedure Calling Mechanisms (CLIPCM or CLIP)* [SC22/WG22 N 194R]. This project intends to specify a generic way for referencing procedures. A draft was circulated among SC22 member bodies for registration as a CD document in February 1991.
- *Specification for a Set of Common Language-Independent Data Types (CLID)* [ISO 11404]. This standard defines specific common language-independent data types by [Ref. X3 1991n]:

  - Identifying distinct data types by their characteristics, functions, values, value-relationships, etc.
  - Assigning identifiers, or formal reference syntax, to each distinguished data type
  - Defining a means by which users or related standards may define additional data types
  - Defining the form of and requirements for mappings between the data types of a programming or specification language and the language-independent data types defined by the standard.
- DIS 10967, *Language Compatible Arithmetic Standard (LCAS)* [ISO/IEC JTC1/SC22 N 796]. This standard, which specifies the essential properties of integer and floating point numbers that can be relied upon in writing portable software, is currently undergoing public review. A new work item proposal is underway to cover, in addition, complex arithmetic and mathematical procedures.

Bindings for fourth generation languages (4GLs), however, have yet to be standardized. This could pose a problem if 4GLs were used for database queries.

12.3.2 Software Engineering Environments

ECMA and NIST have both been working on a *Reference Model for Frameworks on Computer Assisted Software Engineering Environments*. NIST draft version 1.3, 18 July 1991, prepared by the NIST Integrated Software Engineering Environment (ISEE) Working Group, is a revised version of ECMA Technical Report 55, December 1990, developed by ECMA TC33 Technical Group on Reference Models (TGRM). It is the functional description of a set of services needed to describe software engineering environment frameworks.

Another software engineering environment standardization project in addition to the CAIS-A project is the PCTE. Other projects standardize the interfaces between tools which might be combined to create an environment. Of particular interest are CASE tools.

The PCTE project was begun in 1983 by the Commission of the European Communities (CEC) European Strategic Programme for Research in Information Technology (ESPRIT). It is now being considered by ECMA Technical Committee 33 and is expected to be submitted to ISO for balloting as an international standard [Ref. PCTE 1989] in 1991. The *ECMA PCTE Abstract Specification* (ECMA-149) was completed in September 1990 with formal approval in December 1990 [Ref. Davis 1990]. The C *Programming Language Binding to PCTE* (ECMA-158) was approved in June 1991. An Ada *Programming Language Binding* is in final draft form--the most recent version is Draft 5, ECMA/TC33/91/105, October 1991. Concern has been expressed, however, about a substantial overlap and possible conflict between PCTE and the pre-existing standard (DIS 10728) on IRDS. An option is the incorporate those PCTE functionalities not in DIS 10728 into future IRDS versions [IST:21 N 3057, September 1991].

The goal of the PCTE project was to describe and prototype tool interfaces that could be used to define a software development environment. The environment would comprise a set of public tool interfaces (PTIs) as well as a data management system. As defined by the PCTE project, a PTI is a non-proprietary interface existing as a library unit that may be used by a tool to provide access to system services. Tool builders might use the interfaces to either integrate or attach their tool products to an environment. The distinction between integration and attachment reflects the degree to which the environment monitors, controls, and makes use of the information on a given tool. An integrated tool makes full use of the services provided by the environment such as logging an audit trail and data management. An attached tool does not. For example, data are maintained in a repository known only to that tool.

The criteria for development of the PCTE were that it be policy and mechanism independent, support a distributed environment, provide easy tool integration, provide a complete interface definition, and provide multi-language support. To accomplish this, PCTE defines the services needed by the tools. The services provided by PCTE include data management, tool execution and communication, distribution and environment management, and programmer interface for user interface management.

The NATO Independent European Programme Group (IEPG) TA-13 is responsible for managing the evolution of PCTE to a standard tool interface for civil and defense use [Ref. Dowling 1988]. This language independent tool interface is called PCTE+. It offers the following extensions to the facilities provided by PCTE:

- Composite entities
- Version support
- Security
- The process as an object
- The metabase
- Multiple inheritance of entity type definitions
- Type definition modes
- Notification of specified object accesses
- Accounting
- Real and enumeration attribute types.

In addition to these extensions, constraints existing in PCTE as a result of its aim for compatibility with UNIX have been removed. Issue 3 of PCTE+ (upon which the ECMA standard is based) contains an abstract specification with bindings for C and Ada.

The Portable Common Tools Interface Set (PCIS) effort is aimed at converging CAIS-A and PCTE+. This effort may result in the best of both standards and shift consensus to the jointly developed interface.

Among the other work being done in this area is an IEEE Computer Society Project (P1209) for a *Recommended Practice for Evaluating CASE Tools*. The PAR was approved on 1 June 1989. The IEEE Committee has met four times and has published a draft that is still not stable. Balloting is expected within 2 years.

The Institution of Electrical Engineers (IEE)/British Computer Society Joint Working Party on Software Engineering Standards has also discussed the possibility of investigating CASE tools, in particular, the way in which their use supports conformance to high quality standards. However, their only planned activity is to comment on IEEE P1209. In discussions related to a proposed U.K. MoD standard (DEF-STAN-00-55), *Requirements for the Procurement of Safety Critical Software*, the remark has been made that currently available CASE tools would not meet their requirements, since none of the tools have been or can be subject to the kind of formal methods analysis laid down in the proposal [Ref. Kemp 1990].

Another issue with respect to tools and toolsets is the ability to interconnect tools from different software developers. Consequently, the IEEE Computer Society approved a PAR for a *Standard for Interconnections Among Computing System Engineering Tools* (P1175) in February 1988. The core of this standard is the Standard Text Language (STL), which describes concepts such as data, conditions, events, and states, as well as transformation, control-transition, and state-transition operations. The proposed standard supports both textual and graphical forms [Ref. P1175 1989]. It is currently in the final stages before IEEE balloting as a trial-use standard.

The CASE Integration Services (CIS) Committee is also trying to provide direction for integration standards in the CASE arena. Originally formed to discuss a standard interface for services to assist in the integration of software engineering tools into CASE environments, the CIS committee is now a public forum with many organizations participating in its deliberations and others monitoring the process as observers. The CIS committee has chosen to focus on two areas: (1) data integration, the sharing of meta-data among tools, and, (2) control integration, the sharing of control information among tools.

A standard known as ATIS (Atherton Tools Integration Services, or alternatively, A Tools Integration Standard) [Ref. CIS 1990] which was developed jointly by Digital Equipment Corporation and Atherton Technology, was proposed as a Base Document for the CIS work and is under review by committee members. ATIS is based on the object-oriented interfaces in Atherton Technology's Software BackPlane product. While it addresses many of the integration issues, it does so as a monolithic solution and has several deficiencies. However, the general solution offered by ATIS, (i.e., an object-oriented approach based on defined and extensible schema and methods) is considered by CIS members to be the preferred approach to providing integration services. Thus ATIS can provide a starting point for the ongoing work of CIS [Ref. Nolan 1990]. At CIS's request, ANSI is considering making CIS a group to pursue this standards issue.

Another standardization activity in this area is the CASE Data Interchange Format (CDIF) effort. The CDIF Technical Committee operates under the authority of the Electronic Industries Association (EIA), and its charter is "to develop an ANSI standard (eventually to become an ISO standard) for the exchange of information between CASEs." Three releases of standards are planned: a framework standard, a syntax standard, and a semantic standard. Their EIA Project Numbers (PNs) are 2387, 2389, and 2329, respectively. The Committee plans to publish the standards as interim standards in the summer or fall of 1991 [Ref. Ornstern 1991]. Both CALS and P1175 representatives have participated in the meetings.

12.3.3 Knowledge-Based Systems (KBSs)

Areas where standards are lacking, probably due to technological immaturity, include knowledge-based systems (KBSs), and software repositories. There are no standards for knowledge exchange, knowledge management or development of knowledge bases for life-cycle maintainability. Several standards exist or are under development in the areas of software process models and development methods.

The U.K. General Expert System Methods Initiative (GEMINI) is an example of a project that is addressing needs for knowledge-based standards. In mid-1988, the CCTA launched this project to lay the foundation for a systematic KBS development methodology. A feasibility study concluded that there is strong support for such a method and that its development is both timely and feasible [Ref. Montgomery et al. 1989].

On March 21, 1991, the IEEE Standards Board approved a PAR for the development of a *Standard for an Architecture for Knowledge Representation.* The IEEE Project number is P1252 [Ref. P1252 1991]. This is a broader issue than KBS, development methods or tools.

An important method of integrating KBSs is by means of the IRDS (ISO 10027). The first area of standardization for expert systems will likely be bindings between expert systems and programming languages, databases, and user interfaces. Progress towards providing decision support and decision making tools and methods is slow but may be stimulated by the early release of the IBM Repository [Ref. MODITSB 1989].

ASC X3, Information Processing Systems recently announced a development project for IRDS *Extensions to Support CASE Environment for Information Interchange.* This standard would define an IRDS, based on ANS X3.138-1988, capable of supporting the full range of IRDS applications. In particular, it would be capable of acting as the IRD in a traditional data processing environment and capable of providing the stable store necessary to support an integrated CASE environment. The standard would include both the semantics of the IRDS and a software interface suitable to the needs of active CASE and Dictionary tools. The development has been assigned to Technical Committee ANSI X3H4.2 [Ref. X3 1990].

12.3.4 Software Repositories and Reuse

Software repository standards to facilitate software reuse do not yet exist. These might include library structure, cataloging scheme, retrieval, documentation and maintenance, validation and verification, and reuse policy and guidance standards. Reuse is a strategy with potential to increase software productivity, reliability, and quality.

12.3.5 Process Models and Development Methods

A model of the software development process is the ordered sequence of activities that occur during the course of software development. Examples of software development process models include the waterfall method, rapid prototyping, and the spiral model. By contrast, a software development method (methodology) is the way the specific development activities are actually carried out by the developer. An example is the object-oriented approach.

There is currently a single U.S. standard, DoD-STD-2167A, *Defense Software Development Standard*, for the process of software development. It superseded DoD-STD-2167, which was tied to the waterfall method and did not easily allow tailoring to other methods. ANSI and the American Institute for Aeronautics and Astronautics (AIAA) recently issued a related standard, *Guide for Implementing Software Development Files Conforming to DoD-STD-2167A* (ANSI/AIAA G-009-1991).

The IEEE has a project underway (IEEE P1074), *Standard for Software Life Cycle Processes*, which will define the processes of the software life cycle and describe the activities required to develop or maintain software in accordance with existing IEEE standards.

The IEEE publishes a volume of Software Engineering Standards [Ref. IEEE 1983] comprising 17 standards developed for software engineering. Most of the standards are ANSI/IEEE standards and they provide recommendations reflecting the state of the art in the application of engineering principles to the development and maintenance of software. The 17 standards are:

1. ANSI/IEEE Std. 610.12 - *IEEE Standard Glossary of Software Engineering Terminology*, 1990
2. ANSI/IEEE Std. 730 - *IEEE Standard for Software Quality Assurance Plans*, 1984
3. ANSI/IEEE Std. 828 - *IEEE Standard for Software Configuration Management Plans*, 1983
4. ANSI/IEEE Std. 829 - *IEEE Standard for Software Test Documentation*, 1983
5. ANSI/IEEE Std. 830 - *IEEE Guide to Software Requirements Specifications*, 1984
6. IEEE Std. 928.1 - *IEEE Standard Dictionary of Measures to Produce Reliable Software*, 1988

7. IEEE Std.928.2 - *IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software*, 1988
8. ANSI/IEEE Std. 983 - *IEEE Guide for Software Quality Assurance Planning*, 1986
9. ANSI/IEEE Std. 990 - *IEEE Recommended Practice for* Ada *as a Program Design Language*, 1986
10. ANSI/IEEE Std. 1002 - *IEEE Standard Taxonomy for Software Engineering Standards*, 1987
11. ANSI/IEEE Std. 1008 - *IEEE Standard for Software Unit Testing*, 1987
12. ANSI/IEEE Std. 1012 - *IEEE Standard for Software Verification and Validation Plans*, 1987
13. ANSI/IEEE Std. 1016 - *IEEE Recommended Practice for Software Design Descriptions*, 1987
14. IEEE Std. 1028 - *IEEE Standard for Software Reviews and Audits*, 1988
15. ANSI/IEEE Std. 1042 - *IEEE Guide to Software Configuration Management*, 1988
16. ANSI/IEEE Std. 1058.1 - *IEEE Standard for Software Project Management Plans*, 1987
17. ANSI/IEEE Std. 1063 - *IEEE Standard for Software User Documentation*, 1989.

Standards under development in this series include:

- IEEE P1016.2 *Guide to Software Design Descriptions*
- IEEE P1044 *Classification of Software Errors, Faults, and Failures*
- IEEE P1045 *Software Productivity Metrics*
- IEEE P1059 *Software Verification and Validation*
- IEEE P1061 *Software Quality Metrics Methodology*
- IEEE P1062 *Software Acquisition*
- IEEE P1074 *Software Life Cycle Processes*
- IEEE P1219 *Software Maintenance Standard*
- IEEE P1228 *Software Safety Plans.*

Development of international software engineering standards by ISO/IEC JTC1 SC7 on Software Engineering is still in its early stages. The emphasis for the next 3 years will be on establishing a foundation on which to build future standards. The following standards projects are underway in SC7's four working groups [Ref. Edelstein et al. 1991]:

- WG1--Symbols, charts, and diagrams
  - Conceptual framework for software development diagrams
  - Charting techniques for software development and maintenance
  - Conventions for use of symbols and icons in software systems

  - Transfer of information between life cycle phases
- WG2--Software system documentation
  - Guidelines for documentation of computer-based systems
- WG3--Software engineering and quality management
  - Software quality characteristics
  - Software configuration management
  - Software life cycle management
  - Software quality management
  - Requirements/design/testing, etc.
  - Evaluation and selection of CASE tools
- WG5--Reference model for software development
  - Reference model
  - Reference model overview
  - Reference model--mapping of relevant information systems engineering standards.

International activity that will affect software development is the standardization of quality management systems. ISO 9001 represents a concise, generic description of the essential elements of management systems for assuring quality in development, production, and qualification with emphasis on the "what" over the "how." ISO 9001, Part 3: *Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software*, was approved by international ballot and adopted by TC 176 in November 1990 [Ref. Edelstein et al. 1991].

There are currently no standards specifically for the development of expert systems. It is not clear that the development of expert systems will need to follow a different or unique process model.

The ESPRIT project "accueil de logiciel futur" aims to provide a knowledge-assisted software process model on top of the PCTE [Ref. Brettnacher et al. 1988].

Development methods tend to be proprietary and not subject to standardization. However, one IEEE project (P1152), *Standard for Object Oriented Programming Language and Environment,* is developing a standard based on the SmallTalk programming language and environment.

12.4 Assessment of Coverage by Standards

There are international standards for most, but not all, of the commonly used programming services. Although ISO and the U.S. Government have adopted ANSI X3.159, Programming Language C , there are potential compatibility problems between C and C++. While COBOLis an ANSI and ISO standard, many non-standard versions of it and extensions to it exist, creating interoperability problems. The other standards are stable. However, Ada is undergoing a revision process and some aspects of the current language may not be upwardly compatible with its successor, Ada 9X.

There is no standard set of guidelines for using the features of the Ada programming language; without guidance, applications written in Ada may have unpredictable portability. Further, bindings between Ada and special-purpose languages (such as 4GLs) may be required for CCISs.

Standards have not been developed for languages used for certain technologies and application areas. If applicable to a CCIS, these areas might include languages used in artificial intelligence (standards for LISP and Prolog have been developed but not for other languages) and used for interfaces to specific COTS/NDI software. LISP is more popular in the United States while Prolog is more popular in the United Kingdom and Europe, posing potential interoperability problems.

Standards for software development environments, including CASE tools and environments, are in the early phases of development. Some are currently restricted to interfaces between tools while others address entire environments. The extent to which environments such as PCTE and CAIS can evolve and be tailored is unknown. Moreover, CAIS is already suffering from a dearth of conforming commercial products. Tool interfaces based on commercial products may lack flexibility. Standards for KBS do not exist. Software repository standards to facilitate reuse do not yet exist. This could have an adverse effect on a COTS/NDI acquisition strategy by making NDI software difficult to identify.

Software engineering standards that address the software development process and development methods, and ultimately software quality, are in the early phases of the international standardization process. It will be at least 3 years before a foundation for these standards is established. To date, none address the development of expert systems.

(This page intentionally left blank.)

13. APPLICATIONS AND APPLICATIONS PORTABILITY INTERFACES

13.1 Applications Portability

Quick Reference	
Topic	Page
Applic Portability Profile	264
Assessment	279
CAE	270
EWOS OSE	277
IAP	263
ISO	259
NIST	261
X/Open	262
Open Sys Environment	264
OSF	262
OSF Profiles	274
Requirements	259
TOP	274

13.1.1 Requirements for Applications Portability

Portability is a software attribute representing the ease and cost effectiveness with which that software and data can be used on heterogeneous hardware/software platforms. Three key aspects of portability are the operating system, database access, and applications software. Hardware environment changes that require change of the operating system are in many cases significant to portability. This aspect of application portability is addressed by enforcing a standard (POSIX) for an operating system *interface*.

The interoperability aspects of information exchange mean that CCISs need to have a consistent way to record meanings and relationships of data, and to distribute and replicate the data and changes to the data. This leads to the need to standardize the data models (schema) for databases and the services for accessing those databases. SQL is an example of a standard for services to databases conforming to a relational data model. Additional standards may need to be developed for other data models. Standards for applications software take the form of programming language standards, together with standard methods for using the programming language.

Following the guidelines and standards will improve the prospects, but not guarantee, application portability. Many aspects of implementations of POSIX, SQL, and Adaenvironments are inherently hardware dependent. Further, the standards do not provide all the needed services. Use of nonstandard options available in the implementations of operating systems, SQL, and programming languages can greatly restrict portability.

13.1.2.1 ISO

In April 1988, JTC1 of the ISO/IEC began a formal Joint Technical Study Group (TSG-1) for Applications Portability (JTAP). Managed directly under the JTC1, and not any of the subcommittees, the JTAP study addressed five areas: (1) concepts and

definitions related to applications portability, (2) user requirements, (3) portability issues, (4) internationalization (to investigate the interface requirements of users with different cultural backgrounds), and (5) a framework for interfaces for applications portability (IAP). The final report [Ref. JTAP 1991] contains eleven recommendations. It does not contain an explicit list of application portability standards as mentioned in the original mandate because such a list would comprise almost all of the JTC1 projects and standards. The recommendations of the JTAP report are that JTC1 should do the following:

1. Instruct its standards groups to use the methods and concepts described in the report.
2. Establish channels of communication with groups outside JTC1 in order to assist them in developing, recording, and using application environment profiles.
3. Use application environment profiles to identify standards work needed.
4. Establish procedures for managing application environment profiles, taking both user requirements and TR 10000-1[48] into account.
5. Establish procedures for the coordination of the work on base standards and application environment profiles that may lead to the development of new standards.
6. Initiate work to develop a taxonomy for application portability.
7. Instruct all of its standards groups to implement the portability considerations of Annex A [to the JTAP report] ("Necessary Portability Considerations for all JTC1 Standards Development").
8. Publicize activities in relation to the development of standards relevant to application portability in order to increase user awareness and participation, and promote the early use of standards.
9. Solicit user needs and priorities when initiating and guiding work relevant to application portability.
10. Should review its mechanisms for coping with subjects that span multiple subcommittees such as application portability, security, and internationalization.
11. Should establish means (e.g., Special Group) for:
    - Interacting with user groups
    - Recording application environment profiles
    - Developing a taxonomy for application portability.

JTAP terminated on 19 September 1991. As a result of the JTAP work, SC22 has initiated Working Group 20 on Internationalization. The Group will take the POSIX work as input to address the complex technical problem of porting applications across other languages and cultures. The Japanese National Body has proposed the establishment of a

---

[48] TR 10000 is an ISO technical report by the Special Group on Functional Standardization (SGFS) detailing the framework and taxonomy for International Standardized Profiles (ISPs). See Section 14.1.2.

new JTC1 subcommittee to be devoted entirely to application portability [SC21 N 6402, September 1991].

ISO has recognized that standardization is needed for information processing that goes beyond data communications services and protocols. As will be shown in the sections that follow, there are major efforts under way in the areas of standard interfaces to operating systems, databases, graphics, user input and display devices, and programming languages. In addition, open systems standards are being developed for document interchange and distributed processing.

SC21 has identified [Ref. SC21 N 3134 1988] the need to provide standardization in the following areas related to CCIS interoperability:

- Information exchange
- Internetworking of systems
- Specification of functions needed in systems built for specific purposes
- Portability of applications across system hardware and software
- Definition of common interfaces to system services
- Security of systems
- Reliability of systems
- Human-computer (man-machine) interfaces
- Definition of common concepts
- Safety and legal requirements.

SC21 specifically plans to address standardization for database management systems and single and distributed processing environments, in addition to open systems interconnection.

13.1.2.2 National Institute of Standards and Technology (NIST)

NIST has been working with the IEEE and other US organizations to identify environments for open systems that can be specified with existing OSI and other open system standards. The NIST recommendations are contained in the APP, discussed in Section 13.1.3.3. NIST is promoting in the United States the concept of an Open System Environment (OSE), which IEEE P1003.0 defines as:

> The comprehensive set of interfaces, services, and supporting formats, plus user aspects, for interoperability or for portability of applications, data, or people as specified by information technology standards and profiles.

An OSE is the basis for profiles. The NIST APP OSE/1 and POSIX are both examples of OSEs. By contrast, a profile, as defined by IEEE P1003.0 is:

> A set of one or more base standards, and where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards, necessary for accomplishing a particular function.

A profile is a list of standards as opposed to an OSE, which is a list of services. Profiles are therefore, subsets of OSEs. They do not specify functionality, but combine multiple base standards, choose and select options and parameters, and address coherence among the base standards. [Ref. Gambrel 1991]

13.1.2.3 X/Open

X/Open is a non-profit consortium developing extensions to UNIX SVID operating system standards to support a distributed transaction processing environment that meets OSI standards. X/Open is developing a Common Applications Environment (CAE) to promote applications software portability. This is planned to be achieved by adopting and adapting existing industry and *de facto* standards, rather than by creating a new standard.

The X/Open System V Specification (XVS) is the initial recommended standard for the operating system. Future goals for the CAE are alignment with POSIX P1003.1 (with a large number of extensions) and ANSI X3J11 C together with interfaces for Indexed Sequential Access Method (ISAM) and an embedded standard relational database language (SQL). The X/Open version of ISAM is based on a major (implementation nonspecific) subset of C-ISAM Version 2.10 (January 1985) from the Informix Corporation. The initial X/Open version of SQL is not fully compliant with ANSI X3.135-1986 [Refs. X/OPEN 1987; X/OPEN 1988; Lambert 1987]. Standards recommended for the CAE are discussed in Section 13.1.3.4.

13.1.2.4 Open Software Foundation (OSF)

The Open Software Foundation (OSF) is an international consortium formed in May 1988 to promote applications portability. OSF is identifying technologies and products to be included in its Distributed Computing Environment (DCE). In December 1990, OSF issued the first release of its OSF/1 operating system. OSF has integrated a number of existing advanced technologies into its vendor-neutral operating systems. As noted in Section 7.2.2, OSF/1 includes significant portions of IBM's AIX 3.1 operating system and the Mach kernel technology from Carnegie Mellon University. OSF expects to release subsequent versions of OSF/1 every 12 to 18 months [Ref. OSN 1990]. Other standards recommended for OSF are identified in Section 13.1.3.5.

13.1.3 Standards for Applications Portability

This section discusses the standards recommended as profiles for applications portability. Each of the major recommendations is based on POSIX. The areas addressed are Interfaces for Applications Portability, NIST APP, United Kingdom's (U.K.) Ministry of Defense (MoD) Model, X/Open CAE, OSF, the Technical and Office Protocol (TOP), Multivendor Integration Architecture (MIA), and EWOS Profiles for Open System Environment.

13.1.3.1 Interfaces for Applications Portability (IAP)

JTAP [Ref. JTAP 1990] examined the interfaces that need to be standardized in order to facilitate portability of applications. It concluded that there are three types of portability: programs, data, and people. Thus, standards relevant to IAP must address the following:

- Source code portability
- Data portability
- User interface
- Documentation portability
- Operating system interfaces
- Communication services
- Database management services
- Software engineering tool interfaces
- Internationalization.

Further, the JTAP study identified the following IAP issues to be addressed in JTC1:

- Standards need to define consistent handling for exceptions encountered by applications during execution.
- Standards need to identify ways to enable adaptation of applications by automated means to accommodate options and other environmental variations (e.g., implementation-defined characteristics, option identification).
- Standards for IAP need to take into account external object names, providing methods to minimize the impact of variations of external object names across application platforms. Language standards need to provide corresponding services and capabilities to enable applications to accommodate these variations (e.g., variable length strings, services for acquiring object names from external sources, object name composition/decomposition).
- Qualitative metrics for application portability may be useful.

IAPs can be language independent, operating system independent, or both. Proposed work in SC21 will be for IAPs that are both language and operating system independent. Language-specific constructs could be developed in SC22, as the mapping of abstract data types to language-specific constructs is primarily the work of defining language bindings.

Specification of an IAP would include definition of data types of the interfaces and may include rules for describing behavior and sequencing of functions within an interface (e.g., blocking or non-blocking procedure calls) and levels of enforcement of these rules. A model of IAPs is needed and should be related to or possibly included in the models for Extended AIX (Application Layer Structure) (XALS) and ODP. It was proposed that the IAP model, as well as the XALS and ODP models, should include a means to extend the

interface to include user- or application-specific extensions or abstractions. For example, it should be possible to invoke a procedure to store application data type within the X.500 Directory Service without changing the interface definition [Ref. SC21 N 4523 1990].

In its May 1991 plenary, SC21/WG4 decided not to register a Question on Application Programming Interfaces (APIs) as National Body comments on its proposal [SC21 N 6017, May 1991] indicated that the scope is wider than WG4. WG4 requested SC21 to take up whether APIs should be standardized and how. It further noted relevance of SC21/WG6 work on interface definition notation (IDN), language bindings of SC22, and work of TSG-1 on IAPs.

In August 1991, Japan initiated a proposal for a new work item: *Model and Framework of Interfaces for Application Portability* [JTC1 N 1534; SC21 N 6405]. The new work item builds on the TSG-1 report's method of realizing an IAP which is to define Application Environment Profiles (AEP) for OSEs for each application area. In order to do this, it is necessary to establish the concept of AEP, the classification of application areas, and the evaluation methodology of AEP so that all standardization activities for AEP are carried out based on a sound and common reference model and framework. The new work item therefore suggests that a technical report address the following items:

- Dimensions of the IAP reference model
- Relations among application, application platform, and the real world
- Evaluation method for base standards and AEP
- Porting process model and conformance testing method.

A working draft is planned for the first quarter of 1992, CD by the end of the third quarter of 1992, DTR by the end of the second quarter of 1993, and TR by the end of 1993.

13.1.3.2 Example Model for the Open Systems Environment

Figure 15 provides an example of a model for an open systems environment developed by the U.K.'s MoD [Ref. MoD 1989] and used to promote applications portability. It includes users, developers, managers, and providers. It also explicitly includes security and OSI system and project management.

13.1.3.3 NIST Applications Portability Profile

This section discusses the APP developed by the NIST. The NIST approach to applications portability is based on an architectural approach that provides interfaces for functionality to accommodate a broad range of applications requirements. The functional components of the architecture are viewed as a "tool box" of standard elements that can be used to develop and maintain portable applications. These tools are based on an open systems concept and are required to be developed as an integrated collection of non-proprietary standards. The NIST OSE embraces three concepts:

- Extensibility. Based on an architectural framework that allows an extensible collection of interfaces, services, protocols, and supporting formats to be defined
- Non-proprietary. Interfaces, services, protocols, and supporting formats defined in non-proprietary specifications
- Consensus based. Evolution is controlled by a consensus-based process for definition and specification of interfaces, services, protocols, and supporting formats.

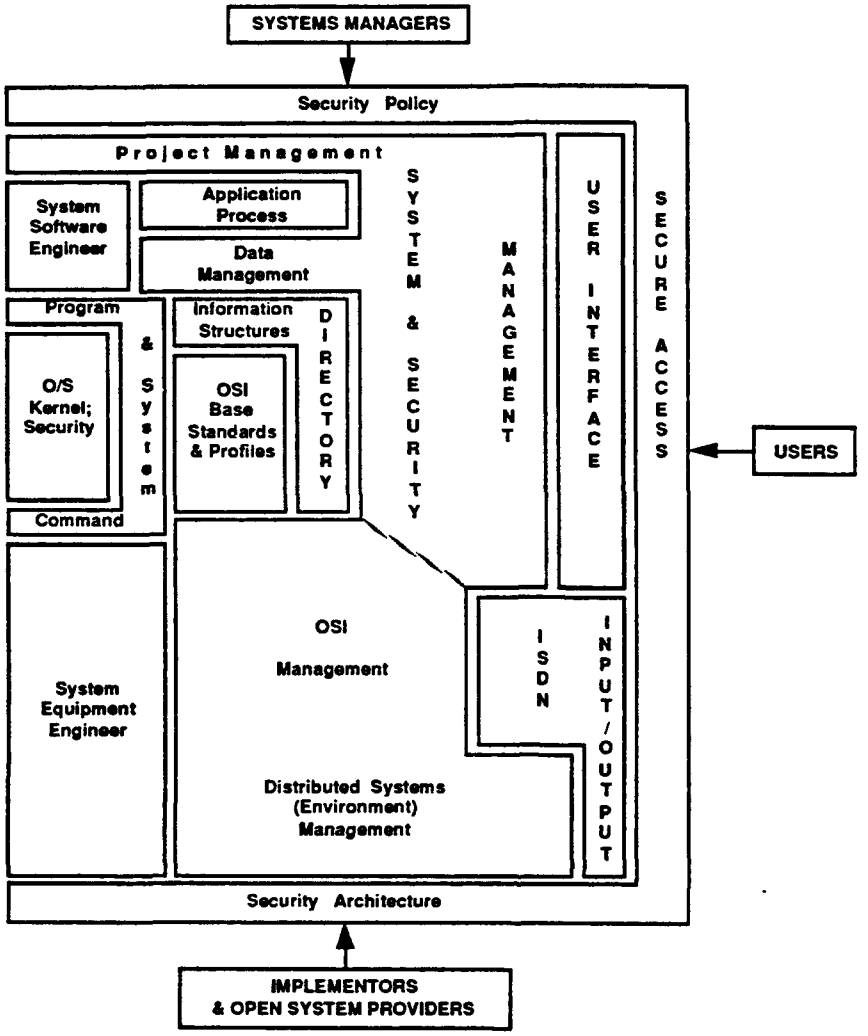
Moreover, it stresses the following:

- Portability. The ability to use application software and data on heterogeneous hardware and software platforms
- Interoperability. The ability to have application and software operating on heterogeneous hardware and software platforms cooperate in performing some user function
- Scalability. The ability to use the same applications software on many different classes of hardware and software platforms, from personal computers to supercomputers.

A full complement of standards should be available under the APP by 1995 [Ref. APP 1991]. Version 1 of the *Application Portability Profile (APP): The U. S. Government's Open System Environment Profile OSE/1* (NIST Special Publication 500-187) was published in April 1991. It recommends 26 standards and specifications, provides guidance in areas where standards do not exist for seven service areas, and makes strategic evaluations with respect to those standards. The three strategic classifications are:

- Strategic now. Users reasonably safe in making substantial investment and long-term plans in mission-critical systems and infrastructure
- Strategic in the future. Specifications subject to change but appear to be headed for standardization; some risks but consensus process minimizes them
- Nonstrategic. Stop-gap recommendations with warning that user investment will be at significant risk; not appropriate for long-term planning.

APP specifications are selected according to the following order of precedence: International Standards, US National Standards (e.g., ANSI, IEEE), US National Standards Committee work in progress, other Federal standards (e.g., DoD standards), and specifications that are publicly available and for which implementations are commercially available from a variety of sources (e.g., X-Window System, Version 11) [Ref. Fisher 1991].

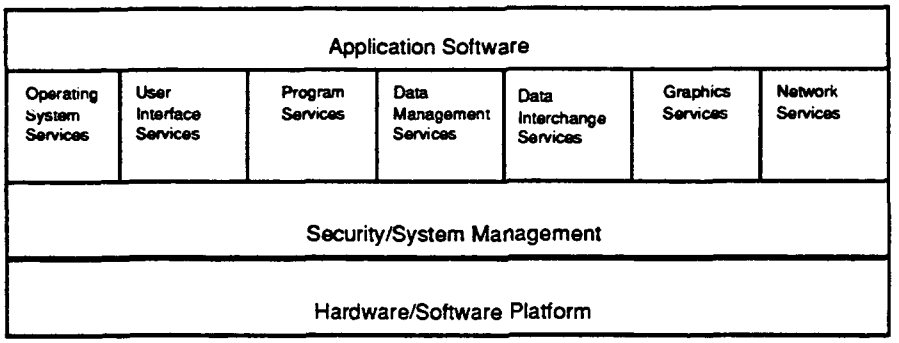


Source: *Scope for MOD Information Technology (IT) Standardization and Responsibilities.* UK MOD Information Technolgy Standards Board, 11 August 1989.
Notes: OS: Operating System
ISDN: Integrated Services Digital Network

Figure 15. A Model for the Open Systems Environment

Figure 16 provides a high-level view of the architectural approach that underlies the APP. The APP comprises seven of the eight service areas identified for CCISs (see Section 3.2). The differences are that Graphics is a separate service in the NIST APP but considered part of Data Exchange in this paper and Security and OSI Management are not explicitly shown as a service in the NIST APP since they are assumed to be integral to all other services.

Table 23 identifies the elements (tools) and the associated interface specifications of the recommended standards [Ref. APP 1991] for the APP. The key elements are OSI for data communications; (extended) POSIX for the operating system interface; SQL and IRDS for database management; and X-Windows for the user interface.



Source: [Ref. Fisher 1991]

Figure 16. An Example View of the Architecture for the Applications Portability Profile

Table 23. Standards for the Applications Portability Profile

Function	Element	Reference for Standards
Operating System	Extended POSIX GNMP	IEEE P 1003.1+Extensions (FIPS 151) Draft FIPS, 8 March 1991
Data Management	SQL IRDS RDA	ISO 9075 (FIPS 127) ANSI X3.138 (proposed FIPS) ISO 9759
Data Interchange		
- Graphic Data Interchange	CGM	FIPS 128
- Product Data Interchange	IGES STEP	NBSIR 86-3359, NBSIR 88-3813 DP 10303
- Document Interchange	SGML ODA/ODIF	ISO 8879, ISO 9069, ISO 9070, TR 9573 ISO 8613
Graphics Services	GKS PHIGS	ISO 7942, ISO 8651, ISO 8805 FIPS-153
Network Services Data Communications Transparent File Access Distributed Computing Services	 OSI TFA OSF/1	 GOSIP (FIPS 146) IEEE P1003.8/x
User Interface	X-Windows XVT	FIPS-158 XVT Software, Inc.
Programming Services	C COBOL FORTRAN Ada Pascal PCTE+ SCCS	ANSI X3J11/86-151-Oct 1986, X3.159 ANSI X3.23-1974, 85, FIPS 021-2 ANSI X3.9-1978, FIPS 069-1 FIPS 119 ISO 7185-1983 (FIPS 109) ECMA AT&T

Source: *Application Portability Profile--The US Government's Open System Environment Profile OSE/1*, Version 1, NIST Special Publication 500-17, NIST, April 1991.

Key:
- GKS: Graphical Kernel System
- GNMP: Government Network Management Profile
- IGES: Initial Graphics Exchange Specification
- ODIF: Office Document Interchange Format
- PHIGS: Programmer's Hierarchical Interactive Graphics System
- SGML: Standard Generalized Markup Language
- STEP: Standard for Exchange of Product Model Data
- XVT: Extensible Virtual Toolkit

An extended version of POSIX is recommended in the APP for the operating system interface (see Section 7.2.1). NIST plans a FIPS on the Government Network Management Profile (GNMP) for network management (see Section 8.3). SQL (see Section 5.2.2.2) and the Information Resource Dictionary System (IRDS) data dictionary standard [Ref. Goldfine et al. 1988] (see Section 5.2.4) are recommended for database management. The distributed data component will be handled through Remote Database Access (RDA) (see Section 5.2.3). Recommended for data interchange are the following:

- Computer Graphics Metafile (CGM) (see Section 9.2.2.2)
- Initial Graphics Exchange Specification (IGES), used for engineering graphics (see Section 9.2.1)
- Standard for the Exchange or Product Model Date (STEP) (identified in Section 9.2.1)
- Standard Generalized Markup Language (SGML) (see Section 9.1.2)
- Office Document Architecture/Office Document Interchange Format (ODA/ODIF) (see Section 9.1.1).

Graphics Kernel System (GKS) and Programmer's Hierarchical Interactive Graphics System (PHIGS) are recommended for Graphics Services (see Sections 11.2 and 11.4).

Standards and options identified in US GOSIP (see Section 14.4.3) are recommended for the open systems data communications, as well as Transparent File Access (TFA). OSF/1 Network Computing Services (NCS) is recommended for distributed computing services. X-Windows is recommended for the user interface, providing a non-proprietary windowing capability.

Until a standard is developed, the NIST APP specifies a commercial product, the Extensible Virtual Toolkit (XVT), available from XVT Software, Inc., as its window system interface. XVT provides a logical platform to provide some, it not all, of the graphical and character user interface functionality needed in applications.

Five standard programming languages are recommended (C, COBOL, FORTRAN , Ada, and Pascal), but standard bindings to POSIX for some of these languages (all but C) are still being defined [Refs. Martin 1990; Hankinson 1988; APP 1990]. In addition, the ECMA's Portable Computer Tools Environment (PCTE) (see Section 12.3.2) and the Source Code Control System (SCCS) from AT&T are being recommended for programming services.

NIST plans to update the *APP Guide* every six months. Some planned APP enhancements include adding more about integrated software engineering environments to the Programming Services area and possibly replacing the Graphics Services area with Multi-Media Services. New APP initiatives that NIST may undertake include the following [Ref. Hankinson 1991]:

- Registry of public specifications (for example the consortium specifications from OSF, X/Open, and OPEN88)
- Repository of Open System Frameworks
- Implementors' Workshops, similar to those NIST holds for OSI and ISDN to give APP standards and specifications more rigorous definition.

The IEEE Computer Society's Technical Committee on Operating Systems (TCOS) has formed a number of working groups to progress POSIX and other standards that are required to facilitate applications portability. Table 24 identifies the documents (and working groups known by the same name) being prepared by IEEE on areas other than POSIX for application portability [Ref. NIST 1990a]. The scope and status of POSIX standards work are discussed in Section 7.2.1.

A review of the interface specifications for the APP shows that there are not yet international standards for many of the elements of the recommended architecture. Some are being considered by ANSI, IEEE, and other standards defining bodies, and others are US standards. For example, X-Windows is being considered by the ANSI X3H3.6 working group, and has been promulgated as FIPS 158. The C language bindings are being considered by the X3J11 ANSI working group. NIST is developing interim standards for file management and is recommending NFS to IEEE P1003 as the best starting point for these interfaces [Ref. Hankinson 1988]. The engineering graphics standard (IGES) is still only available as a NIST publication.

Table 25 gives an evaluation of the stability and completeness of the standards recommended by NIST for the APP. Each standard in the seven service areas (security is not addressed) is identified by source and evaluated as one of the following:

- Strategic (i.e., appropriate for long-term planning) new standard, relatively stable (STR)
- Strategic standard expected to be available in the near future, subject to change but nearing international or national standardization (FTR)
- Nonstrategic, serving only as a stop-gap measure and not appropriate for long-term planning (GAP).

Table 24. Applications Portability Standards Being Developed by IEEE for Submission to ISO Through ANSI

P1003.0, *Applications Portability Guide*--addresses the broad applications portability issues, such as: benefits and risks of open system architecture, architectural framework for portability, applications portability concepts, operating systems services, data management and interchange services, data interchange services, graphics services, network services, user interface services, and languages/application development environment services
P1201.1, *Interfaces for User Portability*--defines a formal standard for programming interfaces for the portability of application software that employs Graphical User Interfaces (GUIs) based on the Xt Intrinsics and Xlib programming interfaces defined by the X-Window System (Ballot expected 2Q 1993)
P1201.2, *Drivability*--defines a recommended practice for those elements and characteristics of user interfaces that must be consistent to permit users to easily transfer from one look-and-feel or application to another (Ballot expected 2Q 1992)
P1201.3, *User Interface Management System (UIMS)*--defines a language-independent dialogue applications programming interface to develop applications systems that are independent of user interface concerns and can be more easily ported across a wide range of user interface styles and technologies; would address such features as: separation of presentation-dependent and presentation-independent aspects, and mechanisms for data and control exchange between application and dialogue layers (not yet approved by TCOS)
P1201.4, *Xlib*--submits for direct ballot, without any changes to semantics or syntax, the MIT X Consortium's X-Window System specification X11 (Release 4) of the Xlib functional specifications with integrated C language binding (direct ballot planned for early 1991)
P1224, *Common* ASN.1 Object *Management Applications Programming Interface (API) for X.400 and Directory Services API*--defines an ASN.1 Object Management API...provide a standard interface supporting the manipulation of complex arguments and parameters used by X.400 and Directory Services (Draft 3, August 1991, Ballot of Draft 4 planned for 1Q 1992)
P1224.1, *X.400 Based Electronic Messaging API)*--defines an X.400 API that makes the functionality of a message transfer system (MTS) accessible to a message store (MS) or user agent(UA)...define an X.400 Gateway API with two components: a mail system gateway, and an X.400 gateway service. Base document is from X.400 API Association and X/Open. Work to be done before the ballot include adding language independence features, adding assertions and other test methods, and reformatting the standard into IEEE/ISO form. (Ballot of Draft 4 planned for 1Q 1992)
P1237, *Remote Call Procedure (RPC) Interface Language*--defines an interface description language and a very limited set of procedure interfaces to allow applications to use an underlying RPC mechanism layered on an OSI stack (balloting planned for mid-1992 and approval early in 1993)
P1238 *OSI Application Program Interfaces*, Part 1: *Common Connection Management and Supporting Functions*--defines an API model for connection-oriented OSI Application Layer services (ballot of Draft 4 in January 1992]
P1238.1, *OSI Application Program Interfaces*, Part 2: *File Transfer, Access, and Management (FTAM)*--provides an application program interface to the detailed OSI FTAM services and higher-level user-oriented FTAM-based services (ballot in 1993)

Source: "Applications Portability and Open Systems Environments: Status Report," presented by Roger J. Martin, NIST, *8th APP/OSE Workshop*, NIST, Gaithersburg, Maryland, 12 November 1991.

13.1.3.4 X/Open Common Applications Environment (CAE)

This section discusses the CAE developed by the X/Open international consortium and specified in the X/Open Portability Guide [Refs. Lambert 1987; X/OPEN 1987; X/OPEN 1987a; X/OPEN 1988; XPG3 1989]. The Portability Guide recommends standards and options within standards to achieve an open environment in which new applications can be ported without modification. Several international consortia have endorsed the X/Open CAE as a basis for developing open environments.

Table 25. Applications Portability Standards Being Developed by IEEE for Submission to ISO Through ANSI

	STR	FTR	GAP
OPERATING SYSTEM SERVICES			
Portable Operating System Interface for Computer Environments (FIPS PUP 151-1)	●		
NIST Planned FIPS PUB on POSIX Shell and Utility Applications Interface for Computer Operating System Environments (IEEE P1003.2 Draft 11)		●	
NIST Planned FIPS PUB on Government Network Management Profile (GNMP)		●	
Security Interface for the Portable Operating System Interface for Computer Environments (IEEE P1003.6 Draft 6)		●	
USER INTERFACE SERVICES			
User Interface Component of Applications Portability Profile (FIPS PUB 158)	●		
Extensible Virtual Toolkit (XVT)			●
PROGRAMMING SERVICES			
Ada (FIPS PUB 119)	●		
C (FIPS PUB 160)	●		
COBOL (FIPS PUB 021-3)	●		
FORTRAN (FIPS PUB 069-1)	●		
Pascal (FIPS PUB 109)	●		
ECMA Portable Common Tools Environment (PCTE)		●	
Source Code Control System (SCCS)			●
DATA MANAGEMENT SERVICES			
Information Resource Dictionary System (IRDS) (FIPS PUB 156)		●	
Database Language SQL (FIPS PUB 127-1)	●		
Remote Database Access (RDA)		●	
DATA INTERCHANGE SERVICES			
Office Document Architecture/Office Document Interchange Format (ODA/ODIF), ISO 8613:1989	●		
Standard Generalized Markup Language (SGML) (FIPS PUB 152)	●		
Computer Graphics Metafile (CGM) (FIPS PUB 128	●		
Planned FIPS Initial Graphic Exchange Specification (IGES)			●
Standard for the Exchange of Product Model Data (STEP), ISO DP 10302		●	
GRAPHICS SERVICES			
Graphical Kernel System (GKS) (FIPS PUB 120)		●	
Programmer's Hierarchical Interactive Graphics System (PHIGS) (FIPS PUB 153)	●		
NETWORK SERVICES			
Government Open System Interconnection Profile (GOSIP) (FIPS PUB 146-1)	●		
Transparent File Access (TFA) (IEEE P1003.8 Draft 4)		●	
OSF/1 Network Computing Services Remote Procedure Call (NCS/RPC)			●

Sources: *Application Portability Profile -- The US Government's Open System Environment Profile OSE/1*, Version 1.0, NIST, US Department of Commerce, April 1991, UNCLASSIFIED.

Key: STR Strategic new (relatively stable).
FTR Strategic in the future (subject to change but nearing standardization).
GAP Nonstrategic (stop-gap measure, not appropriate for long term planning).

The foundations of the X/Open CAE are the interfaces of the UNIX System V operating system, as defined in the AT&T System V Interface Definition (SVID), and the C language. The X/Open CAE consists of features grouped in five functional areas: operating system, languages, data management, hardware, and networking. The Third Edition of the Portability Guide (XPG3), published in 1989, defined the CAE in seven volumes:

- Volume 1, System V specification commands and utilities
- Volume 2, System V specification interface and headers
- Volume 3, System V specification supplementary definitions
- Volume 4, Programming languages (revised from earlier version; the COBOL definition is aligned with ANSI COBOL 85)
- Volume 5, Data management (revised)
- Volume 6, Window management (completely new)
- Volume 7, Networking surfaces (completely new).

The next phase of the X/Open CAE will complete the convergence with the current POSIX standard (IEEE P1003.1).

The primary feature of the operating system is the X/Open System V Specification (XVS) that defines the applications interfaces to be provided by the underlying operating system. Another feature of the operating system functional area is the X/Open Native Language System, which is a set of interfaces designed to facilitate the development of applications that can operate in different languages and cultural environments. These two features are defined in the following ways:

- XVS mandates the entire SVID base definition with the exception of the mathematics group.
- XVS has extended the SVID, including extended use of symbolic names to replace numeric constants.
- Some of the SVID kernel extensions are optional in XVS (use of these options could restrict portability).
- The Native Language System is supported by a message catalogue system (messages in the appropriate language are retrieved at run time); a mechanism whereby native language, local custom, and code-set requirements can be identified to applications at run time; enhanced interface definitions of standard C library functions to provide language-dependent character-type classification and special conversions; and a set of standard commands and library functions that will operate correctly with 8-bit characters.

The C language is the primary feature of the language functional area. The X/Open Portability Guide provides guidelines for writing programs designed to be portable and to avoid problems that arise between the AT&T System V C language standard (used for the initial X/Open standards) and the draft standard issued by ANSI X3J11. X/Open has also established definitions for COBOL(based on ANSI X3.23-1974), FORTRAN (based on FORTRAN 77, ANSI X3.9-1978), and Pascal (based on ISO 7185-1983 Level 1).

Data management includes Indexed Sequential Access Method (ISAM) interfaces that are defined for creating, managing, and manipulating indexed files, and SQL for access to relational database management systems. The ISAM definition is based on Version 2.10

of C-ISAM by the Informix Corporation. SQL is based on ISO 9075 (ANSI X3.135-1986) but contains extensions and deviations (see Section 5.2.2.2).

Hardware includes media and formats defined for transferring source code in machine-readable form. The features include 40- and 80-track 5 1/4-inch floppy disks, 1/2-inch magnetic tape, and utilities for transferring files. The primary magnetic tape format is 9-track, phase-encoded at 1,600 bits per inch.

Networking is based on ISO standards and interim standards recommended by the Standards Promotion and Applications Group (SPAG). X/OPEN is working to develop definitions in three areas where there are not yet standards:

- Generalized interprocess communications, with detailed definitions for message passing between processes, shared memory, and semaphores
- Distributed file system
- Distributed transaction processing.

XPG3 was offered to the European Committee for Standardization/European Committee for Electrotechnical Standardization (CEN/CENELEC) as a standard in 1989. Balloting on Draft European Standard (prENV) 40002 was unsuccessful [Ref. CEN 1989]. XPG3 consists of 12 components (listed with reference to other standards work as applicable):

- X/Open System Interfaces (XSI) Commands and Utilities (DP 9945-2, IEEE P1003.2)
- XSI System Interfaces and Headers (ISO 9945-1; IEEE P1003.1)
- XSI Internationalization
- XSI Curses Interface
- Source Code Transfer
- C Language (DP 9899; ANSI X3.159; SC22/WG14 work)
- COBOL (ISO 1989; SC22/WG4 work)
- ISAM (ANSI X3.23 work)
- SQL (ISO 9075)
- Window Management Library Interface
- Transport Interface (IEEE P1103.8)
- Personal Computer Interworking.

The following summarizes some of the comments provided to CEN and EWOS regarding the adoption of the Portability Guide as a European Standard (ENV) [Ref. CEN 1989]:

- XPG3 depends totally on UNIX, which needs an AT&T license, and the AT&T version of C Programming Language which differs from ongoing work in SC22/WG14 (Denmark).

- The X/Open COBOLdoes not agree with ISO 1989 COBOL; the X/Open recommendations appear to match only one existing product (the MicroFocus compiler). X/Open COBOLexcludes some features and specifies some extensions to ISO 1989. There is no real coordination between X/Open recommendations and SC22/WG4 (France).
- The X-Windows standard differs from the one developed at MIT and currently is being used to progress such work in ANSI for possible submission to JTC1 (United Kingdom).

13.1.3.5 Open Software Foundation (OSF) Profiles

The OSF has identified a Level 0 portability profile that is based on the following elements:

- POSIX and the XPG3
- Programming language bindings for ANSI C, COBOL, Pascal, Ada, BASIC, and LISP
- X/Windows
- GKS and PHIGS for graphics
- OSI protocols for networking
- Database Language SQL.

The Level 1 OSF profile standards are still being defined through a request for technology (RFT) process. The base standard for the operating system will be the IBM AIX Version 3 of UNIX. This will be compatible to UNIX System V Releases 2.0 and 3.0 and conformant to POSIX [Ref. OSN 1988a]. The GUI will be a combination of the Microsoft OS/2 Presentation Manager, the Hewlett-Packard window manager, and the Digital Equipment Corporation's toolkit.

OSF is planning a develop a DCE that includes such "technologies" as Architectures, Remote Procedure Call, Naming and Directory, Authentication and Authorization services, Time Management services, Distributed File services, and others [Ref. OSF 1990].

OSF recently issued an RFT for defining and implementing a distributed management environment (DME). The DME is intended to allow heterogeneous computing systems to be managed in a uniform and efficient manner. It will consist of a framework that supports a consistent management approach as well as management applications, common management services, and management information storage systems. After assessing scope, quality, and completeness of the submissions, OSF plans to announce its final selection in the second half of 1991 [Ref. OSN 1991].

13.1.3.6 Technical and Office Protocol (TOP)

The TOP is part of a combined industrial and government effort on the part of users to specify a profile of standard protocols that can be used in commercial applications to

provide connectivity and interoperability. TOP is associated with another effort, Manufacturing Automation Profile (MAP) (see Section 6.3.2.3).

The TOP specification [Ref. Thacker 1987] defines a functional network for distributed information processing for technical and business functions. TOP Version 1.0 (November 1985) is summarized in Table 26. It provides for Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and Token Bus LANs using the connectionless X.25 Internet Protocol and the Class 4 transport protocol. FTAM is supported at Layer 7.

Table 26. Standards for TOP Version 1.0

Layer	References for Standards
7. Application	ISO 8571 (FTAM)
6. Presentation (Null Layer)	(ASCII and binary encoding)
5. Session	ISO 8327
4. Transport	ISO 8073 (Transport Class 4)
3. Network	ISO 8473 (Connectionless and for X.25--Subnetwork Dependent Convergence Protocol, SNDCP)
2. Data Link	ISO 8802/2 (Type 1, Class 1 Logical Link Control)
1. Physical	ISO 8802.3 (CSMA/CD Media Access Control) ISO 8802.4 (Token Bus Media Access Control)

TOP Version 3.0 was released in 1989, and it is expected to have a six-year stability period before release of another version. It provides not only FTAM but also VT, Directory services, network management, and MHS at Layer 7. It further includes the ODIF (ISO 8613), Computer Graphics Metafile (CGM) Interchange Format (DIS 8632), Product Definition Interchange Format (PDIF), and the GKSinterface (ISO 7492). IGES Version 3.0 from ANSI [Ref. ANSI DP ANS Y14.26M-1986, IGES 1986] is included. At the lower layers, TOP Version 3.0 provides for Token Ring LANs and for X.25 packet switching via X.21 and X.21 bus at Layer 1. TOP Version 3.0 is summarized in Table 27.

Table 27. Standards for TOP Version 3.0

Layer	References for Standards
7. Application	ISO 8571 (FTAM) CCITT X.400-1984 (MHS) ISO 9041 (VT, subset VT-B) ISO 8613 (ODIF) ISO 8632 (CGM) ISO 7492 (GKS) ISO 9594 (Directory) ISO 9595 and 9596 (Network Management) ISO 8649 and 8650 (ACSE)
6. Presentation	ISO 8823
5. Session	ISO 8327
4. Transport	ISO 8073 (Transport Class 4)

Table 27. (Continued)

3. Network	ISO 8473 (CLNP, SNDCP) CCITT X.25 PLP
2. Data Link	ISO 8802/2 (Type 1, Class 1 Logical Link Control) CCITT X.25 HDLC (LAPB)
1. Physical	ISO 8802.3 (CSMA/CD) ISO 8802.4 (Token Bus) ISO 8802.5 (Token Ring) CCITT X.21 and X.21 bus (Packet Switching)

PLP: Packet Level Protocol
HDLC (LAPD): High Level Data Link Control (Link Access Precedure Version D)

The international organization, Open Systems Interconnection for Technical and Office Protocol (OSITOP), has been examining architectural issues and has produced a position paper on a solution for connection-oriented network service (CONS) and connectionless-oriented network service (CLNS) internetworking (see Sections 3.2.2 and 6.2.2). This paper reaches the following conclusions:

- It is not realistic to sidestep the CONS vs. CLNS issue by expecting that one of the two incompatible sets of protocols (CONS or CLNS) be abandoned or by accepting the existence of two non-communicating OSI islands.
- Three solutions are valid, although not architecturally correct according to OSI principles:
  - The "265" internetworking function (based on TP4 over CONS)
  - A Distributed System Gateway (DSG)
  - A Multi-System Distributed System Gateway (MSDSG).
- OSITOP recommends the MSDSG solution.

13.1.3.7 Multivendor Integration Architecture (MIA)

Nippon Telegraph and Telephone Corporation (NTT) has announced the introduction of its Multivendor Integration Architecture (MIA). The architecture, developed together with NTT Data Communications Systems (NTT DATA) and five computer vendors (IBM Japan, Digital Japan, NEC, Hitachi, and Fujitsu), will enable the creation of systems composed of different vendors' computers. The architecture has been developed with the intention of providing a multivendor system that users will find easy to use. The information processing system software consists of an operating system with user programs, databases, and interface programs installed for connecting terminals and other equipment. In developing MIA, deferment was given to international standards such as program language specifications and communication protocols that have been time-tested. In areas that have not yet been standardized, the emphasis was on determining what would be necessary from the user's standpoint. In adopting the specification, efforts were focused on either expanding the international standards or on adopting *de facto* standards

and specifications proposed through joint research. MIA consists primarily of three interfaces common to vendors [Ref. OSN 1991a]:

- Application Program Interface (API). The interface located between basic software and application programs which sets the specifications for three programming languages (COBOL, FORTRAN, and C) and the database language SQL, based on ISO and ANSI standards. An interface called the Structured Transaction Definition Language (STDL) was newly specified for the communication access interface and user access interface for distributed transaction processing.
- System Interconnection Interface (SII). This prescribes a communication protocol consisting of four types of upper-layer protocol specifications: file transfer, mail transfer, distributed transaction processing, and network management. The lower layer protocol specifications are also prescribed based on Internet and OSI.
- Human Interface (HUI). MIA uses three types of human interface specifications from OSF/MOTIF, OPEN LOOK, and IBM's Common User Access (CUA).[49] These three interfaces, which are becoming industry standards, are used with UNIX and IBM's OS/2.

13.1.3.8 EWOS Profiles for the Open System Environment (OSE)

EWOS has been studying the application of profiling concepts to the domain of OSE since it proposed (ENV 40002) to create European functional standards for the CAE (see Section 13.1.3.4). ENV 40002 applies the methodology for OSI profiles to the CAE domain, so that the use of the corresponding base standards could also be specified in a similar way for use in procurement.

EWOS has issued a draft document on OSE profiles (EWOS/TA/91/68, April 17, 1991). The document covers the use of standards in a number of broad domains:

- User access techniques
- POSIX interfaces (ISO 9945)
- APIs to system and information services
- Data formats for storage and interchange
- OSI protocol profiles
- Application development tools, languages, and bindings
- Internationalization.

If approved, it would be forwarded to ISO's SGFS for functional standardization. Table 28 shows the proposed taxonomy for OSE profiles.

---

[49] CUA is the user interface portion of IBM's Systems Application Architecture (SAA).

13.1.3.9 Unix International's ATLAS

Unix International recently announced its UI-ATLAS Distributed Computing Program which has the support of 20 companies. UI-ATLAS is designed to meet five challenges to the open systems industry [Ref. Unix 1991]:

- Provide a framework for systems software beyond the operating system level that delivers a complete open systems environment.
- Provide a model for allowing alternative technologies through standard interfaces without loss of investment.
- Interoperability with the installed base of computer systems to protect customer investments.
- Harmonize the industry's diverse approach to open systems technology by allowing the implementation of competitive technologies under a single framework.
- Provide a new paradigm for distributed applications which uses object orientation to better manage the complexities inherent in heterogeneous distributed computing.

Table 28. EWOS Profiles for the Open System Environment

POEnn	Open System Environment Profiles		
	POE0	Base Environment	
	POE1	Workstation Environments	
		POE10	Terminal Environment
		POE11	Personal Workstation Environment
		POE12	Professional Workstation Environment
	POE2	Utility Server Environments	
		POE20	Electronic Message Serving Environment
		POE21	Directory Serving Environment
		POE22	Access Control Serving Environment
	POE3	Information Server Environments	
		POE30	DBMS Server Environment
		POE31	Document Serving Environment
	POE4	Transaction Processing (TP) Environments	
		POE40	Simple TP Environment
		POE41	Enhance TP Environment
	POE5	Real-time Environments	
		POE50	Real-time Environment, seconds
		POE51	Real-time Environment, milliseconds
	POE6	Supercomputing Environments	
POCaa	Open System Environment Components		
	POCA	Application Program Interfaces	
		POCAM	APIs for Management Services (e.g., APIs to access and manipulate managed objects)
		POCAU	APIs for End-User Services (e.g., FIMS API)
		POCAS	APIs for System Services (e.g., ISO 9945-2)
		POCAI	APIs for Information Services (e.g., ISO 9075.2)
		POCAC	APIs for Communication Services (e.g., X.400 API)
	POCL	Look-and-Feel Definitions	
	POCF	Formats	
	POCP	Protocols	

POC: Profiles for Open System Environment Components.
POE: Profiles for Open System Environments.

13.2 Assessment

TBD.

(This page intentionally left blank.)

14. INTERNATIONAL AND NATIONAL STANDARDIZED PROFILES

14.1 Profiles of OSI Standards

The following sections provide examples of the profiles of standards being considered for migration toward open information system environments.

Quick Reference	
Topic	Page
COS/COSINE	295
EPHOS	292
EWOS	281
Int Standardized Prof	282
NATO GOSIP	293
North American OIW	281
OSI Environments	295
POSI	281
Taxonomy of Profiles	283
UK GOSIP	288
US GOSIP	288
Canada's COSAC	288

14.1.1 Regional Workshops Developing OSI Profiles

Three regional international workshops have been established to promote OSI. These are the EWOS, POSI--the Asia/Oceania Workshop (AOW), and the North American OSI Implementor's Workshop (NAOIW; since the NAOIW is hosted by NIST, it is sometimes called the NIST OIW).

A Regional Workshop Coordinating Committee has also been established to promote dialog and harmonization among the regional workshops. The goal of the workshops is to define standards profiles that will ensure interoperability of products from different vendors. They are public technical fora organized to provide timely development of implementation agreements and testing details based on international standards. As indicated in Section 14.1.3, the *Stable Implementation Agreements* [Refs. NIST 1988; NIST 1990b] from the NAOIW form the basis of US GOSIP. A companion document, *Continuing Agreements* [Refs. NIST 1989; NIST 1990c], provides the basis for enhancements and future revisions to US GOSIP.

While the current NAOIW represents a successful model for bringing developers together to identify the additional specificity and precision required to insure product interoperability, the workshop process may need to change to:

- Include users in an active and visible role of stating requirements and priorities
- Broader the base of technology providers participating in workshop activities
- More closely align and synchronize assignments, responsibilities, processes and work priorities, and outputs with other regional workshops, user groups and vendor consortia
- Provide a way for bridging specification gaps with other specifications where appropriate *de jure* standards do not exist
- Adopt a top-down versus bottom-up approach that reflects a market-driven instead of technology-driven perspective.

Moreover, the NAOIW has formed an ad hoc group to explore issues and if appropriate propose recommended actions needed to expand the NAOIW's scope and associated processes into OSEs by establishing an OSE Workshop. The group's report, which was to be presented in December 1991, recommends that the NAOIW [Ref. Landberg 1991]:

- Revise the NAOIW's charter to explicitly state that technical subjects beyond OSI and into the realm of OSE be addressed
- Permit the use of public domain specifications by technical work groups where approved by the general membership
- Create new Workshop committees to manage expansion and technical issues surrounding OSE scope and frameworks
- Develop mechanisms to accept user requirements from external sources
- Increase liaison with other regional workshops to resolve generic OSE issues and to coordinate work activities and study groups.

14.1.2 International Standardized Profiles (ISPs)

ISO/IEC JTC1 has set up a Special Group on Functional Standardization (SGFS) to develop standards for International Standardized Profiles (ISPs). An ISP is somewhat more general than the common use of the term "profile" in that a profile is a stack of protocols to be used in combination, whereas an ISP is a document in which one or more profiles are published. The procedures adopted for specifying ISPs are unique because international harmonization is intended to be achieved before candidate ISPs are submitted to ISO. Proposals for ISPs are expected to be accepted by the international regional workshops EWOS,[50] NAOIW, and the AOW before becoming proposed draft ISPs (PDISPs). As noted in Section 14.3.3.2, the SGFS has developed a six-part draft ISP for FTAM. Dozens of others are being discussed in the regional workshops.

The SGFS meets in plenary session in June of each year, 1991-1995 [Ref. SGFS N 242 1991]. The scope of the work of the SGFS is the following [Ref. SGFS N 293 1991]:

- Definition of functional standardization and functional standard
- Development of a catalogue of functional standards with appropriate classification
- Definition of a methodology for achieving functional standardization
- Development of a set of operating procedures and assessment of resources
- Execution of the review of proposed draft functional standards

---

[50] EWOS taxonomy for profiles for open systems environments is given in Section 13.4.3.8.

- Consideration of the requirements of functional standards on conformance and maintenance
- Development of expeditious publication procedures.

The main work of the SGFS is the development of a framework (TR 10000-1) and a taxonomy for ISPs (TR 10000-2), which gives priority to profiles for OSI but recognizes that the profile principles may also apply to other technical areas. This taxonomy contains a classification and identification scheme for candidate profiles, is being adopted by TSGCE SG9, and will be used in forthcoming editions of the *NTIS Transition Strategy*. TR 10000 identifies profiles (specification for how to accomplish a function) and ISPs (harmonized documents). TR 10000 allows an ISP to contain one or more profiles by permitting more than one part, each of which can contain a profile. It is expected that an ISP may contain 5 to 10 profiles. Profiles may only be submitted to the SGFS by one of the three regional workshops (NAOIW, EWOS, and Asia Oceania Workshop). Fifteen profiles were submitted to the SGFS in 1990, of which 4 were published and 11 are under review prior to balloting. An additional 15 profiles were expected to be submitted in 1991, and 25 more are under development in the regional workshops [Ref. SGFS N 295 1991].

A directory of ISPs and profiles contained therein accompanies TR 10000 to provide additional information about ISPs and profiles [SGFS N 100, September 1991] It includes:

- Status information about each profile identified in TR 10000
- Summaries of existing or proposed profiles
- Information about the possible joint use of A/B profiles.

The June 1991 meeting of the SGFS in Berlin considered the extensions that have been proposed to the work already performed and foresees several major activities. It plans to update TR 10000-1 to accommodate experience with the first group of pDISP submissions and to take account of new profiles which have been identified and which fall within the scope of TR 10000-2. A working draft will be submitted to the SGFS for postal comments, and once these comments have been incorporated will be submitted to national ballot as a draft revision of TR 10000-1. TR 10000-2 was updated in June 1991 to include several requested amendments and extensions to the taxonomy. The draft revision was approved by the group and was to be submitted to national ballot in the second half of 1991.

The SGFS meeting in June 1991 considered documents from member bodies and from EWOS and SC22/WG15 relating to the extension of the TR 10000 framework and taxonomy to encompass the OSE. It was resolved to convene an Authorized Subgroup meeting to discuss the development of the concepts needed to incorporate profiles for OSE in the area of functional standardization. During 1992 there will potentially be a

requirement to update TR 10000 and the procedures document (SGFS N 100) in line with the agreements of the ISP-SWG meeting in Geneva during June 1991. [Ref. SC6 N 6977 1991]

SGFS has accepted the responsibility for profile test specifications, which will be produced on the same basis as the profile definitions produced by the SGFS [Ref. SC6 N 6976 1991]:

- They will be published as ISPs or ISP parts, related to the ISPs for the profiles to which the tests relate
- Criteria for inclusion of references to the base standards for relevant abstract test suites will be the same as those for references to PICS proformas
- Methods of generating and balloting ISPs will be the same as for profiles.

The Regional Workshops Coordinating Committee (RWS-CC) of ISO JTC1 has noted a number of harmonization efforts: conveyance of ODA over MHS(84); FTAM document types from CGM, *COBOL*, ODA, and EDI; a Document Application Profile (DAP) for raster graphics in ODA; general upper layer agreements; character set repertoires and their encoding; and an international registry (IR) or library (IMIL) [Ref. SGFS N 282 1991].

Table 29 shows the overall organization and labels (taxonomy) used to identify and distinguish ISPs. It shows the distinctions created by the choice of connection-oriented (CO) or connectionless (CL) modes (see Section 3.2.2). There are four classes of ISPs in the taxonomy of TR 10000: application profiles (*AXX nn* for those requiring the COTS and *BXX nn* for those requiring CLTS); interchange format and presentation profiles (*FXX nn*); transport profiles (*TX nnnn* and *UX nnnn* for CO and CL profiles, respectively); and relay profiles (*RX p,q*).

14.1.2.1 Interchange Format and Presentation Profiles

These profiles are coded by information type (three letters), document structure (first digit), and architecture (second digit). The information types are (the last two have no two-digit extensions):

- Office document: *FOD nn*
- Data stream: *F n*
- Virtual terminal control objects: *F n*
- Computer graphics: *FCG nn*
- SGML document: *FSG*
- Directory data definitions: *FDI*.

Section 4.1.1 lists the office document profiles under development.

Table 29. Overview of Taxonomy for International Standardized Profiles

A	Application profiles using CO-mode transport service (TS)
B	Application profiles using CL-mode TS
F	Interchange format and representation profiles
T	Transport profiles providing CO-mode TS
	- TA CO-TS over CL network service (CLNS) using Transport Protocol (TP) Class 4 as defined in ISO 8073/DAD 2
	- TB CO-TS over CO network service (CONS) with provision of TP Classes 0, 2, and 4
	- TC CO-TS over CONS with provision of TP Classes 0 and 2
	- TD CO-TS over CONS with provision of TP Class 0
	- TE CO-TS over CONS with provision of TP Class 2
U	Transport profiles providing CL-mode transport service (TS)
	- UA CL-TS over CLNS
	- UB CL-TS over CONS
R	Relay profiles between T- or U-profiles

14.1.2.2 Application Profiles

These profiles are coded by application supported and transport mode required (three letters, where the first letter is "A" if requiring COTS and "B" if requiring CLTS--no *BXX nn* profiles have yet been identified), service type (first digit), and functional association (second digit). The applications are :

- FTAM: *AFT nn*
- MHS (1984): *A/3 nn*
- MHS (1988): *AMH nn*
- VT: *AVT nn*
- TP: *ATP nn*
- RDA: *ARD*
- OSI Management: *AOM nn*
- Directory: *ADI n.*

Section 6.3.3.2 lists stable FTAM profiles that have been developed and are under development. Others are [Ref. OSN 1991c]:

- AMH 11, *MHS, Common Transfer Facilities: MTA to MTA (P1)*, Source: EWOS, 1991
- AMH 12, *MHS, Common Transfer Facilities: UA to MS (P7)*, Source: EWOS, 1991
- AVT 22, VT, *Basic Class (S-mode), Forms*, Source: EWOS
- pDISP 11183-1, AOMnn - *OSI Management - Management Communications Protocols - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by ROSE and CMISE*, Second Version, 27 April 1991 [SGFS N 357 and 358, 24 May 1991]

- pDISP 11183-2, AOMnn - *OSI Management - Management Communications Protocols - Part 2: Enhanced Management Communications*, Fourth Version, 27 April 1991 [SGFS N 359, 24 May 1991]
- pDISP 11183-3, AOMnn - *OSI Management - Management Communications Protocols - Part 3: AOM11 - Basic Management Communications*, Draft pDISP text, First Version, 23 May 1991 [IST/21:2808]
- AD1, Directory, *Directory Access Protocol*, Source: NAOIW.

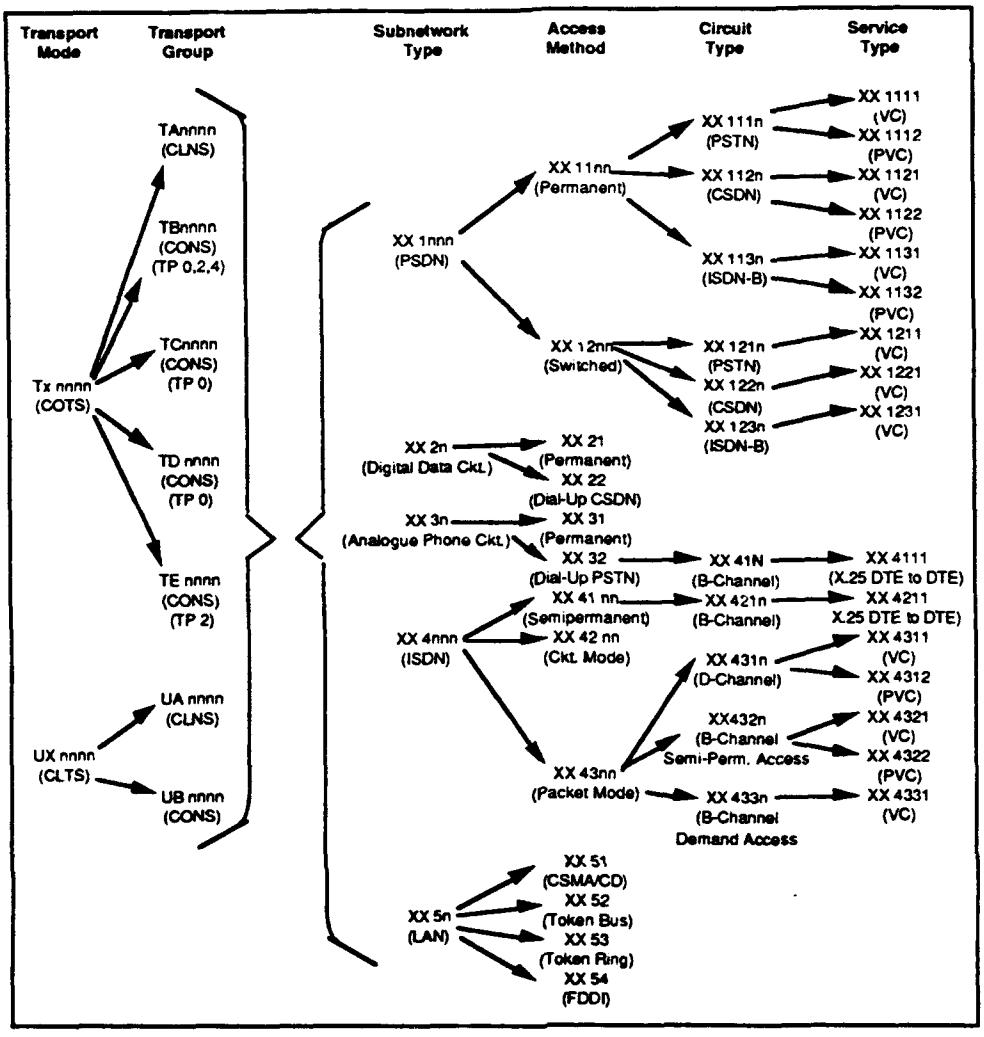
14.1.2.3 Transport Profiles

These profiles (Figure 17) are coded by transport mode (first letter "T" for COTS and "U" for CLTS), transport group (second letter), subnetwork type (first digit), access method (second digit), circuit type (third digit), and service type (fourth digit). The transport groups are CLNS (*TA* or *UA*), TP 0/2/4 over CONS (*TB* or *UB*), TP 0/2 over CONS (*TC*), TP0 over CONS (*TD*), and TP2 over CONS (*TE*). The subnetwork types are PSDN ("1"), digital data circuit ("2"), analogue telephone circuit ("3"), ISDN ("4"), and LAN ("5"). The access methods differ for circuits and LANs:

- Circuit access methods: permanent ("1"), switched ("2"), and packet mode ("3")
- LAN access methods: CSMA/CD ("1"), token bus ("2"), token ring ("3"), and FDDI ("4").

Transport profiles under development include [Ref. OSN 1991c]:

- pDISP 10609, *Transport Profiles, Parts 1-9* [SGFS N 249-257, 19 July 1990]
- pDISP 10608, *Local Area Network Profiles, Parts 1, 2, and 5* [SGFS N 260-262, 19 July 1990]
- TA 52, *LAN, Token Bus: CLNS*, Source: NAOIW
- TA 53, *LAN, Token Ring: CLNS*, Source: EWOS, January 1991
- TA 54, *LAN, FDDI: CLNS*, Source: AOW
- TC 1131, *PSDN: ISDN: B-channel semi-permanent, Virtual Call*, Source: EWOS, 1991
- TC 1231, *Switched Access to a PSDN:* ISDN *B-channel case: Virtual Call*, Source: EWOS, 1991
- TC 41. ISDN, *Semi-permanent Service*, Source: EWOS, 1991
- TC 42. ISDN, *Circuit-mode Service*, Source: EWOS, 1991
- TC 43, *ISDN, Packet-mode Service*, Source: AOW, 1991
- TC 51, *LAN CSMA/CD*, Source: EWOS, 1991
- TC 53, *LAN, Token Ring*, Source: EWOS, 1991
- TC 54, *LAN, FDDI*, Source: AOW.



Source: [Ref. Onufer 1990].

Figure 17. Taxonomy for International Standard Transport Profiles

14.1.2.4 Relay Profiles

These profiles are coded by relay type:

- CLNS: *RA p,q*
- CONS: *RB p,q*
- X.25: *RC p,q*
- MAC using transport bridging: *RD p,q*
- MAC using source routing: *RE p,q*
- CLNS to CONS: *RZ p,q*.

The four-digit numbers p and q each use the four-digit numerical classification of the transport profiles. They thereby identify the subnetwork types between which the relay occurs.

Relay profiles under development include:

- RA51.51, *Relaying CLNS, CSMA/CD - CSMA/CD, Source*: EWOS, 1991
- RA51.1111, *Relaying CLNS, CSMA/CD - PSDN/Virtual Call/PSTN Leased*, Source: EWOS, 1991
- RA51.1121, *Relaying CLNS, CSMA/CD - PSDN/Virtual Call/Digital Cct. Leased*, Source: EWOS, 1991
- RC51.1111, *Relaying X.25 Packet Layer Protocol, CSMA/CD - PSDN/Virtual Call/PSTN Leased*, Source: EWOS, 1991
- RC51.1121, *Relaying X.25 Packet Layer Protocol, CSMA/CD - PSDN/Virtual Call/Digital Cct. Leased*, Source: EWOS, 1991
- RD51.51, *Relaying MAC Serv. Using Transparent Bridging, CSMA/CD - CSMA/CD*, Source: EWOS, 1991
- RD54.54, *FDDI-FDDI*, Source: AOW, tbd.

14.1.3 UK, US, and CA GOSIP

This section discusses UK GOSIP and US GOSIP, illustrated side by side in Figures 18 and 19. Documentation for UK GOSIP was originally issued in March 1988 for mandatory use in 1990. It is now in Version 4 [Ref. OSN 1991i, 19]. Figure 18 shows the standards recommended for UK GOSIP. Documents for Version 4 of UK GOSIP, *UK Government OSI Profile*, are:[51;52]

- Volume I, *Introduction*
- Volume II, *Specification*
- Volume III, *Procurement Handbook*.

Previously, UK GOSIP was completely revised and updated on an annual basis. Now the life span of the new GOSIP 4 document sets is expected to be 2-3 years which will allow periodic updates to be added into the new ring-binder format. [Ref. OSN 1991m]

Rather than repeat UK GOSIP, Canada has prepared *Canadian Open Systems Applications Criteria (COSAC)* as a Government strategy toward open systems. The strategy is analogous to UK GOSIP and fully subscribes to ISO conventions. The mandate

---

51 *GOSIP 4 Supplier Set*, Six volumes; Volume 1 - Overview; Volume 2 - Network Support, Volume 3 - Application Services (1); Volume 4 - Application Services (2); Volume 5 - Interchange Formats and Ancillary Services; and Volume 6 - Annexes (containing interim specifications).

52 *GOSIP 4 Purchaser Set*, Five volumes; Volume 1 - Overview; Volume 2 - Network Support, Volume 3 - Application Services; Volume 4 - Information Interchange and Supporting Services; Volume 5 - Annexes (containing tutorial material and references).

of the Department of National Defence in Canada is to follow COSAC (i.e., UK GOSIP) where defined and otherwise to revert to ISO open systems specifications. Canada does not plan to develop a national, made-in-Canada open system architecture. The COSAC manual has not yet been printed; it is expected to be available after February 1992. [Ref. Beggs 1992]

Figure 19 shows the standards and options recommended for US GOSIP, Version 2.0 [Ref. GOSIP 1990]. These are based on the March 1990 *Stable Implementation Agreements for Open Systems Interconnection Protocols*, Version 3, Edition 1, of the NAOIW [Ref. NIST 1990b]. Version 1.0 was issued as FIPS 146 on 3 August 1988. Version 2.0 was issued as FIPS 146-1 on 3 April 1989. Use of FIPS 146 was mandatory August 1990, and FIPS 146-1 became mandatory on 3 October 1991.

Whereas in Version 1.0 of US GOSIP only the CL-mode network layer protocols were recommended for packet switched wide area networks (WANs), Version 2.0 makes CO-mode network service optional. This, and the addition of the Network Service Access Point (NSAP) address structure, will align the standard with those currently being addressed by ISO.

In addition to recognizing, including, and resolving Version 1.0 errata, Version 2.0 of US GOSIP, published in October 1990 [Ref. GOSIP 1990], also includes the following protocols: VT (forms profiles and TELNET), ODA/ODIF, ISDN, connection-oriented network service, connectionless transport, and end-system to intermediate system (ES-IS) network layer protocols. These protocols would be added in Version 3.0, which is planned for 1995: Directory services (CCITT X.500), VT (page, scroll, and forms), 1988 CCITT extensions to MHS, FTAM extensions, FDDI, optional Transport Class 2, Computer Graphics Metafile, MMS, network management, optional security enhancements, SGML, EDI, and intra-domain routing protocols. Version 4.0, planned for 1997, will include transaction processing (TP), remote database access (RDA), additional network management, additional optional security, and inter-domain routing protocols [Ref. OSN 1991e, 4].

Future versions of US GOSIP will continue to be based on the agreements reached in the regional NIST OSI Implementor's Workshop. Working agreements from the NAOIW that have not reached final form are found in the *Working Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements*. These agreements provide the basis for projections of US GOSIP for 1992 and beyond.

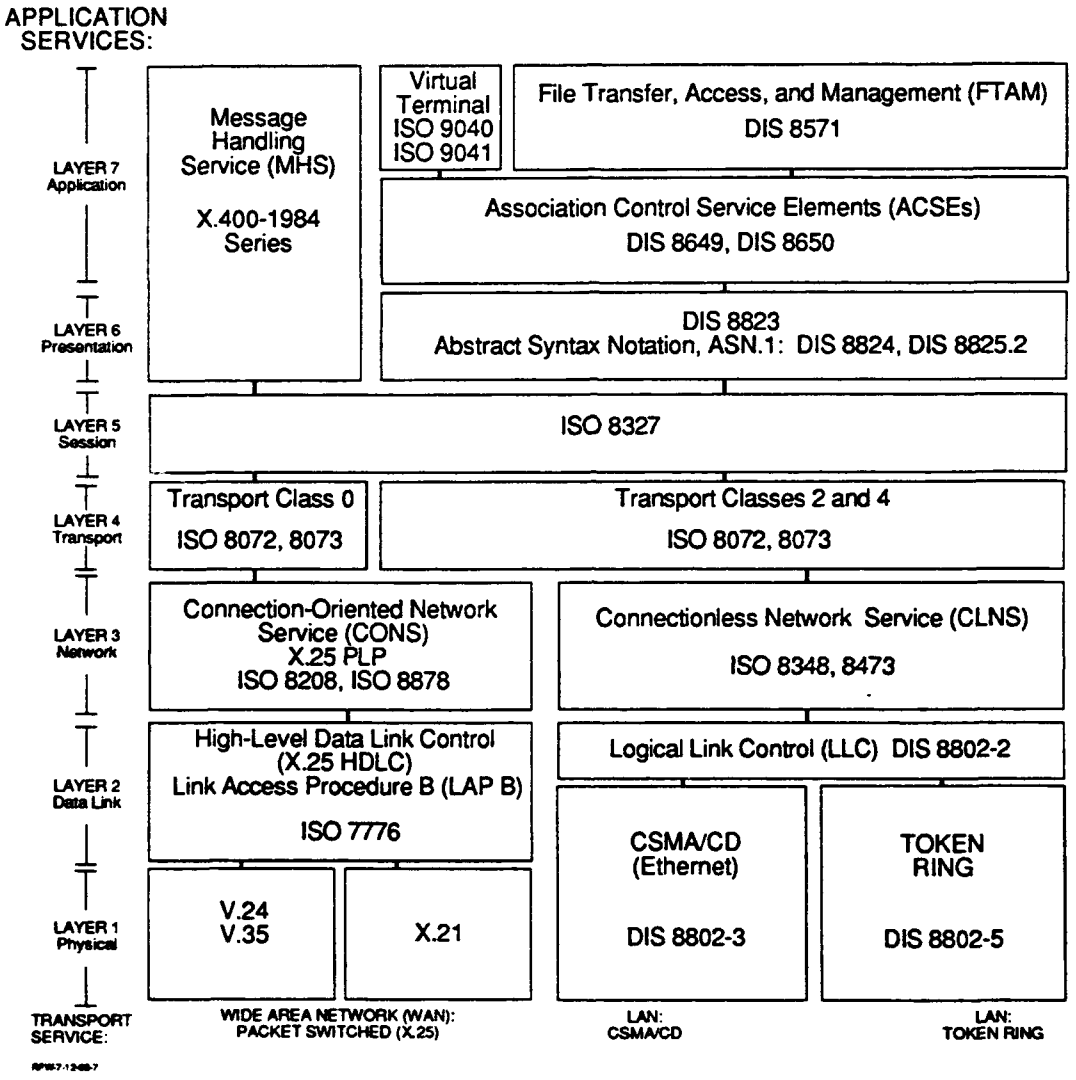


Figure 18. Stacks of Standards Recommended for UK GOSIP

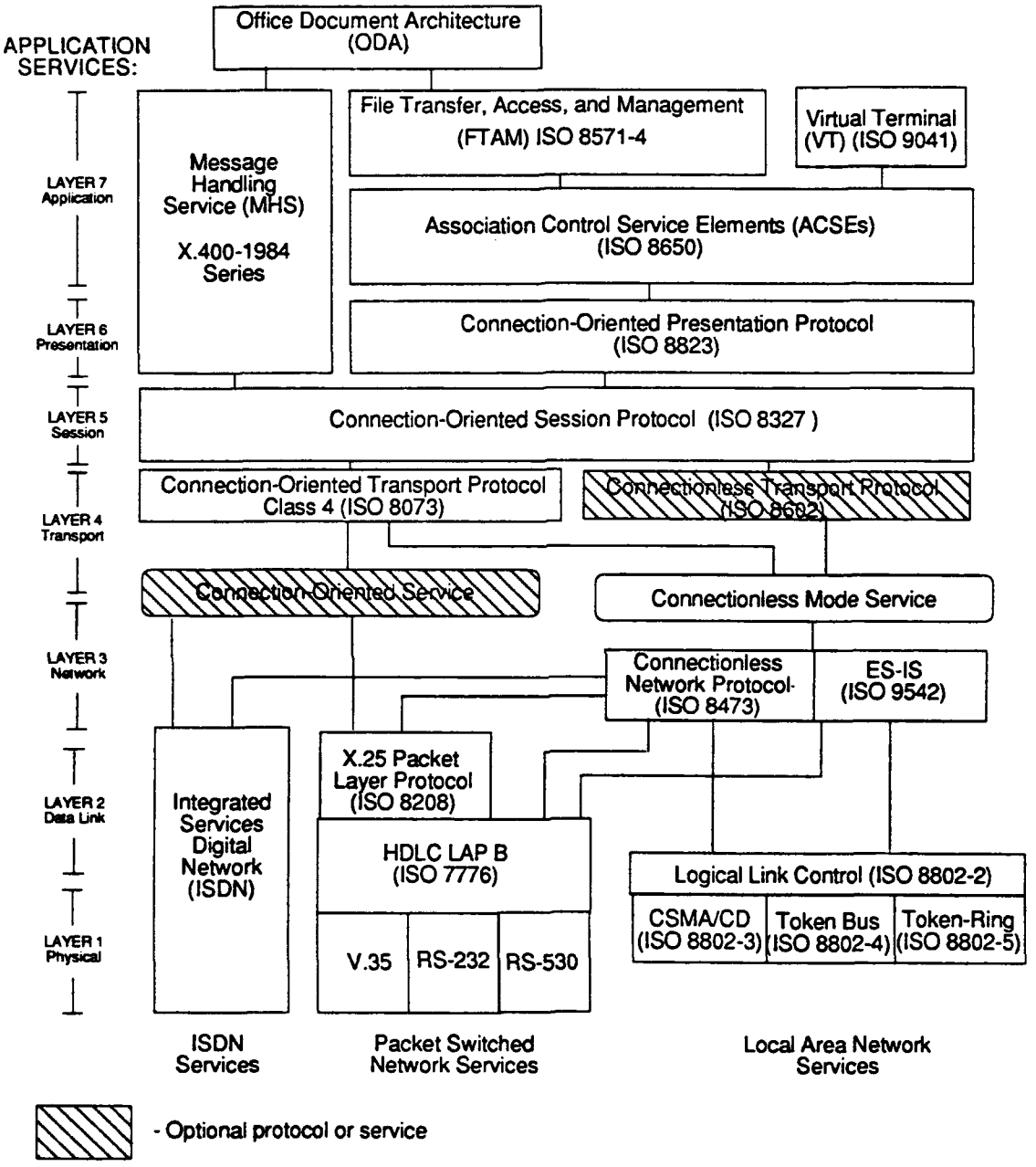


Figure 19. Stacks of Standards Recommended for US GOSIP (Version 2.0)

A detailed description of the plans, based on US GOSIP, to introduce OSI protocols into the US DoD is provided in *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy* [Ref. MITRE 1988]. The baseline for US tactical implementation of OSI standards and protocols will be based on the work of TSGCE SG9, the *NTIS Transition Strategy*, and associated STANAGs. Tactical networks may use GOSIP-specified lower-level protocols until NTIS protocols are developed and commercially available. When the NATO standards are complete, approved, and available, those required for DoD use will be introduced as GOSIP Advanced (post-1989) Requirements [Ref. MITRE 1988].

While some major vendors such as IBM are offering (or about to offer) OSI for much or all of their product line, they are typically offering TCP/IP as well. The 15 August 1990 GOSIP mandate seems to have influenced the schedule for many of the OSI implementors, so a number of first generation OSI products either are just appearing or expected shortly. Activity in the TCP/IP product lines is undiminished [Ref. PSSG 1991].

NIST is publishing a series of GOSIP evaluation guidelines that are now available for electronic mail and transfer. These guidelines explain how implementations can differ, and they assist Federal agencies and other users in determining which among several implementations best suits their needs [Ref. OSN 1991e, 5].

Since Version 3 of GOSIP will be introducing standardized network management, an important area where a lot of standards work remains to be done, NIST is developing a number of FIPS concerning network management. They will be published in stages, one each year for the next three years, and will describe the objects that have to be managed to perform network management or OSI management in the following functional areas:

- Phase I: 802, X.25, ISDN, FDDI, modems, multiplexors, bridges, and physical link
- Phase II: protocol software, routers, terminal services, MTAs, PBXs, and circuit switches
- Phase III: applications, services, operating systems, computer networks, and DBMSs.

The staging of these FIPS reflects user priorities. In a survey of Federal agencies, NIST found that the most important area is management for local area networks and Layers 1 and 2 of the OSI Reference Model. Next were Layers 3-7 and then network management applying to operating systems, applications, and services [Ref. OSN 1991e, 7].

14.1.4 European Procurement Handbook for Open Systems (EPHOS)

Decision 87/95 from the European Community (EC) requires the specification of OSI standards for public procurements. A document is being developed by France,

Germany, and the United Kingdom to provide guidance for such procurements. The document is called the European Procurement Handbook for Open Systems (EPHOS) and is based on base profiles of the UK GOSIP specification. Where possible, EPHOS will cite European standards and ISPs.

In early 1991, EPHOS achieved two significant milestones. The Phase I draft covering X.25, MHS, and FTAM now reflects member nations' formal comments, and Phase II has progressed to the point of agreement on further coverage. The original intention to publish procurement guidance on MHS-88 has been undermined by slow progress on the European standards, and EPHOS Phase I has been revised to focus on MHS-84 with only preliminary guidance on specifying MHS-88 added functionality. Phase II topics will include: Phase I maintenance, FTAM, MHS-88, LAN, cabling, document formats, character repertories, Security, EDI, directory services, VT, LAN/WAN interworking, and identification of areas where standards are inadequate or absent [Ref. OSN 1991g].

14.1.5 International Versions of GOSIP

Initiatives have been taken to develop an international version of GOSIP. The initial meeting in October 1988 was sponsored by the United Kingdom, with participation from France, Germany, Canada, Japan, Sweden, and the United States. The next meeting in Japan will highlight attempts to gain support from other Pacific nations.

14.1.6 NATO GOSIP and NATO Standardized Profiles (NSPs)

A number of profiles have been developed in TSGCE SG9. These include (see Appendix H) the *Military Message Handling System* (draft STANAG 4257), R.131(M)--*Relay for Connecting PSDNs using X.75*, TC 111(M)--*Permanent Access to a PSDN*, and TA 51(M)--*COTS over* CLNS *and CSMA/CD LAN*. Profiles identified in the *NTIS Transition Strategy* are described in Appendix B. TSGCE SG9 is considering developing a NATO OSI standard profile along the lines of UK and US GOSIP.

The US Data Communication Protocol Standards (DCPS) Technical Management Panel (DTMP) has agreed to focus its work on preparing DoD Standardized Profiles (DSPs) that meet the military requirements identified by SG9 and that could be submitted to SG9 as draft NSPs. [Ref. Booz-Allen 1991]

NIST has pointed out that focusing solely on developing DSPs (and by implication NSPs) would be shortsighted and that a balanced strategy for the US DoD (and by implication for the Nations) would be to make every effort to promote the military requirements in the regional workshops that are developing the ISPs to try to get the military requirements agreed in implementor's workshops, thus with some chance of getting them incorporated in future commercial products. NIST noted that military

requirements had been successfully incorporated in base standards and in profiles by working with civilian agencies and, using NIST, through ANSI to ISO in such areas as TP4, CLNP, MHS, FTAM, and VT--all of which have functions that support DoD requirements. NIST has suggested that the most effective roles for DoD in commercial information technology standardization are [Ref. Mills 1991]:

- Identify requirements
- Develop basic technical solutions
- Work with NIST to achieve commercialization
- Support the results through purchase and deployment of the resulting products
- Limit DoD enhancement to only the most essential items (e.g., the security labelling scheme in the current version of GOSIP).

NIST points out that a DoD focus on military enhancements tends to perpetuate DoD-unique solutions and to increase market fragmentation. Fragmentation could slow down the deployment of OSI. In addition, there will continue to be a temptation to identify new or different requirements, even where existing commercial products satisfy the DoD requirements, which necessitate major investments in standards development, maintenance, test suite development, testing, and seeking to gain commercial acceptance. Fragmentation also lessens the impact of Government-wide adoption of GOSIP (e.g., GOSIP 3.0, which is expected to be cited by such sectors as manufacturing, aerospace, and electric power industries).

14.1.7 Industry/Government Open Systems Specification (IGOSS)

Efforts in North American to align the MAP/TOP, US GOSIP, and the Utility Communications Architecture (UCA) developed by the power industry have not been fully successful, primarily because of the different times and slightly different requirements addressed in these specifications. A panel of members from key organizations associated with these specifications has been formed (October 1991) to develop a single US or, if possible, North American OSI specification that consolidates the requirements of all major users. The common specification will be called the Industry/Government Open Systems Specification (IGOSS). A draft of IGOSS for public review and comment is planned for August 1992; an expeditious review could lead to promulgation for ratification by March 1993. It is envisioned that the base document for IGOSS would be US GOSIP Version 2, that NIST would be the coordinating editor, and that the final text would be promulgated as a FIPS in the United States. [Ref. Collela 1992a]

14.1.8 Other Profiles and Transition Strategies

This section is intended to be expanded to address additional activities and options to support transition from existing military and other standards to standards for open

environments. Examples are application gateways, test systems, and test methodologies. Efforts to highlight functional standards, select stacks of mature standards and options within standards, and harmonize implementations will be examined. One example is the *Guide to the Use of Standards* [Ref. SPAG 1987] developed by SPAG in Europe. Functional standards based on OSI standards are being developed by the Interoperability Technology Association for Information Processing, Japan (INTAP), specifically towards an interoperable distributed database system [Ref. Konoike 1987]. Recommendations for functional standards and cooperation with European and US organizations and companies are also provided in Japan by POSI.

14.2 OSI Environments

14.2.1 ISO Development Environment (ISODE)

ISODE is prototype software, developed as a tool to study OSI. In the current vacuum of OSI implementations; however, ISODE has become a default reference implementation of the OSI upper-layers, a platform for deploying OSI services, and a means for transitioning from TCP/IP to OSI protocols.

The ISODE software supports various OSI protocols and applications. ISODE is aligned with US GOSIP. The current modules include the following [Ref. Rose 1990]:

- OSI transport service (TP0 on top of TCP, X.25, and the CO network service; TP4 for SunLink OSI)
- OSI session, presentation, and association control services
- ASN.1 abstract syntax/transfer notation tools
- OSI reliable transfer and remote operations services
- FTAM/FTP gateway
- OSI Directory services
- OSI VT (basic class and TELNET profile).

14.2.2 COS/COSINE Recommendations

Initial profiles for Cooperation for Open Systems Interconnection in Europe (COSINE) have been released. These profiles are summarized in Table 30. In addition to those standards cited in the table, COSINE is evaluating:

- Virtual Terminal, ISO 9041 (with AD2 screen mode)
- EWOS Profile A/122 for file access
- Additional message handling services (CCITT X.400-1988)
- Job Transfer and Manipulation (JTM), ISO 8832 and ISO 8833.

Table 30. Standards for COSINE Profiles

Layer	References for Standards
7. Application	ENV 41204 (FTAM) ENV 41910 (Remote Terminal Access) EWOS Profile A/111 (File Access) RARE MHS and CCITT X.400-1884 MHS Services Remote Job Entry (to be defined in EWOS)
6. Presentation	(Null Layer)
5. Session	(Null Layer)
4. Transport	(Connection-Oriented)
3. Network	(Connection-Oriented)
2. Data Link	CCITT X.25-1984
1. Physical	Local Area Networks (not specified)

14.3 Assessment of Coverage by Standards

Some issues and related findings for communications services are:

- Lack of capability to cross between connection-oriented and connectionless-mode services in OSI profiles. The OSI Reference Model is now being revised to incorporate connectionless services (previously treated as an addendum). Most work on crossover is being addressed by transport or relay bridges, some of which do not conform to the Reference Model. This is a major problem for interoperability between North America (which uses predominantly connectionless modes) and Europe (which uses predominantly connection-oriented modes). As an example, US and UK GOSIP are not compatible and no progress has been made to converge these efforts. However, Version 2.0 of US GOSIP includes an optional connectionless transport service and an optional connection-oriented network service for use on end-systems connected to X.25 networks that are not going to be connected to local area networks.
- Few international standardized profiles (ISP) have been adopted by ISO. Work on FTAM profiles is the most mature and three of the FTAM ISPs have been adopted by ISO. EWOS is preparing a number of candidates for adoption in ISO, but these emphasize connection-oriented services. Profile work in NIST is progressing rapidly, but the products are not yet in the form that can be used for an ISP. Adoption of common ISPs is critical to the compatibility of products based on OSI and other open system protocols.

15. STATUS OF NATO OSI DATA COMMUNICATIONS STANDARDS

15.1 Introduction

This chapter and the next examine NATO efforts to specify and implement open system standards and architectures to achieve interoperability. The purpose is to (1) assess the progress being made in NATO to incorporate military requirements in international standards and to define, where necessary, extensions to those standards, and (2) identify the NATO standards and profiles that may be applicable to ATCCIS (and other CCISs).

This section is followed by a discussion of the eight military requirements defined by TSGCE SG9 (Section 15.2) and an overview of SG9's organization and the plans and activities of the working groups (WGs) within SG9 (Section 15.3). Section 15.4 provides an assessment of the status of draft OSI STANAGs, with particular attention to the way in which each draft STANAG addresses the military features. The chapter concludes with a summary of related standards work in NATO bodies (Section 15.5) and the findings (Section 15.6).

Quick Reference	
Topic	Page
AHWG on ISDN	322
AHWG on MMHS	329
AHWG on OSI Mgmt	319
AHWG on Security	327
Assessment	350
CSNI	316
EUROCOM	349
Lightweight Protocols	348
MIDLA	318
MIDS LVT	333
Military Requirements	297
MPDT	308
NATO OSI Ref Model	333
NIIF	347
NOSIP	304
NSPs	304
OSI STANAGs	333
Transition Strategy	304
WG1-Lower Layers	305
WG2-Upper Layers	311
WG3-CSNI	316
WG4-Data Links	331
WG5-Layer/Profiles	300
WG6-Pan-Layer Issues	300

15.2 Military Requirements for NATO OSI

This section summarizes the requirements associated with incorporating military enhancements into open systems interconnection (OSI) standards. Within NATO, this work has been assigned to TSGCE SG9. General information on NATO and international standards bodies concerned with OSI standards is provided in Appendix F.

Beginning in February 1983, a number of military requirements have been identified in NATO that are not adequately covered by existing OSI standards. Eight military features were identified in the NATO Interoperability Management Plan (NIMP) [Ref. NIMP 1988], and TSGCE SG9 has recommended that the OSI Reference Model (STANAG 4250) be extended to provide support for these features:

- Multihomed, mobile host systems
- Multi-endpoint connection
- Internetworking
- Network/system management functions
- Security

- Robustness and quality of service
- Precedence and preemption
- Real-time and tactical communications.

Table 31 gives the description of the eight military features as provided in *Use of OSI Standards in NATO--Strategic and Technical Issues*, March 1988 [Ref. UK 1988].

Table 31. Eight Military Features for Enhancing OSI in NATO

(1)	Multihomed and mobile host systems. Multihoming is a mechanism for attaching an end system to two or more network access points without the need for a system setting up a call to it to be aware of the extra connectivity. In addition to enhancing survivability, this facility may be extended to support "mobile hosts" such as aircraft and ships.
(2)	Multi-endpoint connections [multi-addressing; multipeer data transmission (MPDT)].[53] In order to transmit data to a number of recipients, it is usually necessary to establish several connections and send separate copies of the data across each connection in turn. More efficient use is made of the communications resources if the sender has to transmit only one copy of the data. The network then takes care of routing, control, and distribution of the data.
(3)	Internetworking. Mechanisms are required to facilitate the interconnection of various NATO systems at the boundary point between subnetworks.
(4)	Network or system management functions. Management functions are required that may be of greater sophistication than those considered satisfactory for civilian networks. Management of broken networks in which layers of protocols are inoperable and fast responses to changes in network topology are essential to maintain important connections.
(5)	Security. Protection measures are required to prevent unauthorized access to information, preserve the integrity of data, and to mitigate against denial of service. [Note: Security includes access control, authentication, integrity, and confidentiality.]
(6)	Robustness (resilience) and quality of service. The range of quality of service parameters required for military systems exceeds that currently permitted within commercial OSI networks. In particular, in order to maximise the survivability of a network, the NATO aim is to maintain an adequate quality of service to the users (or at least to users operating above a given priority level) in the face of a severely damaged or partitioned network.
(7)	Precedence and preemption. In order to minimize congestion, particularly in a damaged network where resources are at a premium, it is desirable to be able to allocate resources on the basis of priority levels assigned to the connections being routed through the congested area. A facility is therefore required to associate a priority level with a connection when it is established.
(8)	Real-time and tactical communications. Certain applications are prepared to sacrifice such aspects of quality of service as sequencing and guaranteed delivery to achieve the minimum possible transit delay.

Source: *Use of OSI Standards in NATO--Strategic and Technical Issues*, Issue 2, TSGCE SG9, March 1988, NATO RESTRICTED.

A top-level view of how the eight military features identified above could potentially affect the layers of the OSI Reference Model is provided in Table 32. The entries in the table are based on the most recent editions of the draft OSI STANAGs (see Section 15.4).

---

[53] As indicated in Section 4.2.1, work in ISO on MPDT has been suspended in SC21/WG1. The completed work is planned to be released as a Technical Report. Canada is serving as the point of contact within SG/9 for maintaining interest in MPDT in ISO. Canada has introduced a draft proposal in ISO on Multi-Party Communications that would address MPDT.

Table 32. Impact of Military Features on Layers of OSI Reference Model

Military Feature	OSI Layer						
	1	2	3	4	5	6	7
1. Multihomed, Mobile Host Systems			TBD				X
2. Multi-Endpoint Connection			X			TBD	X
3. Internetworking			TBD				
4. Network/System Management Functions	TBD	TBD	TBD	TBD			X
5. Security	X		X			TBD	X
6. Robustness and Quality of Service	TBD		X	TBD		TBD	TBD
7. Precedence and Preemption			X	TBD			X
8. Real-Time and Tactical Communications			TBD	TBD		TBD	TBD

Key: X = A deficiency has been identified in the applicable draft STANAG; TBD = "to be determined"; and blank = "not applicable."

Sources: *Use of OSI Standards in NATO-Strategic and Technical Issues*, Annex 6, *Summary of Impact of Military Feature on Layers of Reference Model*, TSGCE SG9, 1 March 1988, NATO UNCLASSIFIED; *Commentaries on the STANAGs of WG1*, Contribution by France to TSGCE SG9/WG1, February 1989, NATO UNCLASSIFIED; the *NATO OSI Security Architecture (NOSA)*, March 1988, NATO UNCLASSIFIED; and recently released draft OSI STANAGs (through December 1991).

TSGCE SG9 is currently evaluating a proposed revised specification [Ref. TSGCE 1990d] of eight military features, in which Robustness and Quality of Service is replaced by Quality of Service, and Real-Time and Tactical Communications is replaced by Real-Time Communications. Table 33 provides the new definitions of these features, showing in italics the changes in wording from the current definitions (in effect since 1984). [Ref. TSGCE 1991a]

Table 33. Proposed Revised Military Features

(1)	Multihomed and mobile host systems. Multihoming is a mechanism for attaching an end system to two or more *nodes of a network* without the need for a system setting up a call to it to be aware of the extra connectivity. In addition to enhancing survivability, this facility may be extended to support "mobile hosts," such as aircraft, ships, *and land vehicles, during moves from one node to another.*
(2)	Multi-endpoint connections [multi-addressing]. In order to transmit *the same* data to a number of recipients (a common occurrence in signal handling), it is usually necessary to establish several connections and send separate copies of the data across each connection in turn. More efficient use is made of the communications resources (in particular improved performance in terms of minimizing delay and conservation of bandwidth) if the sender has to transmit only one copy of the data. The network then takes care of routing, control, and distribution of the data. *Some networks behave this way naturally (e.g., IEEE 802.3, net radio, and broadcast satellites).*
(3)	Internetworking. Mechanisms are required to facilitate the interconnection of various NATO systems at the boundary point between subnetworks.
(4)	Network/system management. Management functions are required that may be of greater sophistication than those considered satisfactory for civilian networks. *Examples are:* management of broken networks in which layers of protocols are inoperable; fast responses to changes in network topology essential to maintain important connections; *and counterattack management, to recognise and counter the effects of intelligent attack on and physical damage to the network.*
(5)	Security. Protection measures are required to prevent unauthorized *access to the system, to provide confidentiality of the information it carries, to* preserve integrity of data and to mitigate against denial of service. *Civilian standards are not always applicable. Secure military networks may require higher quality of service mechanisms and higher assurance levels than civilian networks.*
(6)	Quality of service. The range of quality of service parameters required for military systems exceeds those currently permitted within *civilian* OSI networks. In particular, in order to maximise the survivability of a network, the NATO aim is to maintain an adequate quality of service to the users (or at least to users operating above a given priority level) in the face of a severely damaged or partitioned network. *There is a perceived requirement for an ultimate delivery capability, whereby important communications are sustained, even at very low data rates.*
(7)	Precedence and preemption. In order to minimize congestion, particularly in a damaged network where resources are at a premium, it is desirable to be able to allocate resources on the basis of priority levels assigned to the *messages* being routed through the congested area. A facility is therefore required to associate a priority level with a *message. This requirement is needed for both connection-oriented and connectionless communications.*
(8)	Real-time communications. Certain applications *(often tactical in nature) require communications with specified time outs, which may vary in their range from milliseconds to seconds. Timeouts can affect packet and message sequencing; sequencing accuracy, however, remains essential and must be accomplished. Real time communications will also include high demands on sequencing accuracy.*

Source: *Use of OSI Standards in NATO--Strategic and Technical Issues,* Draft for Issue 4, Contribution by the UK to TSGCE SG9, 8 February 1991, NATO UNCLASSIFIED.

Note: Text shown in italics are amendments to the previous version shown in Table 31 (March 1988).

15.3 Organizational Responsibilities--TSGCE Subgroup 9

TSGCE SG9 has the primary responsibility in NATO for reviewing the military requirements, identifying the potential impact on the OSI standards planned for use in each of the seven layers of the ISO and NATO Reference Model, defining the deficiencies and services required to address these requirements at each layer, and developing draft STANAGs that conform to the Reference Model and provide for the needed services. SG9

has three permanent WGs, three new (proposed) WGs. and three ad hoc WGs (AHWGs) [Ref. TSGCE 1991b]:

- WG1 on OSI Layers 1-4, within which the work on functional profiles[54] is carried out by an AHWG on Functional Profiles. This AHWG is expected to disband in late 1992 or early 1993--its responsibilities will be taken up by WG5.
- WG2 on OSI Layers 5-7, within which the work on the Military Message Handling System (MMHS) is carried out by an AHWG on MMHS. The AHWG is expected to complete the MMHS profiles in 1993.
- WG3, responsible for establishing a memorandum of understanding (MOU) for a multinational program for Communications Systems Network Interoperability (CSNI)--not a permanent WG; work on the MOU is expected to be completed in December 1991, at which time WG3 would be disbanded.
- AHWG on OSI Management (AHWG-OM). The major work is on military managed objects, quality of service, management security, and security of management. When the AHWG-OM disbands (projected for April 1993), the work on military managed objects and quality of service will be taken up by WG6.
- AHWG on Integrated Services Digital Network (ISDN).
- AHWG on Security, responsible for providing security architecture/standards and guidance to other groups as agreed by the SG9 plenary.
- Project Group (PG) 9 on Multifunction Information Distribution System (MIDS) Low Volume Terminal (LVT)--not a permanent WG; PG/9 is expected to be disbanded once its MOU and a NATO Project Steering Committee are established, expected to be completed during the first half of 1992.
- WG4 on Data Links was established in 1991 to consider future data lines and datalink architectures.
- WG5 on Layer/Profile Standards; to be established in 1992. WG5 will be responsible for networking, with specific responsibility for transport and relay profiles. In order to produce a wider perspective on the emergent technologies and related standards that would be achieved by separate reporting lines, it has been proposed that the AHWG on ISDN report to SG9 through WG5.
- WG6 on Pan-Layer Issues (e.g., security, network management, quality of service, conformance, naming and addressing); to be established in 1992. WG6 will be responsible for application profiles.

At the present time, WG5 and WG6 have not been formed. These were introduced as part of the restructuring program developed in 1991 and to be approved in final form by the TSGCE in January 1992. Some time in 1992 (18 to 24 months after April 1991), WG1, WG2, AHWG on MMHS, AHWG on Functional Profiles, AHWG on Security,

---

[54] The AHWG on Functional Profiles has decided that the content and structure of a NATO functional profile should be based on ISO TR 10000. Review of this document shows that TSGCE SG9 intends to specify recommended standards for multiple layers at the interoperability parameter level.

AHWG on ISDN, and AHWG-OM will be phased out and replaced by WG4, WG5, and WG6 (WG3 and PG9 would be retained if necessary for liaison with CNSI and MIDS LVT development). Inauguration of WG5 and WG6 is planned for April 1992. Some work, such as the NATO Open Systems Interconnection Profiles (NOSIP; see Section 15.3.1.2), would be conducted by SG9 through workshops called as needed and an editorial group that meets in conjunction with SG9 plenary meetings.

TSGCE SG9 maintains liaison with many NATO bodies and agencies, including ADSIA, TSGCE SG11 (Tactical Communications), TSGCE PG6 (Tactical Communications Systems for the Land Combat Zone--Post 2000), NATO Industrial Advisory Group (NIAG) SG6 (Compatibility of Naval Data Handling Equipment), ATCCIS PWG, and Allied Tactical Communications Agency (ATCA). Liaison will be initiated with the newly formed TSGCE SG12 on Information Systems, together with its two subordinate groups: WG2 on Data Processing and Management and the AHWG on ATCCIS. (The work of SG11, PG6, and SG12 is discussed in Chapter 16.)

SG9 has become increasingly concerned that its terms of reference (TOR) [Ref. TSGCE 1985] are too broad in nature and that because of resource limitations within the Nations there is a need to formally restate the TOR to reflect the direction of the work SG9 considers most valuable and within its ability to undertake. The proposal developed by the Chairman of SG9 stated the mission [Ref.TSGCE 1990e]:

> To promote cooperation among NATO Nations in ensuring the technical interoperability of data processing and distribution systems used for command and control and in the development and procurement of related equipment and software.

Table 34 gives the specific actions for SG9 identified in the proposal (the proposed draft TOR was discussed at the 11-13 December 1990 meeting of SG9). In a briefing to SG9 in May 1990, the Chairman of SG9 proposed the following strategy for SG9 to carry out the actions of Table 34 [Ref. TSGCE 1990f]:

> In terms of the NIMP, which advocates the use of civilian communications standards (ISO/OSI) for C3 systems (augmented by military features as necessary), TSGCE is tasked to support this policy by undertaking the following:
>
> (1) In conjunction with appropriate NATO agencies, determine the range of standards needed by functional name, type, application area, and time required over a forward time frame of 5 years.
> (2) In light of the SG9 list of military features, determine their applicability to each identified need.
> (3) From (2) estimate the resources needed to produce the standard in terms of effort, skills, and time frame.
> (4) Clearly define SG9 contribution planned (e.g., no involvement, consultancy/review, guidance, or provision).
> (5) Develop policy on forms of support to be given (e.g., on Base STANAGs, profiles, or Parts of STANAG 4250).

(6) Make explicit statements of external work needed.
(7) Define major work items: define responsible 'agents,' time, resources, and expertise.

The following working documents and papers have recently been developed to refine the scope of TSGCE SG9 work on using OSI standards for NATO CCISs:

- *Use of OSI Standards in NATO--Strategic and Technical Issues,* May 1990 [Ref. TSGCE 1990d]
- *The TSGCE Subgroup 9 Support Programme for OSI in Military Communications,* June 1990 [Ref. TSGCE 1990g]
- *The Use of OSI in Military Communications,* June 1990 [Ref. TSGCE 1990h].

The foundation for an assessment of the progress in NATO for adapting to and, where necessary, defining military enhancements for OSI standards is a review of the activity and work plans of SG9. The activity for developing the *NTIS Transition Strategy* is discussed in Section 15.3.1. This is followed by a discussion of the current activity and work plans of the three WGs of SG9: WG1 in Section 15.3.2, WG2 in Section 15.3.3, and WG3 in Section 15.3.4. Status of the current work of the three SG9 AHWGs is discussed next: AHWG-OM in Section 15.3.5, AHWG-ISDN in Section 15.3.6, and AHWG-Security in Section 15.3.7. Because of the scope of its work, the current activity and work plan of WG2's AHWG-MMHS is discussed separately in Section 15.3.8.

Table 34. Proposed Revised Special Tasking Instructions for TSGCE SG9

Subgroup 9 is required to undertake the following specific tasks:

- Sponsor and develop a Single Architecture of NATO Technical Common Interface Standards (SANTIS) structured in compliance with the ISO Basic Reference Model for OSI and in accordance with the policy approved by the TSGCE at its meeting held from 13th to 15th December 1983. The architecture will be developed by using civil sector standards developed by ISO and related recommendations of CCITT, but with enhancements as necessary to provide military features.
- In the light of the approved policy and in consultation with ADSIA, review and support the development of the NIMP to include SANTIS.
- Give guidance to the [other] TSGCE subgroups to ensure that those data transmission standards related to Layers 1 to 3 of the NATO Model, which are the responsibility of those subgroups to develop, conform to SANTIS.
- Review existing communications STANAGs for suitability for the SANTIS and for interoperability with that architecture.
- Identify STANAGs under development that deviate from the Subgroup's policy and, where practicable, influence them to conform to SANTIS.
- In consultation with ADSIA, submit recommendations to the TSGCE on the role it should play in the formulation of test plans and procedures and in configuration management.
- Influence the further development of NATO digital data links to conform to SANTIS where desirable.
- Observe activities in appropriate research study groups of the Defence Research Group and make use of their results and recommendations in areas relevant to the work of the Subgroup.

15.3.1 NTIS Transition and NOSIP Strategy

15.3.1.1 NTIS Transition Strategy

A major project of TSGCE SG9, led by the German delegation, is the development and maintenance of the *NTIS Transition Strategy*. The current version is the 1991 or Sixth Edition; it is dated 11 November 1991 [Ref. NATO 1991] and was accepted by SG9 in December 1991. This document is revised biannually (by Germany) and promulgated by the CNAD. It provides recommendations for international commercial standards, primarily from ISO and CCITT, and intercept strategies (stacks of standards) that can be used by the nations as part of a transition strategy prior to the promulgation of OSI STANAGs. The *Intercept Profile for Military Message Handling Systems*, based on CCITT X.400-MHS(84) (see Section 15.3.8), was included in this edition. The Sixth Edition also incorporates ISDN standards and the 1988 recommendations of CCITT. The Sixth Edition includes use of the new ISO TR 10000 taxonomy for profiles. It describes 9 application, 21 transport, and 11 relay profiles. The *NTIS Transition Strategy* also addresses many of the deficiencies identified in the July 1989 release (Version 1.2) of WP 25, including RDA and TP. As noted in the August 1990 release (Version 2) of WP 25, the following emerging standards not addressed in the Fifth or Sixth Edition should be considered for the next edition of the *NTIS Transition Strategy:* ODP, TM, security protocols, X-Protocol (X-Windows), GKS, CGI, PHIGS, CGM, SQL, IRDS, and RPC. A summary of the standards and profiles contained in the Sixth Edition of the *NTIS Transition Strategy* is provided in Section 6.3.1, especially Figure 13. The profiles are illustrated in Appendix B.

15.3.1.2 NATO Open Systems Interconnection Profile (NOSIP)

In an ad hoc meeting on NOSIP held 25-27 September 1991, representatives from CA, FR, UK, US, STC, and NACISA considered the need for a GOSIP-like document for NATO (NOSIP is sometimes referred to as "NATO GOSIP," but it is not meant to be a set of OSI profiles). Agreement was reached on the need for such a document and its objectives: (1) to state NATO policy and provide a framework for development, management, and use of NATO Technical Interoperability Standards (NTIS) to achieve interoperability among NATO systems; and (2) to provide direction to assist in the procurement and acceptance of interoperable NATO systems. A proposed table of contents is developed that addressed the following topic areas (this was tabled at the SG9 plenary in December 1991) [Ref. Onufer 1991]:

- The NATO C3 Environment--the current C3 architecture and the eight military features.
- Architecture--the NATO Reference Model, the security architecture, the profile architecture, and various pan-layer issues such as naming, addressing, and management.

- NOSIP Standards--the hierarchy of standards, the concept of base standards and profiles, the guidelines for the development of profiles, the NATO profile taxonomy definition, and a directory of approved NATO standards.
- Transition Strategy--the concepts of interim and intercept standards and guidance for use of approved NATO standards.
- Procedural Issues--the procedures for naming and addressing, registration, testing, and configuration management.
- Procurement--the use of approved NATO standards for procurement and the guidance for procurement in the absence of approved NATO standards.

SG9 decided in December 1991 to develop a NOSIP Strategy document to define the range of available profiles, provide advice and guidance for procurement, and define the program of work to be undertaken by the SG9 community. Integrating the overall work plan into the NOSIP strategy reflects the view that producing and using profiles is "the best method of continuing to exploit civil sector standards." Further, such integration would make it easier to identify the work that needs to be done, the work that needs to be curtailed, and the agreed deadlines for completion. Following SG9 plenary agreement to the NOSIP Strategy document, SG9 intends that (1) no work will be permitted by its subordinate bodies that does not come within the GOSIP work program and (2) all tasking will be for fixed tasks with defined end dates--no open-ended tasking will be allowed. The goal is to provide tighter control of SG9 resources and give more effective output using less resources.

15.3.2 Status of Activities and Plans for Developing Lower Layer OSI STANAGs

The two primary tasks of SG9/WG1 are developing lower layer STANAGs (a complete set was tabled in SG9 in December 1991 with a recommendation they be considered for ratification) and developing guidelines for standardizing NATO functional profiles. The status of these activities is summarized below [Ref. Onufer 1991a].

In October 1991, WG1 agreed that the current layer STANAG approach to providing a framework for identifying civilian standards with enhancements for military use is outmoded. Layer standards are being submitted to SG9 in December 1991; WG1 believes that no further work should be conducted on these standards. The rationale is as follows [Ref. Onufer 1991b]:

- The development of civilian standards has proceeded using a subnetwork approach (e.g., LANs, ISDN) rather than a layer approach.
- Military enhancements to civilian standards that are not organized in a layered structure do not provide clear and unambiguous specification.
- The existing layer STANAG approach does not adequately discriminate among end system, intermediate system, and subnetwork issues.

- NOSIP (see Section 15.3.1.2) offers new opportunities to develop a more appropriate approach (e.g., providing a catalogue of approved service definitions, protocol, and profile standards that can be individually augmented with military enhancements.

As a consequence of this finding, WG1 recommends that WG1's work in the future be focused on: (1) developing NATO Standardized Profile (NSP) STANAGs with military enhancements required to fulfill NATO requirements; (2) creating a separate STANAG for each civilian standard that requires military enhancement; (3) providing a catalogue of such STANAGs, and of selected civilian and military standards, as part of the NOSIP document; and (4) establishing within the SG9 structure an ad hoc group dealing with an architecture for OSI internetworking and related subnetwork and Transport Layer issues.

15.3.2.1 Lower Layer STANAGs

WG1 has completed draft lower layer STANAGs (4251-54 and 4261-64) and provided these to SG9 to begin the ratification process. In some cases, conformance statements, and NATO PICS proforma were included. The draft STANAGs do not explicitly require Transport Protocol TP4 to support connectionless operations, but they do include the annex for Layer 3 (Annex E) on the connectionless Internet Protocol (IP). WG1 has determined [Ref. TSGCE 1989] that it is inappropriate for forward error coding (FEC) to be standardized with the OSI framework; therefore, WG1 has relegated FEC as actions to be accomplished on the information bit stream outside the Reference Model. Thus, FEC is not currently being considered in the lower layer STANAGs. The status and military features for the lower layer draft STANAGs is discussed in Sections 15.4.1 to 15.4.4.

15.3.2.2 Functional Profiles

A functional profile guidelines document is being developed as Part 6 of the NATO Reference Model (STANAG 4250); it is intended to be used to specify NSPs and is viewed in WG1 as the basis for the lowest common denominator of interoperability (the new direction of SG9 is to focus most future upper and lower layer work on profiles). The guidelines document is being developed in WG1; it is not clear whether it will be used by WG2. The guidelines document is based on ISO TR 10000 (Part 1--*Framework* and Part 2--*Taxonomy).* WG1 submitted the guidelines document to SG9 in December 1991. This draft has omitted the example profiles since these examples have now been prepared as draft STANAGs instead. At some time in the future, the NSP guidelines document could be moved into the NOSIP.

The NATO International Staff promulgated the *Configuration Management Procedures for NATO Technical Interoperability STANAGs,* which updates the TSGCE configuration management procedures in accordance with AAP-3 and reflects the new

TSGCE subordinate structure. This document identifies the guidelines document as STANAG 4260 (rather than STANAG 4250 Part 6).

15.3.2.3 NATO Standardized Profiles (NSPs)

Two groups of profiles have been developed. The first comprises TAnnnn(M), TA5n(M), and TA51(M), providing a complete profile for 10BASE2, 10BASE5, and 10BaseT CSMA/CD LANs. Additionally, a draft profile has been developed for an FDDI LAN. These will all be combined into a single multi-part draft STANAG whose scope would be all CO transport profiles using the CLNS [i.e., all TAnnnn(M) profiles]. The current drafts were provided to SG9 in December 1991 to be circulated to the Nations for comment.

A second group of NSPs being developed in WG1 are TC1111(M) and TC1121(M), which describe permanent access to a packet-switched data network using the COTS and the CONS. The current drafts of these NSPs were viewed as ready for ratification, but in October 1991 WG1 agreed to reformat them as a single multi-part STANAG for all CO transport profiles using the CONS [i.e., all TCnnnn(M) profiles]. In addition, the NSP protocol implementation conformance statement (PICS) requirements list (NPRL) will be restructured to be consistent with the recent JTC1/SC6 guidelines (the NSP PICS proforma pieces are to be removed).

15.3.2.4 NOSIP

Of particular interest to WG1 was the recommendation in October 1991 that NOSIP incorporate the NSP guidelines and provide for cataloging approved base standards. This led to agreement in WG1 that the layer STANAG approach for recording development of data communications base standards was no longer relevant. Detailed recommendations based on this conclusion were drafted and tabled at the December 1991 SG9 plenary (see earlier discussions of NOSIP in Sections 15.3.1.2 and 15.3.2).

15.3.2.5 Use of OSI in NATO

WG1 has been evaluating a proposal to change the emphasis of SG9 work on military features. The paper, *NATO Approach to OSI--A Review*, says that

> With the possible exception of the work on management however, the analysis of the current ISO position indicates that there is relatively little scope remaining for NATO to influence ISO to provide specific military features.[55] Therefore, we need to focus our work on the facilities that are

---

55 This view is not shared by all of TSGCE SG9; both the AHWG on Security and the AHWG on OSI Management are continuing to work to influence ISO to provide military features. In security, work is continuing to make the TCS conform to the eventual security protocol agreed by ISO--only the implementation would be unique to NATO.

now present and examine how they should be adapted for use. ...there is a need now to develop augmentations to the civil standards.

WG1 agreed that work should be done to adapt present facilities for military use, but that many aspects of the identified military features cannot be satisfied by the present facilities and that additions must be made to the current protocol standards. WG1 further agreed that it is desirable to amend the civilian OSI standards under development to incorporate military features if that it is possible. Finally, WG1 agreed that this represents a shift in emphasis in the WG1 work, but not to the exclusion of having NATO-approved positions presented to ISO.

15.3.2.6 Multipeer Data Transmission (MPDT)

Work is progressing in the US Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) for multicasting. DTMP/WG1 on Lower Layers plans to develop a report on how the US GOSIP would accommodate a combat net radio (CNR) profile. Canada was unsuccessful in its efforts to keep MPDT alive in ISO (the architectural work on MPDT was suspended by SC21/WG1). The US has proposed new work on MPDT to SC21/WG1. Canada has agreed to coordinate this and other NATO-Nation input with ISO.

WG1 has considered national contributions on MPDT. WG1 does not oppose reactivation of MPDT in principle. Before considering reactivation, however, WG1 will require major technical contributions explaining how the generic application requirements can be met, whether a general solution (rather than modifying individual layer protocols) is necessary, and whether the current MPDT document--SC21 N 3287--is a suitable basis for further progression [SC21 N 6197, *WG1 Position on the Reactivation of Project 1.21.9.1 (Multi-Peer Data Transmission)*, WG1, July 1991].

Examples of applications requiring MPDT are [Ref. TSGCE 1991c]:

- Distributed interactive simulation
- Advanced air traffic control
- Distributed processing
- Financial newswire
- Broadcast information dissemination
- Distributed management information services
- Military applications
- Manufacturing automation, robotics, and process control
- Video and data teleconferencing
- Interactive fora.

The US has developed (and submitted to WG1 in its September-October 1991 meeting) the specification [Ref. Harris 1991] of a military supplement to the CLNP to

address requirements for performance and efficiency by supporting best-effort multicasting and network management services. The extension to ISO 8473 is intended to be used by an upper layer protocol implemented in a military-augmented transport protocol.[Ref. Swanson 1991], [Ref. SPARTA 1991]. The multicasting service is designed to provide more efficient transmission of identical data to two or more destinations, primarily conserving network bandwidth and possibly reducing delays in transmission.

ANSI in support of the CCITT SGVII has developed an X.25 Packet Multicast Service Definition (X.PMS) intended to be used by any application that involves two or more end systems. General applications may involve any need to transmit data simultaneously to many recipients where messages, operational status, and process data must be disseminated. X.PMS is a "one in, many out" message service, directly linked to MPDT. X.PMS involves individual recipients, closed and open groups, and dynamic entry into groups. The initial foundations are being laid to define and articulate the breadth and depth of this protocol in the CCITT committees. [Ref. Pant 1991]

15.3.2.7 Multihoming

In May 1991, the UK reported to WG1 that it had approached appropriate ISO bodies to determine the desirability of submitting multihoming features incorporated into the Layer 3 STANAGs. It was determined that ISO had considered multihoming several years ago for the Network Layer and that it had been relegated as a Network Layer issue. There is no current interest in ISO for developing routing protocols for Layer 4. Instead, the CLNP routing support protocols are being used.

Protocol enhancements for multi-homing developed in WG1 are cited in the UK paper as conflicting with the ongoing ISO work on Network Layer routing and management, and the UK recommended that the proposals of the transport STANAGs be reconsidered and not put forward to ISO. Mechanisms are being defined within the Network Layer that are capable of supporting multihoming. The importance of TP4 is re-emphasized, even for its use with CONS. In order to take advantage of Network Layer and other mechanisms, there is a "need for software interface (API) standards to support modular and configurable lower layer products so that NATO enhancements can be implemented cost-effectively for end-systems." [Ref. TSGCE 1991d]

15.3.2.8 Multiendpoint Connection

WG1 noted in May 1991 that the multiendpoint connection feature would be better stated as "multiendpoint communications," since connections cannot be provided over a broadcast-type media (e.g., LANs or radio).

15.3.2.9 Mobile Hosts

WG1 noted a briefing by the UK (Tony Whyman) in May 1991 on the applicability of the ISO 10589 routing information exchange protocol and how it may be used to support

mobile hosts. The potential inefficiencies of ISO 10589 over low-bandwidth networks were analyzed, options for improvement presented, and the use of the proposed ISO interdomain routing information exchange protocol investigated. It was concluded by the presenter that routing information exchange protocol is the "most appropriate" protocol on which to base support for mobile hosts and subnetworks.

15.3.2.10 Lower Layer Addressing

WG1 has been reviewing a number of technical papers on lower layer addressing. These include the EWOS *Technical Guide to OSI Layer 1 Through 4 Addressing* and a draft British Standards Institute guide for *The UK Scheme for the Allocation of ISO-DCC Format OSI Network Service Access Point (NSAP) Addresses*, which was used in the EWOS document as a reference for addressing in Layer 3. The US has submitted papers on naming and addressing and on the compatibility of STANAG 4214 and US GOSIP Network Layer addressing. The UK has developed a rationale for Annex D of draft STANAG 4263 with the goal of resolving differences with STC in an addressing scheme.

15.3.2.11 Precedence and Preemption

Since ISO restricts the Transport Layer levels of precedence to 15 by restricting use of one of the levels, WG1 agreed to reduce from 16 to 15 the number of levels of precedence that would be adequate at the Transport Layer.

15.3.2.12 Real-Time Programs

WG1 has specific proposals for incorporating real-time aspects into the Layer 4 STANAGs. There are issues regarding these real-time services as to their conformance to OSI, differences from CCITT real-time work, and the interest of several nations in other efforts [e.g., US Manufacturing Automation Protocol (MAP) real-time work] as closer to OSI.

15.3.2.13 Glossary of NATO Data Communication Terms

WG1 has developed a *Glossary for OSI Layers 1 Through 4*. Further contributions were provided by STC (*SG9-SG1 Definition of Terms, Initial Draft*) and Canada (*Proposed Definitions of Military Features*) in October 1991. WG1 is recommending to SG9 that SG9 coordinate a glossary for all OSI layers.

15.3.2.14 Liaison With Other Groups

Parts of the *NATO Consultation, Command and Control (C3) Master Plan* developed by NACISA have been forwarded to the Military Committee; none has yet been approved. The *NATO C3 Architecture* is still being worked on; in particular, Volume 1 (*Consolidated Architecture*) has not been accepted (see Section 11.1). STC has an ongoing program to implement X.25 for an investigation of preemption functionality. US/EUROCOM wishes to use STANAGs 4262 and 4263 for the revised STANAG 4269

on the tactical digital gateway but reported in 1990 that the layer STANAGs were not considered stable enough. WG1 has noted that the gateway standard would appropriately be a profile of SG9 lower layer standards, probably a relay profile. WG1 has responsibility for access to ISDN and plans on developing profiles for use of ISDN as a bearer service. In October 1991, WG2 considered an in-depth briefing from the AHWG-OM (Jeremy Tucker), which suggested the efforts needed by WG1 to define (military) managed objects for the lower layers.

15.3.2.15 Work Plan

TSGCE SG9/WG1 has an 18-month work plan (June 1991 to December 1992) that contains the work areas and planned activities on lower layer STANAGs and profiles as shown in Table 35 (the work on layer STANAGs and the NSP guidelines document was completed in October 1991) [Ref. TSGCE 1989a, TSGCE 1989b]. The focus of the work plan is on preparation of products that could be completed by the end of 1992. Items beyond that scope were directed to the new terms of reference and work plan for WG5 [Ref. Onufer 1991c], [Ref. Onufer 1991d].

Table 35. Work Plan and Activities on Lower Layer STANAGs by WG1

(1)	Revise and submit the NSP Guidelines to SG/9 as STANAG 4250 Part 6 in December 1991, together with an example single-part NSP [TC1111(M)] and an example multi-part NSP [TA5n(M)], with a recommendation for inclusion in STANAG 4250.
(2)	Prepare TC1111(M) and TC1121(M) profiles as NSP STANAGs and submit them to SG/9 by December 1991, recommending ratification.
(3)	Prepare TA5n(M) and TA51(M) profiles as a multi-part NSP STANAG and submit them to SG/9 by May 1992, recommending ratification.
(4)	Complete development of the annexes for lower layer STANAGs necessary to incorporate the military features required to support the four above-mentioned profiles and provide the lower layer STANAGs with these annexes to SG/9 by December 1991, recommending that they be accepted as base standards for the profiles.
(5)	Develop a profile based on CCITT X.75 to support on-going work in US-EUROCOM.
(6)	Develop and architecture for the NATO Internet
(7)	Develop profiles to support internetworking
(8)	Investigate the interface to ISDN.

Sources: *NATO SG9 WG1 18-Month Work Plan*, TSGCE SG9 WG1, 27 June 1991, NATO UNCLASSIFIED; *Chairman's Report of the June 1991 AHFP Meeting*, 18 September 1991, NATO UNCLASSIFIED.

15.3.3 Status of Activities and Plans for Developing Upper-Layer OSI STANAGs

The status of WG2 activities (as of October 1991) is summarized in the following paragraphs [Ref. TSGCE 1989c, TSGCE 1990i] [*Report of the TSGCE SG9/WG2 Meeting of 30 September to 4 October 1991*, US Representative to WG2 (LCdr Katie Bryant), October 1991, NATO UNCLASSIFIED].

15.3.3.1 Proposed SG/9 Restructuring

SG9/WG2 noted that the work of SG9 (other than data links) fell into three areas: transport profiles, application profiles, and pan-layer issues. WG2 concerns were that it might be unmanageable to do all the profile work in one group (WG5) or pan-layer work in one group (WG6) and that the new structure might be less efficient and require more national staffing.

15.3.3.2 Naming and Addressing

WG2 reviewed a proposed draft STANAG 4250 Part 3 on Naming and Addressing and recommended that it be brought to the December 1991 SG9 plenary for ratification.

15.3.3.3 MMHS STANAG 4406

Revised drafts of the rationale, base standard, and two interoperability profiles have been produced. A draft STANAG (4406) has been prepared. It contains the Military Base Standard and the Alpha Profile Set (for strategic and medium-bandwidth tactical usage) and is ready to take to SG9 for distribution and initiation of the ratification process (see Section 15.3.8). MMHS(84) gateways, directories, protocol implementation conformance statements (PICS), and management requirements still need to be considered. Subsequent submissions will add a Beta (limited bandwidth) Profile Set and gateway specifications. The ratification clause has been amended to allow ratifying nations to specify whether their national system would be procured according to the STANAG (optional for ratification) or whether MMHS compatibility would merely be provided at national boundaries (mandatory for ratification). This two-part clause will allow nations such as the US to ratify the STANAG even though they will implement internal national systems (e.g., Defense Message System) that will not exactly follow the STANAG (such as in the use of Message Security Protocol) as long as they meet the STANAG specifications (e.g., in gateways) at national boundaries.

15.3.3.4 FTAM

WG2 held a one-time meeting on FTAM in June 1990 in order to develop: a statement on the current status of FTAM (including profiles and products); a requirements document outlining requirements for file transfer; determination of base standard and profile enhancements; and a work plan. NACISA has undertaken work in this area in attempting to meet a requirement identified by the UK to transfer large unstructured files. Civilian profiles lack security features to support this requirement. NACISA completed a set of FTAM profiles for use over the STAMINA transport profile that are aligned with the FTAM International Standardized Profile. WG2 will develop a liaison statement to the ISO FTAM Rapporteur and encourage nations to support the work through their national bodies. A draft status report on FTAM (with particular reference to security mechanisms) is planned for September 1992. At some time in the future, it is expected that there will be

a need for WG2 to commence work on drafting an FTAM STANAG or a STANAG to provide for a file transfer capability.

15.3.3.5 Registration

WG2 was active in developing recommendations that led to NATO being designated as a registration authority. WG2 is developing a five-part paper (first draft submitted by STC) for identifying NATO Registration Procedures. WG2 is active in two parts: NATO Registration Authority (Part 1) and Registration of Object Identifier Component Values (Part 2). Other elements of SG9 have been requested to look at the other three parts: Registration of MHS and MMHS Management Domains, Registration of Network Service Access Point (NSAP) Addresses, and Registration of Directory Names.

15.3.3.6 Impacts of NATO GOSIP

WG2 reviewed the SG9 document, Defence Open Systems Interconnection Profile--A Programme for the Creation of a NATO "GOSIP" Standards Base. WG2 supported the concept of a NATO GOSIP and agreed that such a document would provide a suitable forum (that is currently lacking) for the placement of text and recommendations on the overall structure of the NATO Intercept Profile and current and future STANAGs.

15.3.3.7 Upper Layer Security

WG2 has identified a number of areas related to security for which information from the AHWG on Security is required: current NATO documentation on OSI security, including architectural issues and interactions between lower and upper layer security functionality; the role of the Security Application Service Elements; security functionality within applications; and relative roles of WG2 and the AHWG on Security in upper layer security issues.

15.3.3.8 ISDN

WG2 determined that its upper layer work is not affected by ISDN and agreed to continue liaison with the AHWG on ISDN to ensure any future issues are not overlooked.

15.3.3.9 Program of Work

SG9/WG2 has developed a 12-month work plan. Current high priority tasks are the MMHS STANAG, naming and addressing, the NATO "GOSIP" proposal, and upper layer security. The medium priority tasks are FTAM, Directories, and multipeer data transmission (MPDT). Low priority items are conformance testing and functional profiles. No work is currently planned on connectionless-mode communications. A summary of the elements of this plan is provided in Table 36 (the topics are alphabetical) [Ref. TSGCE 1991e].

Table 36. Work Plan and Activities on Upper-Layer STANAGs by WG2

(1) Abstract Syntax Notations. Develop STANAGs covering the use of abstract syntax notations (e.g., ASN.1) and their encoding rules. Ratification of STANAGs 4258 and 4259 without military extensions has been recommended to SG9. WG2 will attempt to identify requirements for military extensions. Areas of analysis have been the use of ASN.1 versus NATO Message Text Formatting System (FORMETS), encryption, and compressed encodings. **Work completed October 1991.**

(2) Application Layer STANAG Format. Develop a STANAG format to deal with Application Layer service and protocol specifications; this format (completed in March 1988) will form the basis for the development of separate service/protocol STANAGs such as for ACSE, FTAM, MHS, and Remote Data Access (RDA). This format will accommodate functional profiles. Functional profiles for an application will be ratified separately and included as annexes to the base STANAG for that application. **Work completed October 1991.**

(3) Conformance Testing. Establish a framework and methodology for testing the conformance of protocol implementations of a particular standard. WG2 initiated the 3-day one-time SG9 meeting on conformance testing held in December 1991. **Low priority.**

(4) Connectionless-Mode Data Transfer. Adopt or develop standards to support connectionless-mode service at both upper and lower layers of the reference model. ISO standards now exist for both the lower and upper layer connectionless-mode protocols. In the upper layers, standards have been approved for connectionless-mode Session, Presentation, and ACSE protocols (see Figure 13 in Chapter 6). **No current work.**

(5) Directory Services. Determine military requirements for directory services in NATO communication systems and evaluate the suitability of the ISO Directory standards to support these requirements. Develop an Application Layer STANAG for Directory services with possible extensions to the civil standards. An ad hoc meeting was held in June 1988 to assess the impact of Directory standards on military communications networks. Further discussion is required but not currently scheduled. **Medium priority.**

(6) FTAM. Determine military requirements for FTAM in NATO communications systems and evaluate the suitability of the ISO FTAM standard to support these requirements. Develop an Application Layer STANAG for the use of FTAM with possible enhancements or modifications to support military requirements. The ad hoc one-time SG9 meeting on FTAM in June 1990 identified some national requirements for file transfer but did not determine complete military requirements. WG2 has agreed to adopt the FTAM International Standardized Profile (ISP) as a Transition Strategy intercept standard. **Medium priority.**

(7) Functional Profiles. Determine how functional profiles will be employed in NATO. The specification and use of NATO functional profiles "should be aligned with SPAG, CEN/CENELEC, and EWOS." Develop a ratification process and STANAG format for NATO profiles. A 1988 proposal has been modified and accept by WG2 for upper layer STANAG structure. Application Layer base STANAGs will have separately ratifiable annex for profiles. WG1 is drafting guidelines for NATO Standardized Profiles based on ISO TR 10000. The AHWG on MMHS has completed an Alpha profile (see Section 15.3.8) based on specifying changes to EWOS X.400 profiles. This item is inactive pending further developments in civil profiling. **Priority to be decided.**

(8) ISDN Upper Layer Issues. Determine the implications of ISDN for the OSI upper layers. The AHWG on ISDN has addressed OSI-to-ISDN address mapping and teleservice profiles. No further activity is anticipated on direct ISDN issues. **No current work; completion expected in March 1992.**

(9) Military Features. Comment on the specification of military requirements to reflect the current features of the civil international standards. Further consideration of military features will be within the framework of the NATO "GOSIP." **No current work; completion expected in March 1992.**

(10) MMHS STANAG Review. Review the output documents from the AHWG on MMHS (see Section 15.3.8) and prepare recommendations regarding their suitability for ratification. Suitable STANAGs (e.g., STANAG 4406 with two separately ratifiable annexes) will be referred to SG9. **High priority.**

(11) Multipeer Data Transmission (MPDT). Determine military requirements for MPDT and assess the suitability of international standards to meet these requirements. Intermittent activity, but no resolution for further action. ISO initiated a project on this topic but suspended it due to lack of support. Canadian contributions to ISO/IEC JTC1/SC21 in May 1990 failed to re-establish a work item, and this status will remain for the foreseeable future. NATO must therefore specify its own extensions to existing civil standards to met its requirements. This pan-layer issue may require changes to upper layer STANAGs. In the short term, WG2 has agreed to pursue the development of specific application profiles as a means to identify requirements for general extensions to upper lay STANAGs. **Medium priority.**

Table 36. (Continued)

(12) Naming and Addressing. Define a NATO-wide scheme for the naming and addressing of layer entities, with particular emphasis on the Application Layer. Examine the need for a registration authority within NATO to ensure globally unique names and addresses. WG2 made the recommendations that lead to NATO seeking and being designated as a Registration Authority for International Code Designator (ICD) "0026" by the British Standards Institute under the auspices of ISO 6523. **High priority.**

(13) NATO "GOSIP". Determine the implications of the "NATO GOSIP" (see Chapter 14) and identify any functional requirements based on the OSI upper layers. The objective of this activity is to coordinate the WG2 view of the upper layer architecture (e.g, MMHS, CASE) with the development of the NATO "GOSIP." WG2 has agreed that a NATO "GOSIP" would serve as a valuable "umbrella" that could provide a more appropriate vehicle for a number of topics which are not suitable for STANAGs. **High priority.**

(14) Presentation Layer STANAGs. Develop STANAGs to encompass the OSI Presentation Payer services and protocol specifications (ASN.1 is being addressed as a separate STANAG). Ratification of STANAGs 4256 and 4266 without military extensions has been recommended to SG9. The WG2 questionnaire did not identify requirements for military extensions in the short term. **Work completed October 1991.**

(15) Real-Time Performance. Determine military requirements for real-time performance and its implications on quality of service. A multi-part study, Real-Time Aspects for NATO Technical Interoperability Standards, was completed in October 1990. No activity other than a presentation in October 1989. **Work completed October 1991.**

(16) Session Layer STANAGs. Develop STANAGs that encompass the OSI Session Layer service and protocol. Ratification of STANAGs 4255 and 4265 without military extensions has been recommended to SG9. The WG2 questionnaire did not identify requirements for military extensions in the short term. **Work completed October 1991.**

(17) Upper Layer Security. Determine functional requirements for NATO systems. Potential deficiencies have been identified in the upper layer STANAGs currently out for ratification, but no specific enhancements have been identified. WG2 has decided to become active in upper layer security due to "lack of expertise in the AHWG on Security and its consequent reluctance to address upper layer issues." WG2 will attempt to identify NATO functional requirements and specify suitable mechanisms in the upper layers. **High priority.**

(18) User Requirement Definition. Conducted a questionnaire to survey user requirements for Session and Presentation Layer deficiencies identified in the September 1988 Canadian analysis. Questionnaire was revised and circulated to Nations in May 1989. No requirements for specific changes in upper layers were identified. A recommendation to pursue specific application profiles (FTAM in the near term) was noted. **Work completed October 1991.**

Source: *NATO TSGCE SG9 WG2 Work Plan*, TSGCE SG9 WG2, 31 October 1991, NATO UNCLASSIFIED.

15.3.3.10 Quality of Service

WG2 has considered QoS issues and reviewed a WG1 liaison statement regarding precedence and preemption transport service additions.

15.3.3.11 Conformance Testing

WG2 participated in the 3-day SG9 workshop on conformance testing held at STC in December 1991. This meeting was the first step in a study to progress the understanding of the requirements for testing military extended OSI protocols and to recommend means of testing OSI-based implementations within NATO. The meeting objectives were to [Ref. Rannestad 1991]:

- Discuss national testing programs in both civil and military communities
- Exchange testing experience from current testing programs

- Present proposals for possible collaborative effort in the testing area
- Discuss proposals for possible joint work or information sharing
- Agree on short-term proposals for joint work or information sharing
- Discuss possible ways of feeding national and collaborative study results back into NATO.

One suggestion from WG2 was that multi-nation interoperability testing of X.400 and prototype MMHS implementations be a primary focus early OSI testing. Such a focus might attract national participation. The initial step would be to agree on a functional profile to test, an associated test suite, and an interoperability test plan and timetable.

15.3.4 Nunn Initiatives and Work Plan of WG3

An Ad Hoc Group on Nunn Initiatives was formed by TSGCE SG9 in March 1988 to progress three projects as multinational cooperative efforts. In part, these proposals were aimed to satisfy a request from ADSIAto TSGCE to investigate the feasibility of a transmission-media-independent data link architecture; such an architecture and the associated technical standards are needed to support stated requirements of the Air Command and Control System (ACCS, see Section 11.3). The three original proposals were to:

- Develop, test, and implement techniques for Communications System/Network Interoperability (CSNI)
- Develop an architecture for future data links based on the NATO Reference Model
- Produce draft STANAGs for the products produced in the other two projects.

NATO funds for the last two proposals have not been found.[56] Section 15.3.9 discusses the work of SG9/WG4 on Data Links.

15.3.4.1 WG3 on Communications System/Network Interoperability (CSNI)

SG9/WG3 was formed in October 1989 to develop an MOU under a Nunn Initiative for CSNI. Canada, France, Germany, The Netherlands, the United Kingdom, and the United States have signed the MOU for participation; NACISA and STC have also expressed close interest in the work and STC will be invited to participate in the CSNI demonstration. WG3 tasking ends with a completed MOU among the participating nations, but the CSNI project itself will take about 3 years. The emphasis of this 3-year effort is not on developing standards but rather to demonstrate the operational utility of internetworking using enhanced OSI profiles with military features, specifically demonstration and

---

[56] US DoD support for the second and third items was not provided, apparently due to lack of funds.

evaluation of multi-media communications extending from the West Coast of the United States to the center of the European continent. [Ref. Rigden 1991]

The CSNI project plans a demonstration in 1994 for linking subnetworks of countries across long haul multimedia networks supporting multiple modes (voice, data, images). Use of HF ground-wave and sky-wave, VHF, UHF line of sight, UHF SATCOM, SHF SATCOM, and land lines is planned. According to the MOU [Ref. TSGCE 1990j], WG3 will (1) ensure that the work will be closely related to the recommendations, standards, and draft STANAGs of all groups under SG9; (2) provide both feedback into the STANAG development process and practical experience on the implementation of OSI protocols on military bearer systems; (3) provide reports on the demonstration results and performance to SG9; and (4) based on demonstration results, recommend to SG9 the adoption of promising system concepts for different operational applications. An outline of the work areas being considered for the CSNI statement of work is given in Table 37.

In 1992 and beyond, the project responsibility will reside in the CSNI Steering Committee and its subordinate body, the Technical Coordination Group (TCG). The TCG, meeting approximately bimonthly starting in February 1992, will develop detailed project plans. A software development strategy was drafted in November 1991 and is under review by the TCG. A work breakdown structure has been drafted and will be completed by the TCG. These and other documents of CSNI will be marked "in confidence" and distribution limited to participating nations unless specifically approved by the CSNI Steering Committee [Ref. Gee 1991]. The project will start three months after the MOU has been signed by all participating nations. (Completion of the MOU was expected in December 1991 in conjunction with the CNAD meeting.)

Table 37. Proposed Work Areas for CSNI in WG3

1.	System Concepts and Testing
	a. System demonstration architecture
	b. Testing program
2.	Applications and Services
	a. Database exchange
	b. Security
	c. Voice
	d. Messaging
3.	Multinetwork Management and Protocols
	a. Multimedia routing
	b. Enhanced OSI protocols
4.	Communications Media and Systems
	a. Long haul HF
	b. Satellite communications (SATCOM) SHF
	c. SATCOM UHF
	d. VHF
	e. UHF LOS
	f. EF ELOS
	g. EUROCOM
	h. ISDN/GSM.

Source: *Proposed Terms of Reference for WG3*, TSGCE SG9 WG3, October 1991, NATO UNCLASSIFIED.

15.3.4.2 Media-Independent Data Link Architecture (MIDLA)

MIDLA was suggested to TSGCE by ADSIAin 1986 [Ref. ADSIA1986]. During the period 1987-1989, the Nations attempted to identify Nunn Initiative funding for MIDLA, but these efforts were unsuccessful. At the October 1989 SG9 plenary meeting [Ref. TSGCE 1989], the Nations agreed that development of a data link architecture based on the OSI Reference Model to replace antiquated data links was extremely important. However, it was also agreed that resources were not available within SG9 to address the breadth, complexity, and technical aspects of that subject. SG9 agreed to send a letter to TSGCE stating the importance and magnitude of this project. In addition, the Nations were asked to assess again the availability of resources relative to the MIDLA project.

MIDLA is one of the topics suggested for discussion in the newly created WG4 on Data Links. However, it is not an item of current interest to that group (see Section 15.3.9). A bilateral agreement has been established between France and the United Kingdom regarding future data link architectures. At the September 1991 meeting of WG4, France indicated that MIDLA development has not progressed sufficiently for it to be brought into the SG9 forum.[57]

Further, ADSIAhas received an STC study, *An Architecture Based on OSI Principles for NATO Tactical Data Links* [Ref.SHAPE 1989], and has indicated to TSGCE SG9 that no further work on behalf of ADSIAis required for MIDLA [Ref. ADSIA1990].

---

[57] *Report of the US Representative (Capt D. G. Ahern) to WG4*, June 1991, UNCLASSIFIED.

However, tactical data link architecture is being addressed by the TSGCE AHWG on Restructuring as a potential area of work. SG9 has indicated that if the SG9 terms of reference are amended to include tactical links, guidance from the TSGCE would be required on providing necessary resources [Refs. TSGCE 1990k, TSGCE 1990b].

15.3.5 Status of Activities and Plans for Developing Network Management Standards

AHWG-OM. The lead for NATO initiatives on network management is the AHWG-OM, which addresses such pan-layer areas as fault management (detection, isolation, and correction of abnormal operation); configuration management (exercise control over identities and collect data from and provide data to managed objects in order to assist in providing continuous operation of interconnection services); security management (enable the management of the information necessary for providing security services); accounting management (enable charges to be established, and costs to be identified, for the use of managed objects); and performance management (evaluate the behavior of managed objects and the effectiveness of communication activities). Specifically, the AHWG-OM was established to:

- Define the requirements for management in a military OSI environment.
- Investigate the influence of the military features (see Section 15.2) on the OSI management standards under development by ISO. The AHWG-OM has determined that the eight military features will affect, to varying degrees, all management areas.
- Influence ISO, and other standards bodies as appropriate, to adopt any additional military features identified.
- Develop any additional military management standards for the requirements not met by ISO.
- Assist in the coordination of management work within NATO and provide support for OSI management to SG9 and its working and ad hoc groups.

The work of the AHWG-OM has been focused on influencing ISO work; in addition, work has begun on a draft STANAG covering OSI management. Many members of the AHWG-OM are also members of ISO committees, and the AHWG-OM believes its work is recognized by ISO in SC21/WG4 as a major contribution of the development of standards [Ref. TSGCE 1990c].

Network Standards. Many of the ISO network standards have been reorganized and now appear to have a stable framework in ISO (see Section 8.2.3). A new set of functions has been developed, and the model of management information has been significantly modified. The Common Management Information Service (CMIS) and Protocol (CMIP) are now International Standards (ISO 9595 and 9596).

The AHWG-OM has noted that little military influence has yet been brought to bear on Security Management, for which work is progressing very slowly in ISO. The

responses to a requirements questionnaire distributed in June 1989 indicated that almost all network management practices were manual and procedurally oriented and were not relevant to what ISO is trying to standardize in Network Management. However, the results of the questionnaire confirmed the earlier military analysis document in the Working Document *NATO Requirements for OSI Management* (an evolving record/base document of the AHWG on OSI Management results) [Ref. TSGCE 1988]. Enhancements to this document--specifically in Section 7, "Military Features and Their Impact on OSI Management"--arising from the questionnaire were adding the needs (1) for a broadcast facility, (2) for a capability to apply management in real time, (3) to define and work across management domains, (4) to define access control mechanisms for management information, and (5) to provide for survivability of management information (replication mechanisms). Requirements for performance management, event reporting, and management negotiation were dropped [Ref. TSGCE 1990l].

Quality of Service (QoS). In the February 1990 AHWG-OM meeting a formal contribution, addressed from individual nations to ISO, was drafted requesting adoption of Quality of Service (QoS) as a new work item by SC21/WG1, in response to Question Q62 on QoS. The nations are currently balloting the new work item, with the deadline of 6 December 1991. The UK is supporting the work and offering to serve as project editor. Australia, Canada, France, and the US have previously expressed support (the minimum number of ISO nations required to begin new work is five).

An example of the kind of work that requires QoS support is the Time Critical Communications Architecture (TCCA) being developed in ISO. The ISO group has identified a class of networks that carries both bulk data transfers and time-critical messages and that operates over large distances in a possible hostile environment. Communications is considered in this context as time critical if the application process sending a message requires it to be received within a certain time after it submits its send request to the system.

In October 1991, TSGCE SG9 held an ad hoc meeting on QoS to review past QoS papers and the status of QoS in ISO and to develop the approach SG9 should take on this subject. NACISA promoted the adoption of CCITT X.140 as a model to use when mapping user-perceived QoS parameters to network performance attributes as viewed by the providers of data transmission services. Parameters such as quality, availability, and survivability were discussed as examples used to describe military attributes. The participants of the meeting agreed that for a QoS parameter to be meaningful it has to be observable and measurable. However, for certain security services such as non-disclosure, one may not be able to measure the parameter. One issue discussed but not resolved was whether security was a QoS parameter; regardless of the final outcome, there was agreement that security would impact other user-level QoS parameters (e.g., delay, throughput). During work in two special working groups, the participants generally agreed that [Ref. Ahern 1991]:

- Statements of user requirements and definitions of QoS parameters for applications need to be developed and approved by the Major NATO Commands (MNCs) and the TSGCE.
- Mapping QoS parameters at the Application Layer to those at the Network Service boundary needs to be studied (there is no formal model for this mapping).
- Not all factors affecting QoS will need to be standardized. A QoS framework is needed that would identify factors that are standardized, procedural, and capable of being monitored by local processing.
- A formal AHWG on QoS is not needed. The focus of the work should be in ISO (presumably SC21/WG4). The Chairman of SG9 would serve as the NATO focal point for QoS work.
- A definitive QoS framework paper needs to be produced for input to ISO. It would be written by volunteers, with the Chairman of SG9 serving as global editor. The goal is to have a draft paper by the end of December 1991. The UK has accepted the lead for six of the seven sections and the US for one. The proposed organization is:
  - Definitions
  - User requirements
  - Scenarios and examples
  - Assumptions, constraints, and limitations
  - Models, to include organizational, information flow, specification, processing, and communications
  - Mechanisms
  - Impact analysis.

STANAG 4250-4 (Management). Part 4 of STANAG 4250 was finalized in October 1990 and distributed within SG9 and subordinate bodies for comment. Since no comments were received, the document has been prepared for submission to SG9 with the recommendation for ratification. The draft STANAG declares that ISO 7498-4 combined with ISO 10040 will serve as the Reference Model for OSI Management. This document is considered ready for ratification.

STANAG 4250-5 (Military Features). A draft contribution to Part 5 of STANAG 4250 from the systems management point of view is ready for publication. Further work would depend on decisions in SG9 on the structure of Part 5.

STANAG dddd on Systems Management. A draft STANAG dddd, *NATO Reference Model for Open Systems Interconnection - Systems Management,* has been prepared (October 1991). Work on profiles is now suspended and awaits the work of EWOS and other implementor's workshops. The document makes ISO/CCITT standards on management communications, management information, and management functions, cited in the *NTIS Transition Strategy,* the basis for the specification of NATO OSI management profiles. The STANAG has several annexes in preparation: Annex A is a

table of contents for the other annexes and Annex B will address security of management; additional annexes will be developed on profiles. The major annexes are:[58]

- Annex B--Security of Management. This annex will describe how NATO management communications are secured and how access to NATO management information will be controlled.
- Annex C--*Eight Military Features.*
- Annex D--*Guidelines for the Use of OSI Management in NATO Systems,* Part 1, *Overview and Tutorial to OSI Management.* Part 1 was developed and distributed to other SG9 working groups in June 1990; it was revised, and the final text was prepared in November 1991 and provided to SG9 in December 1991.
- Annex E--*Guidelines for the Use of OSI Management in NATO Systems,* Part 2, *Application Method.* The current draft is dated October 1991.

Work Plan. The AHWG-OM has a prioritized 12-month work plan [Ref. TSGCE 1990c] from June 1991 to June 1992. The work in 1990 and early 1991 was on military features, broadcast, out-of-band Telecommunication Management Network (TMN) for ISDN, quality of service, and Parts 4 (Management) and 5 (Military Features) of Edition 2 of STANAG 4250, as well as a three-volume *Management Guide*[59] to provide guidelines on the definition of NATO-managed objects. The work plan developed in June 1991 is described in the following paragraphs. [Ref. TSGCE 1991f]

The focus of work for February 1992 will be on Part 2 of the management guidelines document. Review of draft STANAG 4250-4 is scheduled (a high priority if required). Some work (medium priority) is planned for STANAG dddd, QoS, and security. These plans with the same priorities will continue through the June 1992 meeting of the AHWG-OM. STANAG 4250-5 contributions are expected to be completed in February 1992. The first draft of STANAG dddd [with Annex A on Structure of Annexes) and Annex C (Military Features)] is planned to be distributed for comment in June 1992. Initial distribution of the management guidelines annexes is planned for July 1992.

15.3.6 AHWG on ISDN

An AHWG on ISDN was formed by TSGCE SG9 in 1989 to review the status of ISDN and the applicability of these standards to NATO. The terms of reference are shown in Table 38. An overview of the eight military features was adopted at the April 1990 meeting; the results are given in Table 39 (note that the suitability of the ISDN protocols for use in the tactical domain was agreed to be outside the scope of the meeting) [Ref. AHWG-ISDN 1990].

---

58 Point Paper on the Future of the AHWG-OM, n.d.

59 The full title of the *Management Guide* is *NATO Systems Guidelines for the Use of OSI Management.*

Table 38. Initial Approach to Military Features for ISDN

(1)	Identify the ISDN domains to be standardized to assist the development of consistent ISDN standards within NATO countries and, in addition, to fulfill interoperability requirements and facilitate the development of a NATO Communications Subsystem.
(2)	Identify ISDN civil standards applicable to the systems involved in a NATO Communications Subsystem.
(3)	Review the capability of ISDN to support relevant military features, interworking requirements from tactical users/networks, and other NATO user service requirements.
(4)	Consider specifying enhancements to ISDN civil standards to meet a minimum military requirement.
(5)	Determine the impact of ISDN on the NTIS defined by SG9 in accordance with the NATO Reference Model, for example, the NTIS on network management and security.
(6)	Submit technical papers to SG9 for candidate profiles and/or STANAGs.
(7)	Submit a report to SG9 at each meeting.

Source: *Terms of Reference for TSGCE SG9 AHWG on ISDN,* NATO UNCLASSIFIED.

ISDN is a telecommunications concept developed by CCITT and described in the I-Series Recommendations (signalling is described in the Q-Series Recommendations). ISDN is designed to support a wide range of voice and non-voice applications in the same network. Its key element is the provision of a range of services using a limited set of connection types and multipurpose user network arrangements. In addition to CCITT, the main bodies promoting ISDN standardization are ETSI, ECMA, and ANSI. The key standardization areas (to be addressed by the AHWG on ISDN) are [Ref. STC 1991]:

- ISDN interfaces
  - User-to-network interfaces
    - Basic access: 2B+D
    - Primary rate access: 30 B + D
  - Network-to-network interfaces
    - Signalling System No. 7 (SS7)
    - QSIG (based on the user-to-network interface)
- Services: Bearer services, teleservices, and supplementary services
- Enhancements for military features
  - Security
  - Precedence and preemption
- Terminal adaptation.

Table 39. Military Features for ISDN

(1) Mobile Hosts and Multihomed Systems. A number of scenarios are being discussed, some outside the ISDN domain (e.g., in the tactical area) and some within the strategic ISDN domain (e.g., as user moving from one PABX to another). Only strategic ISDN domain issues are currently being addressed in the AHWG on ISDN. It was agreed that ISDN Suspend/Resume procedures for moving during a call were not applicable to mobile hosts. Some form of slow mobility is required where a user may, for example, move between extensions on the same access switch or even to a different access switch and still maintain the same user identify. This would require a type of registration and cancellation procedure where a user takes the user identity around a fixed network. Specific NATO procedures may be required to realize this feature--further study is required. Procedures associated with the cellular radio service are issues mainly applicable to the tactical domain.

(2) Multi-Endpoint Connections. Information needs to be multicast (or broadcast) to several destinations. A central issue is whether a unidirectional service was required for this feature:

(a) If the requirement were defined in terms of a conference call (bidirectional), then commercial products are expected to be available.

(b) If broadcast facilities were provided at the Application Layer using packet procedures, no specific NATO procedures are required.

(c) If broadcasting were required on all bearer services (e.g., voice and data), then the AHWG on ISDN should wait for CCITT/ETSI to define this feature.

It was generally agreed that the multi-endpoint feature is for data application rather than voice; further study is required on the requirement for voice.

(3) Internetworking. The *NATO C3 Architecture* (Volume 4, *Communications Subsystem*) allows both the "T" reference point and the K, M, and N reference points as possibilities for internetworking. If the "T" reference point were chosen, then a number of enhancements would be required for NATO, such as satellite and routing indicators.

(4) Network and System Management. CCITT is defining a network management structure in both the user-network area (Q.940) and within the network. This work is at the architectural level and has not resulted in a definition of detailed procedures. Of particular interest to SG9 are the management functions of Section 3 of Q.940 for fault, configuration, accounting, performance, and security management--all aligned with OSI management functions. In addition, management reference models have been defined.

(5) Security. Key issues are the applicability of NOSA to ISDN (for data services), the impact of ISDN on NOSA (e.g., security of voice services, protection of signalling channels), and the definition of new security features using ISDN capabilities (e.g., common channel signalling). The first two issues are for the AHWG on Security. The AHWG on ISDN will propose ISDN security features relevant to the third issue (e.g., supplementary services) for approval by security experts of SG9.

(6) Robustness and Quality of Service. The only possible special NATO requirement identified is the QoS parameter, should the ISDN network performance figures given in I.350 not prove to be adequate for military applications.

(7) Precedence and Preemption. This feature is already being addressed (service definition and information).

(8) Real-Time and Tactical Communications. No special real-time requirements are foreseen for ISDN. Note that the discussion was limited to interworking with a tactical network and to the concept of a strategic ISDN activity either as a transit network or to gain access to an ISDN user.

Source: *Report of the 2nd Ad Hoc Meeting on ISDN, Paris, 24-26 April 1990,* TSGCE SG9 AHWG on ISDN, May 1990, NATO UNCLASSIFIED.

Note: The suitability of the ISDN protocols for use in the tactical domain was agreed to be outside the scope of the assessment leading to these requirements.

The AHWG on ISDN is discussing the ISDN Reference Model and has considered papers from France (based on the CCITT Reference Model and the *NATO C3 Architecture*), ETSI, and ECMA. These models describe network-to-network interworking, including CCITT No. 7 and QSIG (an extension of Q.931) protocols.

Discussion of essential bearer services for ISDNs used for NATO communications resulted in a two-page recommendation for the Network Bearer Services [viz., 64-kbps

circuit switched (CS) unrestricted as in I.231.1, CS speech as in I.231.2, CS 3.1 kHz audio as in I.231.3, CS access to packet switching node as in I.231.1, B-channel packet switched access as in I.232.1, and D-channel packet switched access on the Basic Rate Interface as in I.232.1] and the Terminal Bearer Services. Further study has been recommended for Frame Relay (I.122), Frame Switching (I.122), user-to-user signalling (I.232.3), 7 kHz audio, 2x64 kbps unrestricted, H0--384 kbps unrestricted, H11--1536 kbps unrestricted, and H12--1920 kbps unrestricted.

One proposal (submitted by the US) suggests the following as the basis for a draft STANAG on ISDN for packet mode services [Ref. AHWG-ISDN 1990b]:

- Networks shall support a packet-switching capacity in conformance with the 1988 CCITT recommendation on packet-switched data, X.31/I.462, *Support of Packet Mode Terminal Equipment by an ISDN*. At the user interface for the Basic Rate Interface, both B channel and D channel packet switching will be supported. At the Primary Rate Interface, B channel packet switching will be supported. Terminals that support X.25-based packet switching will also conform to X.31.
- Conditional notification shall be supported on switched access connections. On permanent virtual circuits, the option of "no notification" shall be available.

The issues identified in Table 40 have been recommended to be the focus of future efforts in the AHWG on ISDN [Ref. AHWG-ISDN 1990a]. Work is ongoing to add primary rate and supplementary services to the basic services in a draft STANAG. Work on Layer 2 and Layer 3 services has been unable to resolve the differences between the ANSI standards and those promoted by ETSI--this may result in a STANAG with two options but would not solve the North American-European interoperability problem [Ref. Savoye 1991]. A summary of the work plan is provided in Table 41.

Table 40. Initial Activities on ISDN

(1)	Work on progressing the layer integration of the OSI Transport Service with the ISDN Digital Access Signalling System
(2)	Develop and provide directory capabilities for resource identification and selection, to include an Application Title Directory and a Network Address Directory, based on ISO 9594 (CCITT X.500)
(3)	Add naming and addressing issues with respect to ISDN to the SG9 working group pursuing these issues
(4)	Adopt the CCITT Common Channel Signalling System No. 7 (SS7) internationally
(5)	Study further tactical communications support by ISDN, with special attention to interconnection with digital radio and cellular networks and to the requirements for maintaining radio silence (e.g., unacknowledged data transfer)
(6)	Address (in the appropriate SG9 working groups) security and system management services as they pertain to ISDN and the coordination of ISDN and OSI Registration Authority issues
(7)	Accelerate the cooperation between ISDN and OSI standardization and planning efforts
(8)	Address the capabilities of B-ISDN to meet the minimum military requirement and consider viewing B-ISDN as the focus for future telecommunications services
(9)	Resolve the issue of interconnecting TCS "black boxes" to ISDN (TCS interfacing to ISDN needs further study)
(10)	Pursue the resolution of ISDN and OSI harmonization in NATO through direct involvement in established working groups within each individual nation, making these groups aware of NATO needs to promote military requirements.

Source: *ISDN/OSI Integration: Issues, Trends, and Recommendations*, Contribution from Canada to the Initial Meeting of the AHWG on ISDN, January 1990, NATO UNCLASSIFIED.

Table 41. Work Plan for the AHWG on ISDN

Activity	Lead	Next Product
Group A--ISDN User-Network Interface (UNI) (Higher Priority)		
• Layer 1 (Physical) Basic and Primary Rate I.430 & I.431 draft STANAGs	UK	Mar 92
• Layer 2 (Data Link) I.440 & I.441 draft STANAGs	UK	Mar 92
Group B--ISDN Network-Network Interface (NNI)		
• Draft STANAG on SS#7--ISUP	NACISA	Mar 92
• Draft STANAG on SS#7--ISUP	NACISA	Mar 92
• SSCP/TACP and OMAP	-	-
b. Impact	STC	Mar 92
a. Analysis	STC	Oct 92
• QSIG report on DSS.1 external standardization body activities	FR	Jul 92
Group C--Study of Enhancements for Military Features		
• Precedence and preemption (status of civil standards)	US	Mar 92
• Security	STC, GE	Mar 92
Group D--Services		
• Teleservices		Oct 92
• Supplementary services (final list)	US, FR	Mar 92
Group E--Miscellaneous		
• Terminal adaptation		Oct 92
• Numbering and addressing (I.330)	STC, FR	Mar 92
• B-ISDN	STC	Mar 92
• Network management		Oct 92
• Tactical issues	STC	Jul 92

Source: *Report of the 6th Ad Hoc Meeting on ISDN, Paris, 19-21 December, to SG9*, December 1991, NATO UNCLASSIFIED.

15.3.7 AHWG on Security

15.3.7.1 Major Security References

The AHWG on Security has developed three major references for use in SG9: NATO OSI Security Architecture (NOSA) [Ref. NOSA 1988], Security Architecture for NATO Information Systems Interconnection (SANISI) [Ref. SANISI 1989], and the NATO Network Security Information Classification Guide [Ref. NATO 1989a]. NOSA was developed to give guidance to contractors and procurement managers on the preferred placement of security services within OSI-conformant systems. SANISI provides detailed rationale on the placement of security services and mechanisms within the OSI Reference Model. A key element of SANISI is the requirement in Layer 3 for a Trusted Communications Sublayer (TCS). NOSA and SANISI do not identify a requirement for security protocols for Layer 4. The current drafts of NOSA and SANISI are Versions 3.1 dated March 1991.

15.3.7.2 Layer 3 and Layer 4 Security Protocols

Two security protocols (SP3 and SP4) have been introduced into ANSI from the US Secure Data Network System (SDNS) [Ref. TSGCE 1989] and have been accepted as a work items in SC6/WG4 in ISO. SP3 is the protocol most closely aligned with TCS. SC6/WG4 has combined three security protocols [into the Network Layer Security Protocol (NLSP), [CD 11577] that have been introduced for Layer 3: SP3, Northern Telecom's SPX, and the UK's End-to-End Security Protocol (EESP). SP3 was judged by the AHWG on Security as equivalent to the end-to-end encryption portion of the TCS. SPX adds connection-oriented service to SP3. The EESP adds CO services to SP3 and includes integrity and traffic padding.[60]

The AHWG on Security has adopted the NLSP as the basis for the TCS to satisfy NATO military requirements [Ref. TSGCE 1990m]. In its December 1991 meeting, the AHWG developed specific text for the NLSP that could be introduced into SC6/WG4 to progress the standard and to develop a PICS to define NLSP extensions necessary for NATO military applications. The AHWG is planning its work on TCS to be based on the ISO standards. CA, UK, and US are all active in bringing AHWG work back into SC6/WG4. [REF. Staton 1991]

15.3.7.3 Security Activities[61]

The AHWG on Security is reviewing and maturing concepts of an ISDN security architecture. The AHWG has noted that the *NATO C3 Architecture* (see Section 11.1)

---

[60] EESP was introduced into SC21/WG1 during the May 1990 meeting in Seoul. EESP has been proposed to the JTC1 as a new work item.

[61] This section is based on the *Report to the Ad Hoc Working Group on Security to the SG9 Coordination Group*, Hal Staton, Chairman of the AHWG on Security, 29 October 1991, NATO UNCLASSIFIED.

underlines the importance of becoming aware of the security problems associated with an architecture that combines circuit switching with packet switching handling real-time voice and high-bandwidth data.

Three papers have been developed on TCS and security management issues: Systems Management, Access Control Management, and Key Management. These will be revised and eventually condensed and included as annexes to STANAG 4250-4 or in Part II (Architecture) of the NOSIP Strategy document (see Section 15.3.1.2).

Work has begun on Part 2 (Security) of STANAG 4250 to determine if it could become the appropriate reference document incorporating the pertinent parts of SANISI and NOSA. The actual composition of Part 2 has not been determined.

The AHWG is reviewing exploratory developments (such as one being conducted in France for MHS) to identify security mechanisms such as security gateways for MHS interoperability (e.g., X.400-1988 and ACP 127 systems) and security services for ISDN. In the French work, the security services are provided by the Message Transfer Agents (one an end-to-end basis) rather than by the User Agents. The French prototype provides security services at the User Agent via a message security protocol using a Thompson-CSF secure workstation. The French exploratory development is very much like the US SDNS.

The AHWG has agreed that a formal language specification of TCS/NLSP is needed before an implementation phase can be reached and requests the nations to coordinate their efforts with the AHWG to avoid duplication or non-interoperable approaches. One immediate interoperability problem is that connectionless option of NLSP is not identical nor interoperable with SP3; since SP3 is the US standard, adoption of NLSP could produce interoperability problems for systems already implementing the current (SP3) standard.[62] One approach to this is a future modification to SP3.

Discussion of SANISI has included proposed annexes on application and implementation aspects of the TCS and the Denial of Service definition. Agreement has been reached that once an event object is defined, the recovery mechanisms are the same whether the cause was malicious or accidental and so is a management issue. A review was conducted of the SANISI annexes to determine if these can be downgraded to NATO UNCLASSIFIED and be permitted to be used as technical input to ISO--it was determined that these annexes could not be downgraded below NATO CONFIDENTIAL, so that other means will need to be used to provide technical input to ISO.

15.3.7.4 Security Support for CNSI

The AHWG has expressed strong support for the WG3 CSNI program to demonstrate the proof of concept of the security protocols and architecture. The AHWG

---

[62] The SDNS SP3 is part of the commercial COMSEC Development Program in the United States. Further, the emerging Caneware being developed by NSA implements SP3.

has noted the concerns expressed that SDNS SP4 is not a suitable candidate from a NOSA point of view, as NOSA does not identify a requirement for security services in the Transport Layer. A recommendation has been drafted that WG3 consider the concept of a TCS as in NOSA and SANISI. The TCS services definitions and protocol specification are not yet complete, but will be sufficient to provide the required security services within the next 12 months.

The AHWG on Security held meetings of security experts in 1990 and 1991 to discuss the TCS service definition and protocol specification. Progress was made on providing the additional technical work required for a detailed design specification for the TCS. This specification will be provided to the SG9 WGs for consideration and, in the case of WG3, possible implementation.

15.3.7.5 Work Plan for AHWG on Security

The current 18-month work plan is being revised by the AHWG; expected to be ready in mid-1992, it will address the deliverable documents related to the TCS, management, and upper layer issues. Table 42 identifies the specific tasks given to the AHWG on Security in the revised special tasking instructions.

Table 42. Planned Activities for AHWG on Security

(1)	Develop and maintain a network information security classification guideline for use by NATO elements when developing network protocols and architectures
(2)	Develop and refine a security architecture for NATO information systems based on the OSI Reference Model
(3)	Define the security services required for NATO military application and determine the placement within the basic reference model
(4)	Influence ISO/CCITT and other standards bodies to adopt additional security services as appropriate
(5)	Develop NATO STANAGs for the security architecture and communications protocols based on existing standards
(6)	Extend applicable communications standards to accommodate military security services where necessary
(7)	Complete the detailed design work on security layers and sublayers leading to protocol specification, service definitions, and user requirements documents
(8)	Review, advise, and recommend security annexes to all layer STANAGs
(9)	Liaise with other NATO groups, both inside and outside SG9, working on network security issues.

Source: *Special Report to the TSGCE by the Chairman SG9,* Annex XIII, *Special Tasking Instructions for the Ad Hoc Working Group on Security,* AC/302-D/602, 11 July 1991, NATO UNCLASSIFIED.

15.3.8 Status of Activities and Plans for Developing the Military Message Handling System (MMHS) for NATO

During the last 4 years, an AHWG on MMHS, reporting to TSGCE SG9/WG2, has been working to have features required by the military incorporated into the MHS defined by international standards bodies. The initial proposals, based on X.400-MHS(84), for an MMHS have been accepted as an Intercept Profile by SG9; it addressed security, confidentiality, integrity, authentication, message stores with access protocols,

and directory services. Most of these features have now been incorporated in CCITT X.400-MHS(88). Known as the "Blue Book," MHS(88) was ratified in November 1988.

MMHS will be addressed in a separate Application Layer standard, STANAG 4406 [Ref. STANAG 4406 1991] (September 1991; see Section 15.4.7). STANAG 4406 will incorporate four elements that are being developed simultaneously by the AHWG on MMHS: Base Standard, Rationale, an Alpha Profile, and a Beta Profile. The Alpha profile is intended to address strategic and tactical applications where bandwidth limitations are not severe, and the Beta Profile is intended to address tactical applications where bandwidth is severely limited. For the Beta profile, the AHWG on MMHS assumes that bandwidth will be conserved by eliminating all but the most vital services of MHS. These profiles are being written as a "delta" or change to the MHS profile being developed by the European Workshop for Open Systems (EWOS) [Ref. EWOS 1990a]. Each MMHS profile will be included in STANAG 4406 as a separately ratifiable annex [Ref. WG/1 1990c].

The AHWG-MMHS work has been separated into two sets of functional groups. The first set consist of military messaging services, notification, security, redirection, distribution lists, conversion, ACP 127, and MMHS(84) gateways. The second set will provide directories, message store, physical delivery, management, routing, local services, and PICS. The current (December 1991) draft of STANAG 4406 addresses the first set of functional groups. [Ref. Krick 1991]

The *Intercept Profile for MMHS*, based on MHS(84), has been amended (Issue 2) to include full support for ACP 127 [Ref. MMHS 1990]. It was completed in February 1990. Issue 2 has a new annex (Annex C) on implementation options for the military header extensions. Issue 1 of the profile was accepted as an intercept strategy for the *NTIS Transition Strategy* [Ref. NATO 1991]; however, depending on choices of interoperability parameters, MMHS implementations based on MHS(88) may not be backwards compatible with MHS(84) implementations (see Section 4.3.2.3).

One area of MMHS not addressed by MHS(88) is support for trusted functionality. Such support may be covered by standards developed by the SDNS security protocols SP3 and SP4 to carry out services associated with trusted functionality. The May 1989 meeting of the AHWG-MMHS was devoted to security and succeeded in developing two functional groups of security services. One of these does not require use of asymmetric encipherment mechanisms, but precludes direct support of nonrepudiation services. These have both been accepted by EWOS. The AHWG-MMHS is seeking guidance from the AHWG on Security to identify suitable encipherment mechanisms to support these services [Ref. WG/2 1989]. The AHWG on Security confirms the need for asymmetric cryptographic mechanisms and indicates that such mechanisms must be offered by the Nations for consideration and approval by the appropriate NATO authorities [Ref. AHWG-S 1990a].

Table 43 provides a statement and status summary of the work areas for MMHS being addressed in the 12-month work plan of the AHWG on MMHS for 1992 [Ref. AHWG-MMHS 1990b].

15.3.9 Status of Activities and Plans for Developing Data Link Standards for NATO

The first meeting of SG9/WG4 on Data Links was held in June 1991; five nations (FR, GE, NO, UK, US) participated in the December 1991 meeting. Tasking on various data link topics was provided from the TSGCE to SG9. WG4 was created within SG9 to address such data link topics as media-independent data link architecture (MIDLA), Multifunctional Information Distribution System (MIDS),[63] unmanned aerial vehicles (UAVs), stand-off surveillance target and acquisition (SOSTA) systems, and reconnaissance and target acquisition (RSTA) systems. WG4 will meet twice in 1992: in May 1992 in the United Kingdom in conjunction with a visit to the UK JTIDS Network Test Facility and in October 1992 in Brussels.

WG4 has accepted responsibility for the maintenance and configuration management of STANAG 4175 on MIDS; currently (December 1991) ratified by ten nations, STANAG 4175 will be promulgated shortly. WG4 will address other data link issues such as NATO Improved Link Eleven (NILE) and UAVs. There was specific interest in investigating solutions to the UAV data link requirements but no interest in discussion of MIDLA (see Sections 15.3.4 and 15.3.4.2 for discussion of MIDLA and other topics originally proposed for Nunn Amendment funding). The tasking assigned to WG4 is summarized in Table 44. WG4 is currently focusing on issues relevant to the introduction of MIDS nationally and in NATO and what the group should do to assist in that process. [Ref. Ahern 1991]

---

[63] MIDS is a NATO form of the Joint Information Distribution System (JTIDS) developed in the US. The initial implementation in NATO used the Interim JTIDS Message Standard (IJMS), which is not interoperable with JTIDS. While there are significant differences in hardware, the future message standard for MIDS (STANAG 4175) is essentially the same as the TADIL J used in JTIDS.

Table 43. Work Plan and Activities on MMHS

(1) Group Communications. Draft planned for December 1991.
(2) Routing. Define algorithms and constraints. Started work in June 1990; draft planned for December 1991.
(3) Naming and Addressing. Draft planned for December 1991.
(4) Definition of MMHS Managed Objects. Draft planned for December 1991.
(5) MHS(84) Gateway Defin ion. Draft planned for March 1992.
(6) Physical Delivery. Scop e and produce guidelines for physical delivery. Draft planned for March 1992.
(7) Beta Profile. Draft planned for March 1992.
(8) T Profiles. Identify lower layer requirements for MMHS.
(9) ODA. Evaluate the potential use of the Office Document Architecture and its associated interface format (ODIF) for multiple data formats in MMHS.
(10) EDI. Evaluate the ramification of CCITT's adoption of X.435 defining Electronic Data Interchange with the X.400 series.
(11) MMHS API Extensions. Study the extensions to the APIs required to support MMHS and ACP gateways.
(12) ACP 123 Liaison Issues. Identifies and discusses, in the form of a liaison statement to the ACP 123 Working Group, MMHS-related issues that fall into the operational rather than the technical, area of standardization. The areas would include distribution lists, handling policy, military naming hierarchy, and registration.
(13) Registration. Study the issues of registration as they relate to the MMHS and its protocol.
(14) Security. Continue the study of security requirements of MMHS.
(15) Naming and Addressing Requirements. Study the restraints required in order to create an interoperable name space for the NATO MMHS.
(16) MMHS Use of Directory. Study the exact use and therefore be able to generate the requirements MMHS will have for using Directories in the future.
(17) Conformance Testing for MMHS. Study the issue of conformance testing for MMHS implementation.
(18) Authentication Issues in MMHS. Study the interoperability issues as they pertain to message, originator, and recipient authentication across national borders. If NATO is to be able to interoperate, it must be possible to authenticate messages regardless of their origination and destination.

Source: *MMHS AHWG Chairman's Report to Working Group 2,* Chairman WG2 (M. Krick), 30 September 1991, NATO UNCLASSIFIED.

Table 44. SG9 Tasking Instructions for WG4 on Data Links

- To sponsor and develop technical interoperability standards for data links; control required test and configuration management of data link standards; and promote their use to avoid unnecessary proliferation of application specification data link equipment and systems
- To plan, initiate, and coordinate development, testing, and implementation of interoperable data link equipment and systems
- To provide advice for the TSGCE on all matters related to data links
- To maintain configuration control of STANAG 4175 and collate implementation/transition plans for the introduction of the MIDS within the nations and NATO, monitor its implementation; and identify areas for cooperative activities with the aim of initiating such activities
- To explore the subject of media independent data link architecture based on a layered structure
- To explore the use of an existing or initiate the development of a technical interoperability standard for a common data link for UAVs, SOTAS, and RSTA.

Source: *WG4 on Data Links Report to the Chairman of SG9,* AC/302(SG/9)D/96, Chairman WG4, 10 December 1991, NATO UNCLASSIFIED.

15.3.10 TSGCE SG9 Project Group on MIDS LVT

PG9 on the MIDS Low Volume Terminal (LVT) was formed by TSGCE to develop an MOU for an multinational, multi-Service, cooperative program for a light-weight tactical information distribution system. (PG/9 on MIDS LTV is expected to be disbanded once its MOU and a NATO Project Steering Committee are established, expected to be completed during the first half of 1992.)

The LVT would be a pre-planned product improvement to the Joint Tactical Information Distribution System (JTIDS) that would reduce the size (from 1.7 to 0.6 cu ft) and weight (from 135 lb to 65 lb). The LVT would reuse the JTIDS software, including the LINK 16 (JTIDS) standard [and not the Interim JTIDS Message Standard (IJMS)]. The participating nations[64] (FR, SP, IT, GE, and US) plan ground-based, airborne, and ship-based employment (the US would use it for the F/A-18s). The project definition phase (1987-1990) was followed by the pre-engineering and manufacturing development (EMD) phase (1991-1992), in which the RFP would be finalized and released, proposals evaluated, and contract negotiation. National contractors would be awarded work at the same proportion as national funding. The EMD phase (1992-1997) begins with contract award and includes design, fabrication, integration, test, and technical data package verification. The production phase (1997-2010) is initially planned to acquire 2,750 LVTs (plus spares). [Ref. TSGCE 1991g]

15.4 Status of NATO OSI STANAGs

Table 45 identifies the STANAGs being developed that will specify ISO standards and applicable military options and extensions, if any. Work has begun on all these STANAGs, but only the NATO Reference Model, STANAG 4250, has been ratified. Originally, TSGCE SG9 planned to issue a single STANAG for all services and a second STANAG for all protocols at each layer, giving a total of 14 STANAGs in addition to STANAG 4250, the NATO Reference Model. In October 1987, TSGCE SG9 agreed [Ref. UK 1988, Annex 1.2] to work at the Application Layer for single STANAGs for each Application Layer service, such as MMHS (STANAG 4406). Protocol specifications as well as service definitions would be addressed in that STANAG. This approach will require editorial changes in STANAG 4250.

---

[64] Norway, Canada, and the United Kingdom participated in the project definition phase but declined to continue into development and procurement.

Table 45. NATO OSI Standards

OSI Layer	Service Definitions STANAG	Service Definitions Draft Published	Protocol Specifications STANAG	Protocol Specifications Draft Published
Reference Model	4250 Ed 1 4250 Ed 2 Prt 1 4250 Prt 3 4250 Prt 6	Apr 86 (Ratified) May 90 (Draft)[a] December 1991 Dec 91 (draft)	-	-
1	4251	Oct 91	4261	Oct 91
2	4252	5 Dec 91	4262	5 Dec 91
3	4253	Nov 91	4263	Nov 91
4	4254	Oct 91	4264	Oct 91
5	4255	18 Oct 90	4265	18 Oct 90
6	4256 4258 (ASN.1)	18 Oct 90 18 Oct 90	4266 4259 (ASN.1 BER)	18 Oct 90 18 Oct 90
7	4406(MMHS)[b]	10 Dec 91	4406(MMHS)[c]	10 Dec 91

[a]The May 1990 draft of STANAG 4250 was circulated to the Nations for ratification.
[b]Multiple STANAGs are planned for Layer 7; STANAG 4406 will address MMHS.
[c]For Layer 7 there will be a single STANAG for each pair of related Application Layer Service Definitions and Protocol Specifications.

When stacks of standards, options, and interoperability parameters that involve more than one OSI layer are selected for open systems interconnection for NATO data processing and distribution systems, the agreements will be specified in documents that are to be known as functional profiles. NATO functional profiles, initially to be drafted by TSGCE SG9, will be based on the OSI STANAGs 4250-4259 and 4261-4266. To date, the functional profiles promulgated by TSGCE SG9 are contained in the *NTIS Transition Strategy* and are all based on commercial international OSI standards and the OSI STANAGs. These profiles (application, transfer, and relay) are illustrated in Figure 13 of Section 6.3.1 and Appendix B.

STANAG 4250, *NATO Reference Model for Open Systems Interconnection,* has been revised and the new draft developed in the May 1990 TSGCE SG9 plenary meeting was circulated to the Nations for ratification. The new STANAG will be in five parts, only the first of which is ready for ratification. The first four parts conform to the current structure of the OSI Basic Reference Model, ISO 7498:

- Part 1--*General Description*
- Part 2--*Security*
- Part 3--*Naming and Addressing*
- Part 4--*Management*
- Part 5--*Military Features*.

Two additional parts (*NATO Functional Profile Guidelines* and *Conformance Testing*) were separated from STANAG 4250 and will be drafted and ratified separately. In May 1990, SG9 agreed to reissue Edition 2 of STANAG 4250 as described above without going through a formal ratification process [Ref. TSGCE 1990k]. Thus, STANAG 4250 has been forwarded to the TSGCE for promulgation.

During its meetings in February 1989, TSGCE SG9/WG2 addressed the impact of the eight military features on the Session and Presentation Layers, especially for security, quality of service, and multipeer data transmission. WG2 determined that for both the Session and Presentation Layers there are no military features that have been defined, that are needed in the near term, and that are not supported by the OSI standards. WG2 has therefore forwarded the draft STANAGs for the Session and Presentation Layer (STANAGs 4255, 4256, 4265, and 4266) and ASN.1 (STANAGs 4258 and 4259) to TSGCE SG9 for ratification; TSGCE SG9 decided in March 1989 to distribute these drafts to the nations to begin the ratification process. These drafts were modified by WG2 in February 1990 and provided to SG9 in May 1990. SG9 identified a number of editorial problems with the draft STANAGs, requested these be addressed by WG2, and asked for revised drafts at the December 1990 SG9 plenary meeting.

The remaining paragraphs in this section summarize the scope of the current drafts of these STANAGs. The STANAGs are discussed layer by layer beginning with Layer 1, the Physical Layer. The discussion emphasizes the portions of the STANAGs addressing deficiencies and enhancements for the military features. As noted above, SG9/WG1 is responsible for Layers 1-4 and SG9/WG2 for Layers 5-7.

15.4.1 Physical Layer STANAGs

Draft STANAG 4251 (October 1991) identifies for the Physical Layer all eight areas for potential military enhancements and summarizes the services provided by and the deficiencies of current civil standards. All but three of the areas are identified as "not envisioned to affect the Physical Layer." There are three areas in which enhancements are possible (network/systems management, security, and robustness and quality of service), but these are marked "military enhancements are for further study."

Draft STANAG 4261 (October 1991) also identifies for the Physical Layer all eight areas for military enhancements, summarizes the protocols provided by and the deficiencies of current civil standards, but leaves specific military enhancements for further study. All but three of the areas are identified as "not envisioned to affect the Physical Layer." The three areas in which enhancements are possible are the same as for STANAG 4251.

Requirements and standards for Mechanical Aspects (Annex D) are provided by STANAG 4261 in the areas of connectors, pin outs, cabling, and shielding and dielectric. Standards for Functional Aspects are provided in Annex E, for Electrical Aspects Annex F, and for Procedural Aspects in Annex G, STANAG 4261.

Eight PICS proforma are provided: three in Annex H for mechanical aspects with respect to selected ISO standards (ISO 2110, ISO 4903, and ISO 8802.3); and five in Annex H for functional aspects with respect to selected CCITT standards (V.5, V.6, V.10, V.11, V.24, V.28, and X.1).

15.4.2 Data Link Layer STANAGs

STANAG 4252 will address, as does ISO 8886 upon which it is based, both CO and CL modes of service. None of the security aspects (Annex B) have yet been identified for the Data Link Layer. STANAG 4252 (December 1991) identifies deficiencies only in one of the eight areas for enhancements:

- Network/system management. The definition of the Data Link Management Objects and their manipulation are not covered in the existing ISO standards, but are the subjects of on-going work and are expected to be completed in the near future. After completion, it will be verified if military enhancements are requisite.

The current draft STANAG 4262 (December 1991) indicates that "no need for enhancement was identified" for all but one of the eight areas of potential military features. The remaining area is addressed as follows, without specifying the protocols needing enhancement:

- Network/system management. Enhancements are needed, but these may be provided as a result of the on-going ISO standardization work. If this is not the case, further work would be needed to provide the missing military enhancements. Note: The specification of Data Link Layer Management Objects is the subject of the work item JTC 1.06.44 in ISO.

Annex D of the current draft STANAG 4262 addresses the Balanced Link Access Procedure B (LAP B), based on ISO 7776 and provides for the CO-mode data link service used by packet level protocols (PLPs) such as CCITT X.25 PLP and ISO 8208. Annex E addresses LAP D for ISDN based on CCITT I.440 and I.441. Annex F addresses the Logical Link Control (LLC) and the Media Access Control (MAC) protocols, based on ISO 8802-2 (LLC), 8802-3 (CSMA/CD LAN), 8802-4 (Token Bus LAN), and 8802-5 (Token Ring LAN). The LLC, when used with the appropriate MAC data link sublayer protocol, provides CO and CL-oriented data link service in a LAN environment. Annex G has been deleted. [Annex G addressed the data link protocol Balanced Class of Procedures (BAC) based on the HDLC standards ISO 7809, 4335, 3309, and 8885 and provides CO- and CL-mode services. Options explicitly included Exchange Identification (XID), UI frames for CL-mode data transfer, selective reject, extended sequence numbering, test, and extended frame check sequence capability (32-bit frame check sequence).]

15.4.3 Network Layer STANAGs

STANAG 4253 (November 1991) is based on ISO 8348 *(Network Service Definition),* including the three addenda, and thus provides for both connection-mode and connectionless data transmission. The Security Annex is classified; as provided in the NOSA document (see Section 8.1.3.2), it addresses services such as peer entity authentication, data origin authentication, access control, connection confidentiality, connectionless confidentiality, traffic flow confidentiality, connection integrity without recovery, and connectionless integrity. STANAG 4253 addresses the areas of deficiencies of the civil standards shown in Table 46 for providing military feature enhancements.

Table 46. Areas of Deficiencies and Enhancements for STANAG 4253

(1) Multihoming. In the interest of survivability, an end system, identified by a single "logical" network address, may need to be connected at several Subnetwork Points of Attachment (SNPAs) either with more than one link into the same subnetwork or with links into several subnetworks. Routing management functions will be needed in order to determine the SNPA to be used. **Enhancements** for routing management (if any), maintenance of connections, and data transfer processing **are for further study.**

(2) Mobile Hosts. This requirement is for end systems identified by a single logical address to be able to connect to different SNPAs, although only one connection may be in use at any one time. In this case it may not be possible to determine in advance which subnetwork links will be involved in establishing connections associated with a particular subscriber address. The Network Layer addressing is extended in this STANAG to support logical network addresses that may identify more than one NSAP. **Enhancements** for routing management (if any), maintenance of connections, and data transfer processing **are for further study.**

(3) Multiaddressing. To economize on network bandwidth and increase speed of delivery, an application that involves sending the same data to a number of destinations will require a multi-addressing service (multipeer data transmission) within the Network Layer, which provides either selective addressing or broadcast facilities. The Network Layer addressing is extended in Annex D of this STANAG to support multicast addresses that may identify more than one NSAP. **Enhancements** for multipeer data transmission are **for further study.**

(4) Internetworking. No deficiencies in the application of the civil internetworking standards to military requirements have been identified.

(4) Management. Additional management facilities may be required to support the other military enhancements. Military **enhancements** of the ISO Network Layer management objects **are for further study.**

(5) Security. The ability is required to signal the security label of each network connection and each connectionless service data unit. The security classification will remain constant throughout the life of a connection. **Enhancements: the security label for a network connection or a connectionless service data unit may be signalled as a protection QoS parameter.**

(6) Robustness and Quality of Service. The ability to survive physical damage and denial of service attacks and to route around damaged or partitioned networks is required for military systems. Military **enhancements** to Network Layer management functions for robustness **are for further study.** No requirement for military enhancement for the Network Layer service for QoS has been identified.

(7) Precedence and Preemption. No requirement for military enhancement has been identified beyond the priority QoS parameter defined in ISO 8348.

(8) Real-Time Communications. **Enhancements** for real-time communications **are for further study.**

Source: *Draft STANAG 4253,* November 1991, NATO UNCLASSIFIED.

Annex D to STANAG 4253 discusses the two types of addresses used in the Network Layer: (1) subnetwork addresses, which identify a point of attachment to a

subnetwork (e.g., an X.25 network) and (2) network address, which is (ISO 7498-3) a name, unambiguous within the OSI environment, that is used to identify a set of NSAPs. An NSAP-address is a network address that is used to identify a single NSAP. The subnetwork address must be derivable from the network address, either directly using a field of the network address or indirectly using routing table or directory service. Annex D provides technical detail on:

- Support of multi-addressing by defining Group NSAP addresses. The annex notes that since the relevant ISO standards explicitly prohibit the network user from being able to influence routing decisions through the network layer addressing mechanisms, support for the military requirements for multi-homing and mobile hosts cannot be provided through addressing mechanisms. These features can only be provided through appropriate Network Layer routing algorithms.
- Addressing schemes, including the Initial Domain Part (IDP) and the Domain Specific Part (DSP) of an NSAP-address, the Authority and Format Identifier (AFI) and Initial Domain Identifier (IDI) that make up the IDP, and the four basic schemes recognized by ISO 8348/AD2.
  (1) CCITT numbering schemes for public networks--the IDI is X.121 for public data networks, F.69 for Telex, E.163 for circuit switched networks, or E.164 for ISDNs.
  (2) Schemes with an address allocated under a national registration authority, in which the IDI is an ISO Data Country Code (DCC) according to ISO 3166.
  (3) Schemes with an address allocated under an international registration authority, in which the IDI is an ISO International Code Designator (ICD) allocated according to ISO 6523.
  (4) Local schemes that would only be recognizable amongst a restricted network of systems.
- The NATO-ICD scheme, in which NATO, as an international authority, allocates addresses. The AFI is 46 for ICD decimal addresses and 47 for binary addresses. Currently there is one NATO addressing sub-schema defined, the scheme "X" that uses AFI=46 and NATO Format Identifier=10. This scheme is for use with decimal coded addresses using NATO domain identifiers allocated under STANAG 4214. For NSAP addresses with NATO as the top-level addressing authority, the IDP has an abstract syntax of 460026 or 470027.
- NSAP address allocation, Internet NSAP address structure, Internet address subdomains, address allocation with a subdomain, allocation of routing area selectors, allocation of system identifiers, and Internet NSAP address examples.

STANAG 4263 (November 1991)provides for three types of CO-mode Network Layer protocols: (1) DTE-to-DTE, based on the 2nd Edition of ISO 8208 (*X.25 Packet Level Protocol for DTE,* 1990); (2) DTE-to-DCE, based on ISO 8878 (*Use of X.25 to Provide the OSI CO Network Service*) and the 2nd Edition of ISO 8208 for end systems and on CCITT X.25(1988), Sections 3, 4, 5, 6, 7, and Annexes A-I, for subnetworks; and

(3) STE-STE, based on the X.75 Packet Level Protocol (Sections 3 through 5 and Annexes A through E) for the interconnection of two packet-switched data networks. These all provide the connection-oriented network service (CONS). The use of the X.25 PLP to provide the CONS over an ISO 8802 LAN is not currently addressed in STANAG 4263.

Annex B on security for STANAG 4263 has yet to be produced (as of December 1991), but will address--as provided in the NOSA document (see Section 8.1.3.2)--services such as peer entity authentication, data origin authentication, access control, connection confidentiality, connectionless confidentiality, traffic flow confidentiality, connection integrity without recovery, and connectionless integrity.

The required military enhancements for providing CONS using the X.25 PLP (Annex C) are given in Table 47. Appendix A to Annex C is the PICS proforma. Appendix B to Annex C recommends a set of optional NATO user facilities be added that are always separated from the standard X.25 user facilities by a facility marker. They include (1) "default security level assignment: (an optional user facility agreed for a period of time) to provide for the selection of default security level--the highest security level that may be associated with any virtual call at the DTE/DCE interface--from the list of security levels supported by the network provided"; (2) "security level selection and indication" that may be requested by a DTE for a given virtual call; (3) "default priority levels assignment"; and (4) "priority level selection and indication."

Table 47. Military Enhancements Identified for Annex C of STANAG 4263

(1)	Security. The use of the network service Protection Quality of Service parameter to associate a security level with a network connection is for further study.
(2)	Precedence and preemption. Military systems using OSI protocols need to be able to signal priority of data transferred over a connection, the priority to gain a connection, and the priority to keep a connection. The priority thereby signally may then be used to determine the precedence of data and to control the use of and allocation of network resources. Use of priority facility is optional in this STANAG, but may be enforced by specific profiles. Priority values are integers in the range 0 to 14, with 255 meaning "unspecified." Annex C specifies the procedures to be used when a subnetwork does and alternatively does not implement precedence and preemption facilities.
(3)	Multihoming. Multihoming may be achieved through the X.25 Hunt Group optional user facility, provided the SNPAs corresponding to the various "homes" can be defined as members of an X.25(1988) Hunt Group. The use of the Hunt Group facility for multihoming is transparent to the OSI network service user. Three types of Network Layer management facilities are specified in the STANAG to support the use of a Hunt Group: configuration, multihoming subscription options, and multihoming registration.

Source: *Draft STANAG 4263*, December 1991, NATO UNCLASSIFIED.

An enhancement for only one military feature is specified in Annex D for interconnecting two packet-switched networks using CONS and the X.75 PLP:

- Precedence and preemption. The priority of a network service connection shall be indicated, when appropriate, by means of the network service Priority Quality of Service parameter as in Annex C. This parameter is mapped by the protocol to the X.25(1988) Priority facility. According to X.75(1988), the

Priority facility is relayed unchanged as an X.25 user facility, which may be inspected and whose values are stored, but which does not affect the progress of the virtual call. This STANAG extends the specification of X.75(1988) in the following way: an STE may record the priority of a call and use this value to preempt a lower priority call under certain (implementation-dependent) conditions. In this case, the STE shall clear the call with cause "DCE originated" and reason "QoS not available--transient condition," as though the call had been cleared by one of the interconnected subnetworks according to the specifications of Annex C. Priority values are integers in the range 0 to 14, with 255 meaning "unspecified."

Annex E to STANAG 4263 [*Connectionless Network Protocol (CLNP)*] defines an internet protocol (IP) providing the CLNS. The CLNP relies on the provision of an underlying CL-mode service by real subnetworks or data links. It is classified as a subnetwork-independent convergence protocol. The underlying CLNS may be obtained either directly from a CL-mode real subnetwork or indirectly through the operation of an appropriate subnetwork-dependent convergence function (SNDCF) or protocol (SNDCP) over a CL-mode real subnetwork. Annex E is based on ISO 8473 (Sections 3-9 and Annexes A-C) and provides extensions for the following three military features:

- Security. A security parameter is provided in every IP Protocol Data Unit (PDU) using the Security Option. The structure of this parameter (e.g., security levels and codes) is for further study.
- Precedence and preemption. Priority is realized through selection of a priority parameter in the options part of the PDU header. Use of the priority parameter is optional. When implemented for use within end systems and intermediate systems, the priority parameter may be used as a criterion for pre-empting memory and/or processing resources. This can be achieved by sorting queued traffic within end systems and intermediate systems during periods of anticipated or real congestions. Preemption of resources can be achieved by discarding NPDUs. Encoding of the precedence and preemption parameter and the error conditions are specified in the STANAG.
- Multicasting. It is necessary to allocate and reserve address space for multicasting and broadcasting in IP; extensions to IP to implement and manage multicasting are still to be defined.[65] Concepts for multicast addresses are described in detail in the STANAG.

Annex E on CLNP does not specify the use or non-use of multicasting or broadcasting, but the Annex allocates and reserves address space for these two capabilities. The discussion of multicast encoding addresses the following topics: multicast addresses for subnetworks, multicasting addressing for areas, multicasting addresses for domains, multicasting error conditions, and multicast subscription options (TBD).

---

[65] Draft STANAG 4263 identifies US DoD RFC 1054, *Host Extensions for IP (DoD) Multicasting*, as the source for descriptions of the required extensions to ISO IP. See Appendix H.

Annex E also contains a draft NPICS proforma (Appendix 1) and an informative discussion of CL network routing exchange protocols (Appendix 2). A five-page informative appendix (Appendix 3) discusses security options for CLNP--these options are based on logical extensions of appropriate fields (i.e., Basic Portion fields and Extended Portion fields) within the provisions of ISO 8473. As noted above, support of precedence and preemption is based on use of the priority option within CLNP. Scheduling is protocol data units is a local matter based on priority functions of ISO 8473 subject to constraints defined in CLNP Annex. An optional congestion notification function is also described.

15.4.4 Transport Layer STANAGs

STANAG 4254 (October 1991) provides the transport service definition. Since NOSA (see Section 8.1.3.2) identifies no security services for the Transport Layer, there are no military-specific security services or protocol enhancements. The CO transport service (Annex C) is based on ISO 8072. The CL transport service (Annex D) is based on ISO 8072/AD1 (with the restriction that the note of paragraph 15.2.3 is not retained).

Annex E of STANAG 4254, *Real-Time Transport Service (RTTS)*, has been proposed as fulfilling the real-time military features for NATO military systems. Specifically, RTTS is designed to offer more functionality to such services as connection service and data transfer service and to provide additional services such as synchronization and management. RTTS provides services for broadcasting, selective broadcasting, and concentration. Chapter 2 of Annex E, *Definition of the Real-Time Transport Service (RTTS) Provided by the Transport Layer*, uses concepts, terminology, and structure similar to ISO 8072 for transport Classes 0, 1, and 2. RTTS appears to impact more than a single layer (Layer 4) and does not appear to fully conform to the Basic Reference Model ISO 7498.

Deficiencies and required enhancements in seven areas are noted in STANAG 4254 for both CO-mode and CL-mode transport services as shown in Table 48 (internetworking is not applicable).

STANAG 4264 (October 1991) provides the transport protocol specification. The connection-oriented transport protocol (Annex C) is based on ISO 8073. End systems must implement transport protocol Classes 0 and 2; other classes may be implemented in addition. The deficiencies and enhancements to seven of the military features (internetworking does not apply) are given in Table 49.

Table 48. Deficiencies and Enhancements Identified for STANAG 4254

(1) Multihomed and mobile host systems. No requirement as the transport service is not affected by either the multiple attachment of a host to two or more nodes or subnetworks nor the change at any time by a host of network or subnetwork attachment.

(2) Multiaddressing. The transport service does not provide any service or function related to *multiaddressing*. To specify the addresses of participants in a multipeer connection, the Group Address can be resolved into a number of ordinary addresses or the address parameters in the service definition can be redefined to permit the use of a list of addresses rather than just one.

(3) Network/system management functions. Transport management service primitives are required to satisfy this requirement, and the primitives defined in ISO 9595 (CMIS) are satisfactory for the communication of information related to the Transport Layer managed objects. Specific management objects and functions need to be defined.

(4) Security. Security deficiencies and **enhancements are for further study.**

(5) Robustness and Quality of Service (QoS). **No enhancements are required.** QoS parameters are provided to express the priority of a data transmission.

(6) Precedence and preemption. **No enhancements required.** A QoS parameter is provided to express the priority of a transport connection.

(7) Real-time and tactical communications. In real-time communications, [there is a] requirement to have short transit delay. There is also a requirement for such services as periodic data transmission and synchronization service, which are not provided by the ISO transport service. The requirement of a short transit delay implies no segmentation of data; the length of the TSDU must be limited for that type of communication. For real-time communications, the **definition of services is for further study** (it could be based on the Real-Time Transport Service in Annex E). For tactical communications, ISO transport services are suitable.

Source: *Draft STANAG 4254,* October 1991, NATO UNCLASSIFIED.

Table 49. Deficiencies and Enhancements Identified for Annex C of STANAG 4264

(1) Multihomed and mobile host systems. The protocol shall have the recovery mechanism of Classes 1, 3, or 4 in the case where the Network Service Provider releases the network connection each time the host system changes SNPA and the QoS requirement specifies low probability of unexpected connection release. If the classes 0 or 2 are used, the recovery of the connection shall be provided either in the Network Layer or in the Application Layer. If a host system has more than one NSAP or needs the capability to maintain communication with hosts associated with multiple NSAPs, then it shall support Classes 1, 3, or 4 with the multihoming enhancements specified in Appendix B to Annex C. These enhancements allow a transport connection to be associated with multiple NSAP pairs and shall be used to meet the transport connection resilience requested by the transport service user.

(2) Multiaddressing. Savings in time and bandwidth can only be achieved if mechanisms are introduced into layers that inherently possess the ability to support communications to multiple destinations simultaneously (Layers 2 and 3). At present, only individual addresses can be used by the CO transport protocol and group addresses or lists of addresses are not supported by this *protocol, even in the case where such address schemes are offered by the Network Service.*

(3) Network/system management. Specific military managed objects for the Transport Layer will be specified when they are identified. They will be specified as extensions/modifications to the civilian managed objects.

(4) Security. Security deficiencies and **enhancements are for further study.**

(5) Robustness and Quality of Service (QoS). Transport Layer specifications of the mechanisms needed to respect the QoS requirements are **for further study.**

(6) Precedence and preemption. Annex C describes mechanisms for processing the priority parameter for the ICR and CC TPDU of ISO 8073 to provide for precedence and preemption.

(7) Real-time and tactical communications. The real-time transport protocol, used of a CONS, is to be defined. The real-time transport protocol, used over a CLNS is defined in Annex F (RTTS)

Source: *Draft STANAG 4264,* October 1991, NATO UNCLASSIFIED.

Annex D specifies the connectionless transport protocol, based on ISO 8602. Enhancements are the same as in Annex C with the following two exceptions:

- Multihomed and Mobile Host Systems. Since no data acknowledgement is provided by the service, the protocol is not affected when a remote host system changes its SNPA and is not reachable temporarily.
- Precedence and Preemption. Transport Layer specifications of the mechanisms involved for the management of the priority are for further study.

Annex E specifies the connection-mode transport protocol over CONS, based on ISO 8073 and ISO 8073/AD2 (*Class Four Operation Over Connectionless Network Service*) using TP4. Enhancements are the same as in Annex C with the following three exceptions:

- Multihomed and Mobile Host Systems. In the case of hosts with multiple SNPAs and a single NSAP, the protocol specified in ISO 8073 and 8073/AD1 is adequate, provided that there are automated network/system management mechanisms that manage SNPA changes and reconfigure the network service provider's routing function. Hosts that have multiple NSAPs or need to communicate with hosts having multiple NSAPs shall support the ISO 8073 and 8073/AD1 protocol, including the ability to associate a transport connection with more than one NSAP pair, as is explicitly stated in Appendix B to Annex C. The availability of additional NSAP pairs shall be used to meet the transport connection resilience requested by the transport service user.
- Precedence and Preemption. Transport Layer specifications of the mechanisms involved for the management of the priority are for further study.
- Real-Time and Tactical Communications. The real-time transport protocol is defined in Annex F.

Annex F of STANAG 4264, Real-Time Transfer Protocol Over Connectionless Network Service, is still to be defined.

15.4.5 Session Layer STANAGs

The two Session Layer STANAGs (4255 and 4265) have been developed by WG2 with the US serving as editor. Both these STANAGs have been recommended by WG2 to be distributed by SG9 for ratification without military features.

STANAG 4255 is based on ISO 8326, *Basic Connection-Oriented Session Service Definition*. Annex D is reserved for connectionless session services. The only military deficiency areas identified in the draft STANAG are for security and multi-endpoint connection:

- Security. A mechanism for providing graceful closure may be required by NATO in the long term. At present, this requirement is insufficiently refined to allow a service realization. Therefore, no enhancement of ISO security measures can be provided at this time.

- Multi-endpoint connection. ISO is currently considering multipeer data transmission requirements for the Session Layer. This activity will be monitored by the developer of this STANAG, and this paragraph will be updated as developments warrant. An enhancement requirement is contingent upon ongoing developments within ISO.

STANAG 4265 is based on ISO 8327, *Basic Connection-Oriented Session Protocol Specification*. An annex (Annex D) is reserved for information regarding the Connectionless Session Protocol Specification. The deficiencies and enhancements for STANAG 4265 are the same as for STANAG 4255.

15.4.6 Presentation Layer STANAGs

The two Presentation Layer STANAGs (4256 and 4266) have been developed by WG2. In addition, STANAGs have been drafted for ASN.1 (STANAG 4258) and the Basic Encoding Rules for ASN.1 (STANAG 4259). All four Layer 6 STANAGs have been recommended by WG2 to be distributed by SG9 for ratification without military features.

STANAG 4256 is initially based on ISO 8822, *Connection-Oriented Presentation Service Definition*. An annex (Annex D) is reserved for connectionless presentation services. Potential deficiencies have been noted in three areas:

- Security (Annex B). NOSA has placed additional security-related services in the Presentation Layer, but these are not yet defined in detail. Modifications are anticipated in the ISO standards following ISO 7498-2, which may meet the emerging military requirements. No security enhancement to the ISO Presentation Layer is currently available. However, as solutions are available this STANAG will be amended.
- Mobile hosts and multihomed systems. No deficiencies noted (subject to change dependent upon the ability of the lower layers to support this feature).
- Multi-endpoint connection. Modifications will be needed to the Presentation Layer if multi-endpoint connections are required in an implementation, but no specific requirements have yet been identified. Modifications will be made to the ISO standard once the multipeer data transmission work in ISO has been progressed.

STANAG 4266 is based on ISO 8823, *Connection-Oriented Presentation Protocol Specification*. Annex D is reserved for the connectionless presentation protocol specification. The military deficiencies and enhancements for STANAG 4266 are the same as for STANAG 4256.

Separate NATO agreements will address ASN.1 (STANAG 4258) and the ASN.1 basic encoding rules (STANAG 4259). These are based on ISO 8824 and ISO 8825. No deficiencies were found in these based standards and no enhancements are recommended.

STANAG 4259 observes that additional sets of encoding rules for ASN.1 may be required for specific applications giving either compressed (minimum volume) or encrypted

encodings. No specific requirements in this area have yet been identified. Following work in these areas by ISO, additional ASN.1 encoding rule STANAGs may be developed. A remark provided at the end of STANAG 4258 observes that ISO 8824/1 includes a note that makes reference to the encodings for the Real Type by the *Basic Encoding Rules for* ASN.1 (ISO 8825)--this note is not relevant if alternative encoding rules are to be employed.

15.4.7 Application Layer STANAGs

The only Application Layer STANAG that has been produced in draft form is the draft MMHS STANAG 4406. The status of the MMHS work is discussed in Section 15.3.8. An initial focus meeting on FTAM was planned for June 1990 (see Section 15.3.3.4).

The four-page September 1991 draft STANAG will have four annexes [Ref. Krick 1991a]:

- Annex A, *Military Message Handling System Extensions*, which provides the set of extensions to civilian message handling systems for Interpersonal Messaging Service (IPMS) required for military messaging. Annex A is also known as the Military Base Standard. This annex specifies the extensions of the texts for CCITT X.400 (ISO/IEC 10021-1), X.402 (ISO/IEC 10021-1), X.407 (ISO/IEC 10021-3), X.411 (ISO/IEC 10021-4), X.413 (ISO/IEC 10021-5), X.419 (ISO/IEC 10021-6), and X.420 (ISO/IEC 10021-7).
- Annex B, *Gateway Translations*, which provides detailed specification of the interface between MMHS and other messaging systems, including ACP systems [e.g., ACP 121 *(Communications Instructions-General)*, ACP 126 *(Communication Instructions--Teletypewriter/Teleprinter Procedures)*, and ACP 127 *(Communication Instructions--Tape Relay Procedures)*]. This current text for Annex B is very short. Preparation of Appendix B1, MMHS/ACP 127 Gateway, has been delayed until 1992 because of a decision in the AHWG-MMHS to use the Message Transfer Envelope for the gateway interface to MMHS. The current draft is provided in *STANAG xxxx: Military Message Handling System*, Working Paper (Clean Version), 11 June 1991, NATO UNCLASSIFIED.
- Annex C, *Security Aspects of MMHS*, which identifies the service, protocol, and operational requirements related to security. At present, this annex is empty. It would eventually be classified NATO SECRET.
- Annex D, *Functional Profiles*, which provides a set of profiles, based on and extended from the set developed by EWOS and ETSI, which provide full MMHS functionality. One profile set has been completed, the ALPHA Profile Set. As noted in Section 15.3.8, this profile specifies changes ("deltas") to the six EWOS MHS profiles of May 1991 (A/3311-13 and A/3321-23). The current draft Alpha Profile Set is provided in Annex C of *STANAG xxxx: Military Message Handling System*, Working Paper (Clean Version), 11 June 1991, NATO UNCLASSIFIED.

Table 50 identifies the military features as they affect MMHS. Previous editions of the MMHS draft STANAG have included additional material on Scenarios *and Rationale,* which provided detailed specification of the scenario of application, rationales behind the major decisions, and discussion of the support of the subset of the eight military features that are applicable to a store-and-forward messaging environment. This document is now being prepared separately. The intent is to have an excerpt from this document included in the 1991 edition of the MMHS STANAG, but this has not yet been done. [Ref. TSGCE 1991h]

WG2 plans to submit draft STANAG 4406 with the Military Base Standard (Annex A) and the ALPHA Profile Set (Annex D) to TSGCE SG9 in December 1991 for distribution and recommendation for ratification.

Table 50. Status of X.400(MHS)-1988 Relative to the Eight Military Features

(1) Multihomed/Mobile Host

(a) Multihoming applies to MMHS applications in two ways: multihoming UAs and multihoming MTAs. In the first case, the MHS must allow a single user to have more than one Originator/Recipient (O/R) name. The second case requires MTAs that answer to more than one name. In both cases, the capability in question is outside the scope of the communications standards, but is permitted as an implementation option. Capabilities for multihoming would have no direct impact on either MHS services or protocols, but.are instead more focused on the lower layers.

(b) Similarly, mobile hosting can also be applied to either the MTA or UA. In either case, the key requirement to support mobile hosting is the capability for the functional object in question to disconnect from the network for a period of time without serious consequence. In MMHS there are two mechanisms to support mobile hosting of the UA. One such mechanism is the use of a message store (MS) to act on the UA's behalf while the UA is off line. The second mechanism is use of the Hold for Delivery element of service, in which the service element instructs the MTS to defer delivery of a UA's messages until a later time. No such mechanisms are available to the MTA, however.

(2) Multipeer Data Transmission (MPDT)

Since MHS applications are store and forward (i.e., connectionless) in nature, no end-to-end connections are provided or required by MMHS. However, the MMHS does provide a connectionless MPDT capability in the form of multi-addressed messages. This feature allows a single message to be sent to several recipients with a single submission to the MTS. The MTS is then responsible for performing traffic splitting at the appropriate time. Note that traffic splitting could be substantially more efficient if supported by a lower layer MPDT function.

(3) Internetworking

Internetworking is addressed by the provision of MMHS/ACP 127 and MMHS/civilian gateway definitions. Gateways could also be created to other systems that perform similar message handling functions, but such gateways are at present beyond the scope of MMHS.

(4) Network and System Management

Network management is a pan-layer issue that falls under the auspices of the AHWG-OM in SG9. The AHWG-MMHS will continue to identify MHS-related topics to be considered by AHWG-OM.

(5) Security

Security is a pan-layer issue that falls under the auspices of the AHWG on Security in SG9. The AHWG-MMHS will continue to identify MHS-related topics to be considered by the Security AHWG.

Table 50. (Continued)

(6) Robustness and Quality of Service (QoS)

Most aspects normally associated with robustness and QoS have no meaning in the Application Layer. Three MHS characteristics have been identified as significant in terms of robustness and QoS: loss of messages, end-to-end delivery time requirements, and selection of security services. QoS aspects relating to link quality, hop-by-hop transmission delay, and throughput are primarily lower layer issues, and in any case have little meaning for a store-and-forward Application Layer process.

(a) Loss of message is addressed by the MMHS expansion of X.400's redirection capability. This provides a dead letter box at each MTA so that messages will always be delivered rather than discarded. MMHS also provides both delivery and nondelivery receipt capability to provide additional assurance of delivery.

(b) MMHS has specified end-to-end delivery time requirements consistent with those used by ACP 127. The hop-by-hop transmission delay and throughput necessary to achieve those end-to-end times are lower layer issues.

(c) Selection of appropriate security services is largely dependent on the security policy in force. This policy will determine what services will be enabled during the origination of a message based on its classification or other factors. This selection could be done either technically or procedurally, however, and thus is purely an implementation issue. Whatever solution is used will impact only the originator and will not require changes to the communication protocols.

(7) Precedence and Preemption

The established requirement for military priority in message handling is four levels based on ACP 127. The MMHS base standard provides six priority levels in all protocols necessary to support the use of precedence and preemption in any implementation. However, it is the intent of the AHWG-MMHS to develop functional profiles that support six levels of priority in the UA-to-UA protocols but only three levels in the corresponding MTA-to-MTA protocols. Use of these provided information elements to support precedence and preemption in either the UA or MTA is an implementation issue.

(8) Tactical and Real-Time Communications

MMHS has specified end-to-end delivery time requirements that are purported to represent the tactical environment. In addition, the AHWG-MMHS plans the development of a *Beta Profile* tailored to low bandwidth tactical applications.

Source: *Draft STANAG on Military Message Handling System*, 16 February 1990, NATO UNCLASSIFIED.

15.5 Development of Other Technical STANAGs

This section identifies non-OSI STANAGs that appear to be relevant to CCISs. Media-dependent STANAGs (e.g., tactical data links) are not addressed.

15.5.1 Network Independent Interface (NIIF)

NIAG SG6 is developing a draft specification of a Network Independent Interface (NIIF). This was briefed to the TSGCE SG9 AHWG-OM in February 1989. NIIF is a concept for a combat system data distribution interface that could be used by the NATO Frigate Replacement for the 1990s (NFR90), a programme currently in a project definition phase.

In a subsequent joint meeting with the NIAG SG6 and TSGCE SG9/WG1 in June 1989 [Ref. NIIF 1989], the NIIF was identified as a project to (1) put NACISA in the lead to resolve interface problems and provide management structure for such projects; (2) provide near- and mid-term standards specification for ACCIS interoperability; (3) initially

develop interface specifications to pass character-oriented messages between existing systems; and (4) evolve the specification so that it will be suitable for other services (e.g., file transfer, virtual terminal). The specifications were to be based on ISO OSI standards and on functional profiles of SPAG and CEN/CENELEC that are adopted in the *NTIS Transition Strategy*: T.21 Permanent Circuit (telephonic), T.22 Switched Circuit (telephonic), and T.31 Permanent Access to a PSDN. BID-1000 and KG-84 were identified for communications security. The message handling area was based on A/3211 from the EWOS.

As early as September 1987, NIAG SG6 proposed a draft STANAG for *NATO Naval Intra-Ship Tactical Control and Data Handling Open Systems Interconnection, Network Independent Interface, Transport Service Definition for Connection-Mode Transmission* [Ref. NATO 1987a]. This proposal was based on ISO 8072 with "additions and deletions, where necessary, to reflect a unique Naval, intra-ship, interpretation to it." The NIIF is identified in this proposal as a collection of standards that provide the complete definition of an interface between the User and the Data Transfer System, based on unique requirements for real-time, fault tolerant information exchange between peer systems. Reference 280 provides a statement of the programme of work planned by NIAG SG6 for 1990-1992.

15.5.2 Lightweight Protocols

The TSGCE AHWG on Restructuring has noted that the work of NIAG SG6 is closely related to the work of TSGCE SG9 on OSI standards. Both groups are interested in the area of lightweight LAN profiles for multi-Service use. The basis for the intraship LAN profile being developed by NIAG SG6 is based on France's GAM-T-103, as is the US SAFENET profile and the more general Express Transfer Protocol (XTP) profiles [Ref. AHWG-OM 1990].

The Xpress Transfer Protocol (XTP) is a lightweight (providing simplicity and low overhead) transfer protocol with unified internetwork services associated with OSI Layers 3 and 4. XTP conforms to the architecture of the Transfer Layer in RTTS developed in France for use in LANs (see Section 15.4.4) [Ref. GAM 1987]. XTP is designed to support 100 Mbps sustained transfer rates between application programs with growth to 1 Gbps. XTP is designed to provide services for distributed systems not available in ISO TP4 and US DoD TCP; the requirements include supporting remote procedure calls and rapid request/response operations, coordinating multiple processes, and providing transaction-based file access. XTP supports traditional stream services, bulk transport, real-time reliable datagram service, real-time internet gateways, flow/error/rate control, message delivery confirmation, selective retransmission, message boundary preservation, multiple addressing plans, out-of-band signalling, reliable multicast mechanism, maintenance packets, and multipath capability [Refs. XTP 1988, XTP 1989].

XTP has been submitted to ANSI X3S3 for standardization of its services. Its standardization is also being progressed in the US Navy SAFENET Committee.

15.5.3 EUROCOM and US/EUROCOM

EUROCOM. EUROCOM is a technical working group composed of representatives from the NATO European nations whose aim is to achieve better coordination and interoperability in tactical communications systems between European Allied armies. EUROCOM is a subgroup of the EUROGROUP, an informal grouping of European governments within the framework of NATO. Rather than trying to agree on a single system, it is EUROCOM's plan to introduce communications systems in accordance with agreed operational requirements and basic system parameters in such a way that there is complete interoperability among systems built to EUROCOM standards. EUROCOM standards are frequently offered as the basis for NATO STANAGs on tactical communications [Ref. Manno 1989].

The documents (D) currently promulgated by EUROCOM include:

- EUROCOM D/0: *System Concept*, CONFIDENTIAL (date of last revision unknown)
- EUROCOM D/1: *Tactical Communications Systems Basic Parameters*, 1986 (Revised September 1988), RESTRICTED
- EUROCOM D/2: (title and date unknown) subject is testing.

US/EUROCOM. US/EUROCOM is an informal tactical communications technical working group comprising the EUROCOM nations and the United States, Canada, and France. The purpose of US/EUROCOM is to work toward better and less cumbersome interface arrangements, to monitor the implementation agreements on communications characteristics, and to promote cooperation in the procurement of equipment conforming to these characteristics. Much of the preliminary technical work leading to ratified standardization agreements is accomplished by this group.

With respect to work in OSI, the principal interest in US/EUROCOM is with the lower three layers. Currently, US/EUROCOM is in the process of modifying STANAG 4249, *The NATO Multi-Channel Tactical Digital Gateway--Data Transmission Standards (Packet Switching Service)*, to reflect the 1988 version of CCITT Recommendation X.75. US/EUROCOM is also investigating the application of the protocol implementation conformance statement (PICS)-type proformas to the NATO multi-channel tactical digital gateway STANAGs [Ref. Manno 1989].

On many occasions US/EUROCOM has accepted invitations from TSGCE to work on the NATO STANAGs for tactical communications (not just gateways) and interoperability issues. US/EUROCOM has made major contributions to STANAGs 4206-4211 and 4350. Both EUROCOM and US military standards are being considered for drafts of STANAG 4290, *Fiber Optics*. In each case the technical recommendations from

US/EUROCOM are provided to TSGCE SG11 WG1 for further work, coordination, and distribution as draft STANAGs.

The work of US/EUROCOM in developing a profile for a tactical gateway for packet switching (STANAG 4249) was briefed the TSGCE SG9/WG1 in the October 1989 meetings in Brussels. In addition, Norway provided a paper that suggested US/EUROCOM could undertake several tasks of interest to SG9. These include proposing protocol implementation conformance statement (PICS) proformas for the STANAG 4206-4214 series (and possibly others, such as STANAGs 4290 and 5040); proposing tactical parts of the STANAG 4250 series; identifying profiles required by the tactical communities in NATO; and proposing NATO functional profiles for tactical applications. However, US/EUROCOM's role in developing profiles for NATO is still under consideration and has not been fully accepted by US/EUROCOM. [Ref. TSGCE 1991i]

15.5.4 Other Efforts

STANAG 4214, *International Routing and Directory for Tactical Communications,* may be applicable to ATCCIS technical standards; this standard is the responsibility of TSGCE SG11. TSGCE SG9/WG1 is looking at naming and addressing requirements and the applicability of STANAG 4214. STANAG 4249, *The NATO Multichannel Tactical Digital Gateway--Data Transmission Standards (Packet Switching Service),* also the responsibility of SG11, addresses packet switching using a form of CCITT X.25; as such, this STANAG may also be applicable to ATCCIS technical standards. The Eurogroup on Cooperation of Tactical Communications Systems (EUROCOM) is reported to be preparing a revised draft for STANAG 4249 based on CCITT X.25 and the draft TSGCE SG9 Functional Profile Guidelines document; such a draft would be submitted to SG11 as a contribution and developed into a STANAG.

15.6 Assessment

a. TSGCE has identified and assessed eight military features that need to be incorporated in civil OSI standards, but little detail has yet been released (e.g., in drafts of STANAGs 4251-4266) to show how these features can actually be addressed in military versions of OSI standards. There does not seem to be much value in a set of layer STANAGs that primarily catalogue ISO and CCITT standards.

b. TSGCE SG9 has an ambitious 18-month plan for progressing the NATO OSI data communications standards, but there is a need to reassess and revalidate the military features--clearly the deficiencies of 1991 civil standards are different from those identified in 1983. For example, great progress on internetworking has been made in ISO.

c. TSGCE SG9 has been successful in many areas (such as security and OSI management) for introducing military work into the civil standards bodies and affecting the capabilities of the civil standards. One of the useful approaches being taken by SG9 is the

focus on the applicability and adequacy of civil profiles for use in NATO by addressing specific military scenarios and groups of requirements. Profile-oriented work is essential to ensure interoperability of implementations by the Nations. It is clearly the focus of the reorganization of SG9 that will be evolved in 1992. Current efforts on profiles need to be supported and expanded. This work should be in close coordination with the regional implementor's workshops (e.g., EWOS and the North American OIW), since NATO cannot afford to implement on a wide scale major variations of the profiles negotiated in the civil communities.

(This page intentionally left blank.)

16. NEAR-TERM INITIATIVES AND SYSTEMS FOR ACHIEVING INTEROPERABILITY IN NATO

Quick Reference	
Topic	Page
ACE ACCIS	360
ACCS	362
AHWG on ATCCIS	359
BICES	365
NMOS	365
PG6-Tac Comms 2000+	355
Quadrilat Interop Prog	366
STAMINA	367
TSGCE SG11	354
TSGCE SG12	355

TSGCE is developing recommendations and standards in two areas, in addition to the work of TSGCE SG9 on Data Distribution (described in Chapter 15), that could have significant impact for CCISs. These are SG11 on Communications and SG12 on Information Systems.

Existing and emerging ACCISs are designed to provide command and control information support for NATO and national systems. The ACE ACCIS will provide the higher-echelon support (i.e., at echelons above corps) for the military forces operating in the European region of NATO. ATCCIS will provide support for land combat tactical units, and the Air Command and Control System (ACCS) will support the air operations.

The NATO Maritime Operational Intelligence Support (NMOS) and the Battlefield Information Collection and Exploitation Systems (BICES) will provide intelligence support. Other ACE ACCIS -related projects include the Standard Automated Message Interface for NATO's ACCISs (STAMINA), JRMS, the Status Control Alerting and Reporting System II (SCARS II), and the Nuclear Planning System (NPS).[66]

This chapter begins by reviewing the work or TSGCE SG11 and SG12 (Section 16.1). It further examines the standards specified by near-term NATO and multilateral interoperability demonstration and development efforts in addition to ATCCIS, namely the ACE ACCIS (Section 16.2), ACCS (Section 16.3), BICES (Section 16.4), NMOS (Section 16.5), the Quadrilateral Interoperability Programme (Section 16.6), and STAMINA (Section 16.7).[67] Military features required by NATO are addressed. In addition, this chapter addresses some of the issues associated with evolving from near-term systems to ATCCIS through the use of standards. Profiles of standards that are to be used in transition implementations for several NATO projects are also presented.[68]

---

66 ACCS, ATCCIS, BICES, JRMS, NMOS, NPS, and SCARS II are the seven ACE CCIS-related projects identified in the *ACE Inventory of Key Tasks*, December 1988, NATO CONFIDENTIAL.

67 The information provided in Section 16.2 through 16.7 was reviewed and updated by SHAPE staff in January 1992.

68 Profiles differ from stacks in that a profile usually consists of several stacks of standards and further that profiles are usually recommended for a certain transition strategy or a specific implementation. In some cases, profiles specify options to be used.

The objective of this review is to ensure that the methodology used for the ATCCIS effort is comprehensive and that no classes of relevant standards have been overlooked. Some national initiatives to adopt and extend OSI standards for tactical employment are reviewed in Appendix C.

16.1 TSGCE Work on Communications and Information Systems

16.1.1 Work of TSGCE SG11 on Communications

TSGCE SG11 on Communications (1) promotes collaboration amongst the nations on projects to develop and produce common equipment and systems in the area of communications and (2) prepares required technical STANAGs for communications systems and equipment. The goal is to promote and achieve interoperability between national and NATO-funded systems, both tactical and strategic.[69]

16.1.1.1 Organization of SG11

At the November 1991 plenary of SG11, SG11 reviewed and approved the terms of reference and special tasking instructions for its subgroups and subordinate bodies. The organization of SG11 is as follows [Ref. Pilla 1991]:

- WG1 on Tactical Area Communications, which identifies interface requirements and prepares draft new or modified tactical area communications STANAGs in the areas of terminal, multiplexing, switching, and multi-channel radio equipment as well as interface gateways and devices among tactical systems, strategic systems, and commercial systems.
- WG2 on Narrow-Band Speech, which investigates possible speech techniques in order to achieve high quality (under adverse acoustical conditions) of reproduced voice in as narrow a frequency band as possible.
- WG3 on Tactical Communications Equipment for Use in the Maritime Environment, which identifies interface requirements and prepares draft new or modified STANAGs for secure submarine, air, and surface communications capabilities.
- WG5 on Single Channel Radio Systems, which identifies interface requirements and prepares draft new or modified STANAGs in the areas of single channel and combat net radios.
- WG8 on Satellite Communications Systems, which identifies interface requirements and prepares draft new or modified STANAGs in the areas of satellite communications.

---

[69] The information presented on the work of SG11 is very general. This is because more detailed information, including the special tasking instructions, reports of meetings, and most of the formal correspondence regarding SG11 is being classified as NATO RESTRICTED by the NATO Secretariat. Only material available at the unclassified level and appropriate for wide dissemination has been used.

- PG6 on Tactical Communications Systems for the Land Combat Zone--Post 2000, which is developing technology assessments, an agreed tactical communications architecture, a transition strategy, and standards.
- PG8 on Tactical Spectrum Management System, which is defining a NATO tactical spectrum management architecture and identifies opportunities to harmonize current systems.

16.1.1.2 Activities of the Working Groups

SG11/WG2 is planning tests for low-rate speed coders and will report results in 1992. Planning for testing other voice coders and error correction devices will be conducted in 1992.

SG11/WG5 is developing a STANAG for HF/ECCM; the initial draft for circulation to the nations is planned March 1992. Work has begun on VHF ECCM; a draft STANAG is being considered for VHF interim interoperability using gateways for analog voice. Other areas of interest to WG5 are HAVE QUICK II radios and SATURN radios (STANAG 4372) and the requirements for NATO Improved Link Eleven (NILE). WG5 reviewed STANAGs 4203, 4204, and 4205 in 1991 and will review STANAG 4202 in 1992.

Canada, France, Germany, the United Kingdom, and the United States have signed an MOU for work in SG11/PG8 on the Tactical Spectrum Management Program. Spain is also considering joining this program. [Ref. Howe 1991]

16.1.1.3 Work of PG6 on Post-2000 Tactical Communications[70]

The objective of the work of SG11/PG6 is to seek, through a coordinated program, tactical communications systems designed to common standards, to include collaborative work on subsystems and standards development, where appropriate. The result of the common standards and collaborative work on subsystems is expected to be the achievement of progressively enhanced interoperability.

PG6 has been working in seven areas: architecture, switching, communications media, mobile systems, terminals, system management, and security. This work was divided into three phases--planning, study, and integration--and has resulted in a description of the recommended post-2000 architecture, supported and justified by a number of detailed technology studies. Areas for standardization have been identified. The final product is the *Phase I Final Report* [Ref. TSGCE 1991j], which includes:

- An operational and architectural framework for tactical communications systems for the land combat zone in the post-2000 time frame
- A list of standards and areas for standardization work within this framework

---

[70] Material in this section is based on a private communication with Sal Manno (US Representative to PG6), JTC3A, 9 December 1991.

- Proposals for the next stage of work.

The framework takes into account national and NATO military operational requirements and the SHAPE concept[71] for tactical communications in support of land operations. It is based on several pre-feasibility studies done by the NIAG (completed in 1990) and under a multinational MOU.[72] It describes the preferred architecture and identifies essential system (interoperability) parameters. Figure 10 in Chapter 4 depicts one of the key components of the architecture.

The report identifies standards and areas for standardization required for equipment development according to the preferred architecture. PG6 identifies the existing STANAGs that fit the architecture, the existing STANAGs that may need modification, and areas for standardization in which new STANAGs or other standards will need to be written.

The next phase of work encompasses defining the architecture in greater detail, to include the functional and performance aspects, in order to reach the level of detail needed to prepare the STANAGs, as well as the system- and subsystem-level specifications. In addition, PG6 is planning on a limited number of studies to enhance the base knowledge in rapidly changing or new technologies applicable to communications. The products for 1992-93 are expected to include (1) elaboration of the agreed architecture in more detail and (2) confirmation of the transition strategy. For the period 1994-1997, the emphasis in PG6 will be on the development of standards for the post-2000 era.

SG11 has agreed that PG6 be given the systems engineering responsibility for all SG11 work related to the PG6 tactical communications system architecture and that SG11 manage all the SG11 work and schedules within the framework of that architecture. The overall concept was endorsed by SG11 in November 1991, and PG6 was requested to provide a comprehensive work plan for submission to SG11. [Ref. Manno 1991a]

SG11 has been asked by the TSGCE to provide a schedule at the January 1992 TSGCE plenary for the completion of two CNAD tasks: (1) interoperable communication links for tactical headquarters and (2) interconnection of tactical and strategic communications systems. SG11 has also been asked by the TSGCE to assist in expediting agreements necessary to make HAVE QUICK IIA algorithms available to SATURN radios and to respond to a Conventional Armaments Plan tasking for a second generation ECCM UHF program (and report to the TSGCE in June 1992). [Ref. Howe 1991]

---

71 Only drafts of the concept were completed during the first phase of the PG6 architectural work. These drafts have now been withdrawn and a new tactical communications concept is in preparation. When completed, ATCA intends to work on a military operational requirement based on the tactical communications concept.

72 The 1991 participants in the MOU were Canada, France, Germany, Italy, the Netherlands, Norway, Spain, the United Kingdom, and the United States. The MOU covers a number of pre-feasibility studies that extend the work completed by the NIAG. Portugal as indicated interest in joining the MOU for work in 1992.

16.1.2 Work of TSGCE SG12 on Information Systems[73]

TSGCE SG12 on Information Systems (1) actively promotes and enables collaboration amongst the nations of the Alliance on projects to develop and produce common equipment and systems in the area of information systems and (2) provides technical standards in the area of information systems. The goal is to promote and enable the achievement of interoperability between and among national and NATO-funded CCISs, both tactical and strategic. SG12 has two subordinate bodies, which will establish a close working relationship with each other:

- WG2 on Data Processing and Management, which will recommend standards on data processing and security with ADP systems.
- AHWG on an Army Tactical Command and Control Information System (ATCCIS), which is emphasizing data management and exploiting the Phase I and Phase II technical work on a standards-based architecture during 1984-91 by France, Germany, the United Kingdom, and the United States.

Two other TSGCE groups, originally assigned to SG12 during the initial work on TSGCE restructuring, have now been directed by the TSGCE to continue reporting directly to the TSGCE. They are the Project Group (PG7) on BICES and the Special Working Group on AdaProgramming Support Environment (APSE) (this group had been renamed Working Group on Software Engineering when it was considered part of SG12). Eleven nations have been participating the the MOU on BICES and two others are expected to join. The Working Group on Geographic Information Systems, initially assigned to SG12, has been transferred to the Military Agency for Standardization (MAS).

16.1.2.1 WG2 on Data Processing and Management

Table 51 shows the special tasking instructions for WG2 that govern its work. The initial program of work for SG12/WG2 is as follows [Ref. TSGCE 1991m]:

- Data Management Reference Model (DMRM) and Architecture
  - Monitor the status of work in ISO and other relevant international standardization groups
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging NATO Data Management Policy.
  - Determine, by reference to recognized user representatives at the strategic and tactical levels, the requirements for the NATO DMRM and architecture.
  - Identify the possible options for the selection of a NATO DMRM and architecture and make appropriate recommendations.
  - Timescale and milestones are to be determined; lead nation is France.

---

[73] This section is based on the *Report to the Tri-Service Group by the Chairman of the Subgroup on Information Systems*, AC/302(SG/12)D/7, 21 November 1991, NATO UNCLASSIFIED.

- Data Models
  - Monitor the status of work in OSI and other relevant international standardization groups.
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging NATO Data Management policy.
  - Determine, by reference to recognized user representatives at the strategic and tactical levels, the requirements for data models and in particular make recommendations as to the number and type of distinct models required.
  - Determine the requirements for the production (by others) of an initial data model(s) and for subsequent maintenance of that model(s).
  - Identify a suitable set of software tools and aid packages to assist in the creation and maintenance of such models, and make appropriate recommendations.
  - Timescale and milestones are to be determined; lead nation is the United Kingdom.
- Data Dictionaries
  - Monitor the status of work in ISO and other relevant international standardization groups.
  - Determine, by reference to recognized user representatives at the strategic and tactical levels, the requirements for data dictionaries.
  - Determine the requirements for the reproduction (by others) of an initial data dictionary from the NATO Data Model(s) and for subsequent maintenance of that dictionary.
  - Identify the possible options for the selection of a NATO standard for data dictionary definition, and make appropriate recommendations.
  - Define the structure of a NATO data dictionary using an appropriate meta-language.
  - Identify a suitable set of software tools and aid packages to assist in , or to automate, the process of converting a data model into a set of data definitions for incorporation into a NATO data dictionary.
  - Be prepared to respond to specific queries by the provision of technical advice to staff responsible for the management of the NATO data dictionary.
  - Timescale and milestones are to be determined; lead nation is the United Kingdom.
- Data Definition and Data Schemata
  - Monitor the status of work in ISO and other relevant international standardization groups.
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging Data Management Policy.
  - Determine by reference to recognized user representatives at the strategic and tactical levels, the requirements for data schemata.
  - In consultation with appropriate NATO and National Staff, determine the requirements for the production and subsequent maintenance of data schemata.
  - Identify a suitable set of software tools and aid packages to assist in, or to automate, the process of generating data schemata from a NATO data dictionary, and make appropriate recommendations.

- Be prepared to respond to specific queries by the provision of technical advice to staff responsible for NATO projects.
- Timescale, milestones, and lead nation are to be determined.

- Data Access and Manipulation Standards
  - Monitor the status of work in ISO and other relevant international standardization groups.
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging NATO Data Management Policy.
  - Identify the possible options for the selection of NATO standard access and manipulation languages, and make appropriate recommendations.
  - Identify software tools and aid packages appropriate to assist, or to automate, the generation of applications from initial analysis and outline definition of functional requirements (CASE tools), in conformity with the standards recommended. (This activity is seen as providing guidance and is not to be taken to imply that the Working Group will endorse any particular products nor undertake any form of market survey.)
  - Timescale, milestones, and lead nation are to be determined.

16.1.2.2 AHWG on ATCCIS

The SG12 AHWG on ATCCIS held its first meeting on 4 June 1991. The meeting was organization and focused on the relation of the existing ATCCIS groups (specifically the Permanent Working Group and its two subordinate groups, the Operational Subgroup and the Technical Subgroup). It was noted that the Operational Subgroup is currently meeting (with additional national participation from Canada and the Netherlands) as an ad hoc working group under the Operational Procedures Working Party of the MAS Army Board. One suggestion was that the AHWG on ATCCIS similarly meet with all interested national participation simultaneously with the existing ATCCIS Technical Subgroup, which would avoid creating a new standards body and resulting overlapping efforts. In September 1991, the TSGCE noted a recommendation that SHAPE retain operational sponsorship of ATCCIS, that the existing ATCCIS groups remain in effect, and that a relationship between ATCCIS and the TSGCE be established. The terms of reference for the AHWG on ATCCIS, as well as the terms of reference for SG9, SG11, SG12, and their subordinate bodies, will be reviewed by the TSGCE in January 1992. [Ref. Howe 1991]

The proposed tasks of the AHWG on ATCCIS are to [Ref. ATCCIS 1991]:

- Assist the TSGCE in identifying standards or standards parameters required for interoperability of tactical land force ACCIS as identified in the ATCCIS effort.
- Review and coordinate ATCCIS working papers for TSGCE acceptance and promulgation.
- Document and address key technical standards issues attendant to the emergence of ATCCIS conformant systems.

Table 51. Proposed Tasking Instructions for SG12/WG2 on Data Processing and Management

1. The working group shall adopt the following definition of Information Systems for the purpose of defining the scope of its activities: Data processing systems which are used in support of C3I processes within NATO and the nations, excluding embedded systems within sensor systems and weapons platforms. The requirements of development systems (for developing hardware and software) shall be excluded from the scope of the Working Group.
2. The Working Group shall work in close association and harmonization with the SG12 Working Group on Software Engineering.
3. The Working Group shall ensure that all STANAGs developed by the Group are based to the great est extent possible on existing or emerging civilian standards.
4. The Working Group is required to undertake the following tasks:
   a. Maintain a corporate up-to-date knowledge of present and planned NATO and national data processing and management systems.
   b. Identify, review, and prioritize the requirement for standards for data processing and management systems.
   c. Take account of related activities in NATO and in particular the activities of TSGCE SG9 and its subsidiary bodies; AC/317, including ISWG, ADSIA, ACCSA, and NACISA; AC/35; STC; DRG; Inter-Service Geographic Working Group; and establish effective means of liaising with these and other bodies, both within and outside NATO (such as ISO), so as to establish prioritized requirements and avoid duplication of effort and activities.
   d. Identify and review existing and emerging standards for data processing and management systems to enable it to make recommendations for the adoption or enhancement of these standards for collaborative NATO and national projects, consistent with meeting the identified minimum military requirement and in accordance with authoritative advice and policy on security matters from AC/35 and ACCSA.
   e. Develop STANAGs, in accordance with these recommendations, to ensure interoperability of NATO and national data processing and management systems.
   f. Promote measures for improving the efficiency of, and reducing the cost of, the procurement, operation, and maintenance of NATO and national data processing and management systems including, where appropriate, the development of STANAGs.
5. The Working Group shall report at regular intervals to SG12 and produce a forward plan of work for agreement by the Subgroup. This work plan is to identify both the areas of interest of the Working Group and the documents which will be produced as deliverable outputs to the Subgroup.

Source: *Tasking Instructions for the Working Group on Data Processing and Management*, Appendix 2 to Annex III to AC/302-D/616, *Report to the Tri-Service Group by the Chairman of Subgroup on Information Systems*, AC/302(SG/12)D7, 21 November 1991, NATO UNCLASSIFIED.

16.2 ACE ACCIS

The term "Allied Command Europe--Automated Command and Control Information System" (ACE ACCIS) reflects the intended aim of a common ACCIS architecture to be applied in a uniform way across ACE, that is, to provide automation support for NATO Headquarters at echelons above corps.

Architectural Design Study. A major ACE command and control information system study was conducted between March 1980 and 1982 which was called the ACE Architectural Design Study (ADS). The aims of the ADS were to:

- Identify those command and control related activities of the ACE headquarters which lend themselves to ADP support
- Consider the additional requirements of interfaces to national systems, communications and resources
- Define an ADP architecture which provided the required support to command and control in the "most operational and cost effective way"

- Define an implementation strategy to provide early implementation at an acceptable cost and effort.

System Design and Integration Contract. The system definition project for the ADS was known as the System Design and Integration Contract (SD&IC). The contract was let to a multi-national consortium and was originally planned to cover the period 1989-late 1991. Although the study was ACE wide it concentrated on SHAPE and the Central and Southern Regions, taking account of the need for interoperability, economy and manpower. The SD&IC attempted to develop, as far as possible, a common system design for ACE ACCIS.

The SD&IC had two major objectives: (1) to complete the system architecture for ACE ACCIS and (2) to prepare for the next generation of ACE ACCIS nodes in SHAPE, and the Central and Southern Regions.

Due to unforeseen difficulties the SD&IC fell behind in time scale and budget, which when combined with a changing political and military situation, resulted in some of the products no longer meeting the "current" situation.

The difficulties experienced in concluding the SD&IC resulted in the contract being terminated before completion and the emphasis being placed on evolutionary acquisition of ACE ACCIS as defined in the ACE ACCIS Implementation Strategy (AAIS) of December 1991, which defines the implementation of individual ADP systems building towards an agreed architecture.

STC Testbed Laboratory. STC has developed a testbed laboratory[74] designed to demonstrate concepts for ACE ACCIS and other headquarters information systems (HISs). Initially the testbed provides a message handling network interconnecting headquarters units that have very different message and decision support functionality. Some units are assumed to be limited to generation and display of message text formats, while others are capable of storing messages in command databases and exchanging decision support data (such as graphics displays). The testbed is based on commercial off-the-shelf products (e.g., SUN, UNIX, and X-Windows) and is capable of [Ref. STC 1991a]:

- Message handling over NATO TARE and OSI networks
- Support of generic user functions such as briefing contributions and message processing
- Interoperability with other CCISs, including transfer of decision support data.

The network for these capabilities is the NATO TARE wide area network supported by a SHAPE Information Flow (SHIF) gateway to workstations, personal computers, and

[74] The testbed laboratory is, in part, an outgrowth of an ATCCIS Testbed developed by STC in support of the ATCCIS program.

other command and control systems [e.g., Limited Operational Capability--Europe (LOCE)].

STC is using for its laboratory two prototype CCIS configurations. The War Headquarters Information Dissemination and Display System (WHIDDS) is installed in the SHAPE bunker command room to interconnect the staff cells with a central Headquarters database (based on DEC-VMS, DECNet, and FORTRAN 77). Another system, LENA-2, was developed at STC and is being maintained by SHAPE. An integrated CCIS, LENA-2 is designed to support the Alternate War Headquarters (AWHQ) or other HQ CCIS requirements. LENA-2 is based on SUN, UNIX, and X-Windows. Interoperability for the testbed laboratory is via X.400 and ADatP-3 messages.

16.3 Air Command and Control System (ACCS)

The Air Command and Control System (ACCS) is a system to support air operations planning, tasking, and execution throughout ACE from Major NATO Command (MNC) level to combat unit level.[75] ACCS will interface with the ACE ACCIS at the Principal Subordinate Command (PSC) and Allied Tactical Air Force (ATAF) and will concentrate on new development at the PSC and below. ACCS will progressively replace a current federation of individual systems that support ACCS functions to varying degrees.[76] At the PSC level and above, ACCS functions will be performed by the ACCIS of each Command.

Development of ACCS, which integrates offensive and defensive air command and control functions, has been underway for several years. Implementation is planned to begin in the early 1990s. In April 1989, the ACCS Team completed the ACCS *Master Plan*. The ACCS Team was replaced by the ACCS Interim Management Group and later by the NATO ACCS Management Agency (NACMA). NACMA is conducting a system definition phase. The goal is preparation of system specifications and technical estimates by 1993 to support subsequent procurement of system entities.

Several levels of operational capability (LOC) are being defined for ACCS. LOC1, the first level of interoperability, is planned for the 1997 timeframe. MIDS/Link 16 is an inherent feature of the ACCS design and will be integral to LOC1. ACCS will use Link 16 for ground-air-ground tactical data exchange communications and Link in Support of ACCS (LISA, formerly called Link 1 replacement) for ground-to-ground bit-oriented data exchange. NACMA is coordinating the introduction of MIDS/Link 16 into ACCS and has

---

75 The seven ACCS major functional areas are: Force Management (FM), C2 Resource Management (C2RM), Airspace Management (AM), Surveillance (S), Air Mission Control (AMC), Air Traffic Control (ATC), and Information Exchange.

76 The systems include Improved United Kingdom Air Defense Ground Environment (IUKADGE), Systeme de Traitement et de Representation des Informations de Defense Aerienne (STRIDA), German Air Defense Ground Environment (GEADGE), and NATO Air Defence Ground Environment (NADGE).

initiated a study on the operational, technical, and financial implications of the implementation of Link 16 in ACCS. [Ref. Maes 1991]

The interoperability concept for ACCS is discussed in Volume IV, *Generic Portion of the Overall* ACCS *Design*, of the ACCS *Master Plan*, [Ref. ACCST 1986], and in the *Supporting Document on Organization Components* [Ref. ACCST 1988]. ACCS interoperability is planned through exchange of information through commonly agreed information definitions, formats, and technical standards. Where possible, the standards to be used are those developed by the Military Agency for Standardization (MAS), ADSIA, and TSGCE SG9. Specifically, ACCS will be based on the OSI Reference Model as specified in STANAG 4250 (NATO Interoperability Model), the OSI services for Layers 1 through 7 as specified in STANAGs 4251-4257, and the OSI protocols for Layers 1 through 7 as specified in STANAGs 4161-4267. In addition to the ISO Reference Model standards, the NATO Common Interface Standards will be used. TSGCE SG9 is responsible for the OSI technical standards, and ADSIAis responsible for the procedural standards. Operational interoperability standards will be based, in part, on Allied Tactical Publications (ATPs).

The ACCS communications concept is to integrate the various NATO and national dedicated communications systems currently used to support air operations into a common user data and voice network. ACCS would be hosted on the existing and planned communications without ACCS-unique communications means. Initially a packet switched data communication overlay would be added to the circuit-switched voice system. Continued support for both character-oriented and bit-oriented messages is required. Specifically, use of tactical data link standards such as Link 4, Link 6, Link 11, Interim JTIDS Message Standard (IJMS), and Link 16 would continue through the foreseeable future.

ACCS has been reviewing technical information exchange standards and requirements, including the need to replace Link 1 for data exchange[77] in the ground environment. The current approach is to base a new standard on STANAG 5516 (J-Series messages) and to develop (within ADSIAWG4) new or modified messages to fulfill specific ACCS Information Exchange Requirements. ACCS plans to use a military version of X.25 for packet-switched systems and for transfer over dedicated circuits and through circuit switches. Variable packet lengths are desired. CSMA/CD and token ring LANs are being considered for ADP systems. As in ATCCIS, the ACCS database concept is partitioned and partially replicated (see Sections 2.1.3 and 6.1.1). An ACCS-wide data dictionary is planned. Analysis has included an STC investigation on the applicability of

[77] ADSIA WG4 has been given a Priority One task to develop a Link 1 replacement; ADSIA WG4 has asked TSGCE(SG9) to look at media-independent protocols for such a concept.

ASN.1 and its relation to the syntax of STANAG 5500 (FORMETS). There is a concern as to whether use of FORMETS would permit achieving the full benefit of the OSI model.

The following considerations in ACCS indicate some elements of the technical approach for achieving interoperability:

- ACCS interfaces will be required to the following generic external agencies/systems:
  - NATO intelligence systems (e.g., BICES, NMOS)
  - NATO army headquarters
  - NATO land-based maritime headquarters
  - NATO maritime forces afloat
  - National headquarters, intelligence, army headquarters, maritime headquarters, territorial commands, meteorological services, civilian air traffic control, and local authorities.
- Requirements have been identified for free text traffic (electronic mail), graphics, and facsimile transmission services. Video transmission is a potential long-term requirement for ACCS, but it has been excluded from consideration for the current ACCS planning time frame (1990s).
- Two ADSIAstandardization documents have been considered important for ACCS in the area of formatted messages:
  - ADatP-3/STANAG 5500, containing a catalogue of character-oriented formatted messages
  - Common Information Exchange Glossary (CIEG), containing terms and definitions applicable to the development of both bit- and character-oriented procedural standards.
- ACCS requires an electronic mail service. The planned standard is the Military Message Handling System, based on CCITT X.400 (see Section 10.3.8).
- ACCS further requires automated interactions between databases (e.g., updates) that could be event driven. The FTAM standard has been recommended for consideration for ACCS use, particularly for bulk update of databases.
- The functions (e.g., syntax and formatting rules) of ASN.1 and the associated Basic Encoding Rules (BER) were recognized by the ACCS Team as potentially richer and offering greater scope than NATO Message Text Formatting System (FORMETS) functions of ADatP-3/STANAG 5500. Large investments in FORMETS are being made in operational systems, and NATO interoperability continues to be based on FORMETS and ADatP-3. Eventually, however, FORMETS could be replaced by ISO standards for automated data exchange to make better use of the functionality of the OSI model and the richness of ISO standards. There are potential problems in ensuring interoperability between systems using FORMETS and systems using ISO standards. Investigation is needed on whether the use of an information structure based on ADatP-3 message contents is a sufficient basis for achieving backwards interoperability with FORMETS systems.
- ACCS anticipates the use of gateways for data forwarding (message standard translation), trusted secure interfaces between cooperating ADP systems to

control access to data, and physical interconnection of different communication systems.

- A connection-oriented virtual call protocol has been proposed for ACCS, rather than a connectionless (or datagram) protocol, as the basis for packet switched services. Virtual call services are widely used in civil networks; they can result in more efficient transmission because of significantly lower packet overheads, and they can simplify network management. An issue is whether virtual call would provide adequate flow control under stress conditions. Limited use of a connectionless service may also be required.

16.4 Battlefield Information Collection and Exploitation Systems (BICES)

The Battlefield Information Collection and Exploitation Systems (BICES) will provide intelligence support for the ACE ACCIS , including the land-surface picture for NATO. BICES is a project under the direction of TSGCE PG7. BICES will consist of three segments, which will utilize either national or NATO intelligence capabilities [Ref. NST 1988]:

- Higher national segment includes national capabilities at the MOD-DoD and Theatre Level
- Lower national segment includes national capabilities below NATO PSCs
- The NATO segment of BICES, as the hub of the interconnected systems, will include the NATO capability at the NATO command level (a portion of ACE ACCIS).

The BICES concept will involve integration of national and NATO systems, initial processing, processing/fusion, and user exploitation. The BICES capability will be integrated into the ACE ACCIS. Configuration management for BICES will fall under configuration management of ACE ACCIS. User requirements for the ACE segment of BICES are completed [Ref. BICES 1988], but the majority of the national annexes have not yet been provided. One national operational capability has been designated as part of BICES, namely the Limited Operational Capability-Europe (LOCE) system developed by the US.

Among the approaches being considered for BICES are a common database and a data dictionary, whose scope and content are to be determined. NATO OSI standards from ISO and CCITT will be used unless they cannot meet the BICES requirements.

16.5 NATO Maritime Operational Intelligence Support (NMOS)

The NATO Maritime Operational Intelligence Support (NMOS) will also provide intelligence support for the ACE ACCIS . NMOS provides the naval surface and subsurface picture for NATO. NMOS is a joint project under SACLANT, SHAPE, and CINC-CHAN. The only standards identified for NMOS that are not part of the NATO Common Interface Standards are additional STANAG 5500 (ADatP-3) messages [Ref.

NMICC 1989]. The Military Committee approved the Tri-MNC concept for NMOS early in 1987 [Ref. NATO MC 1987].

16.6 Quadrilateral Interoperability Programme

The Quadrilateral Interoperability Programme is an initiative of four nations--France, Germany, United Kingdom, and United States--to develop and implement, for the short term, an interface through which the four national tactical land ACCISs [respectively Systeme Informatique de Commandement des Forces Terrestres[78] (SICF), Heeres-Fuehrungsinformationssystem fur die rechnergestuetzte Operations-fuehrung in Staeben[79] (HEROS), WAVELL, and Maneuver Control System (MCS)] can interoperate. Software development for the national systems has been completed, and an interoperability demonstration was successfully conducted in May 1990 near Ingolstadt, Germany [Ref. ADSIA 1988a]. Meetings were held in June and July of 1990 to explore options for fielding initiatives based on the Quadrilateral Interoperability Programme standards.

The Quadrilateral Tactical Interface Requirements (QTIR) document [Ref. QIC 1988] expresses the basic requirements. The Quadrilateral Technical Interface Design Plan (QTIDP) [Ref. QIC 1988a] specifies, for the gateway, the technical interface based on the ISO/CCITT OSI Reference Model. The operational requirements specify for information representation the use of formatted messages as described in STANAG 5621 Edition 2 and in accordance with ADatP-3 (STANAG 5500) specifications. The specifications for the common international interface between national gateways are provided in the QTIDP by annexes describing each of the seven layers with options and parameters derived from ISO/CCITT standards in order to meet the specific military requirements (e.g., naming, addressing, priority, sensitivity, size of messages, and segmenting).

Standards specified in the QTIDP are identified in Table 52. Specifications of Layers 1 through 5 are closely related to ISO standards. Layer 6 (presentation) is a null layer. Layer 7 specifies message handling functionality based on the CCITT X.400 (MHS-84) standards for the subset of service elements provided by the P1 and P2 protocols and the service elements provided by Reliable Transfer Service (RTS), as defined by ISO 9066-2, and integrated with the Association Control Service Element (ACSE, ISO 8649 and ISO 8650) that provide support for other application entities. The Quadrilateral Test and Demonstration Management Plan (QTDMP) [Ref. QIC 1988b] specifies a plan for interface testing and interoperability testing before performing the 1990 demonstration. Most of the interoperability parameters are specified by the options, classes, and system parameters selected from ISO/CCITT standards; some of the other

---

78 Information System For Command of Ground Forces (SICF), France.

79 Army Command and Control Information System for the Computer Assisted Conduct of Operations within Staffs (HEROS), Germany.

interoperability parameters are defined in accordance with military requirements defined for messages in the QTIR.

A preliminary review has shown that all standards, stacks, and options for the Quadrilateral Interoperability Programme that are also relevant to ATCCIS have been identified in earlier chapters of this working paper. In addition, a separate analysis [Ref. Ford 1987] has been performed that identifies a large number of interoperability parameters and provides their values.

16.7 Standard Automated Message Interface for NATO's ACCISs (STAMINA)

This summarizes the results of a review of the specifications for STAMINA [Ref. NACISA 1988]. STAMINA is being developed by an Interface Working Group of NATO Communications and Information Systems Agency (NACISA) to be used as a standard interface for passing information among ACCISs. Initial demonstrations are planned for the Central Region ACCIS and three target systems: the Allied Command Baltic Approaches Command and Control Information System (ACBA CCIS), the Central Region Alternate War Headquarters CCIS (CR AWHQ CCIS), and the Allied Tactical Operations Centre CCIS (ATOC CCIS, also known as the EIFEL Follow-On). STAMINA is planned to be used for such interfaces as [Ref. STAMINA 1990a]:

- Central Region (CR) ACCIS to UKAIR ACCIS and to EIFEL (ATOC)
- SHAPE to CR Primary War Headquarters (HQ) and to CR Alternative War HQ (AWHQ)
- ACBA CCIS to CR ACCIS and to EIFEL (ATOC).
- Various interfaces at SHAPE HQ.

Table 52. Standards for Quadrilateral Interoperability Programme

Layer	References for Standards
7. Application	ISO 8649-1986 (ACSE) ISO 8650-1986 (ACSE) CCITT X.400, X.401, X.408, X.409, X.411, X.420 DIS 9066.1, 9066.2 (Reliable Transfer) DIS 8824 (ASN.1) DIS 8825 (ASN.1 Basic Encoding Rules) IS 646, IS 6937 (Coded Character Sets)
6. Presentation (Null Layer)	DIS 8822-1985 DIS 8823-1985
5. Session	DIS 8326-1984 DIS 8327-1984
4. Transport	DIS 8072-1984 DIS 8073-1984
3. Network	ISO 8208-1985 (X.25 PLP) DP 8348 (CONS) DP 8472 (Network Convergence Protocol) DIS 8648-1985 (Internal Organization Network Layer) DP 8878-1984 (X.25 CONS) CCITT X.25-1984 STANAG 4214 (Internal Routing) STANAG 5046 (Communications Directory)
2. Data Link	ISO 7776-1985 (HDLC LAPB) DIS 8886-1985 ISO 3309 (HDLC Frame Structure) ISO 4335 (HDLC Procedures)
1. Physical	ISO TR 7477-1985 DIS 8481-1985 ISO/TC97/SC6 N3473 (DP 10022) ISO 4903 CCITT V.3, V.10, V.11, V.28 CCITT X.21, X.24, X.25 CCITT X.27 (EIA/RS-422-A)

Note: The table shows the status of standards at the time the QTIDP was specified.

STAMINA now consists of two separate transport profiles and an X.400-oriented application profile. The transport profiles support (1) X.25 packet switched networks for use in CR ACE and (2) permanent analogue circuits for point-to-point interfaces using dedicated analog circuits. (A third transport profile, switched analog circuits for use with the NATO IVSN analog voice network, has recently been deleted, as there have been no interest shown in implementing this aspect of STAMINA.)

The entire STAMINA profile for MHS-84 has been adopted by TSGCE SG9 as an intercept profile for the *NTIS Transition Strategy* [Ref. TSGCE 1989d].

Requirements for the Quadrilateral Interoperability Programme and STAMINA overlap, but it is not clear at this time if they will converge. Generally, STAMINA attempts

to provide military features (e.g., four levels of precedence and NATO classifications) as "extensions" in Layer 7.[80] Further, STAMINA provides three transport protocols (using Class 0 and Class 2), whereas the QTIDP provides just one (using Class 2) [Ref. ADSIA1988a].

16.7.1 STAMINA Application Profile

The STAMINA Version 4 application profile for message handling is a modification of CCITT X.400(MHS)-1984. Eighteen military features were added; these features are identified in Table 53. STAMINA messages are free text and text formatted according to the ADatP-3 specification [Ref. ADatP-3 1986a].

Table 53. Military Features Added to the STAMINA Specification

	Military Feature	Description
1.	Extended Authorization Info	Date and time officially authorized
2.	Subject Indicator Code	Eight subject codes for distribution information
3.	Primary Precedence	Grades of delivery (e.g., urgent, normal) for primary recipient
4.	Copy Precedence	Grades of delivery for copy recipient
5.	Security Classification	Five classifications (e.g., NATO NATO UNCLASSIFIED)
6.	Security Category	E.g., ATOMAL, EYES ONLY
7.	Originator Identifier	Originating organizational unit message reference
8.	Address List Indication	Address list type and identifier; on origination conveys multi-destination delivery; on receipt, forwarding action
9.	Clear Indication	Transmitted without any security classification
10.	Codress Message Indicator	Indicates a codress encrypted message
11.	Corrections	Corrections are required in body of text
12.	Exempted Address	Exempted name(s) from accompanying address list
13.	Handling Instructions	Handling instructions accompany the message
14.	Message Instructions	Message instructions accompany the message
15.	Message Type	Distinguish between normal and exercise traffic
16.	Other Recipient Indicator	Identifies other recipient(s) also intended to receive message
17.	Pilot Forwarded	Used in forwarding a message
18.	Security Policy Indentifier	Identifies a security policy

The application profile has two types of user access:

- Private Message Handling Service (MHS) Access: UA and MTA, PRMD to PRMD, A/3211 (based[81] on CCITT X.400-1984 and ISO 8327)
- Military Private MHS Access: UA and MTA, PRMD to PRMD, A/3211(M) (based on CCITT X.400-1984, ISO 8327, ACP 117, and ACP 127).

---

80 STAMINA leaves the commercial P1 and P2 sublayers unmodified and defines new service elements as extensions to P2; the QTIDP redefines both P1 and P2.

81 STAMINA Version 3.0 [Ref. 27] also cites "ISO 8322" for T/3211 and T/3211(M), but this standard does not exist.

The A/3211 application profile is the X.400 MHS, in which the Application Layer (Layer 7) has three sublayers: User Agent Layer defined by X.420, Message Transfer Layer defined by X.411, and Reliable Transfer Server defined by X.410. The A/3211 Presentation Layer (Layer 6) is defined by ISO 8823 (based on X.410), and the Session Layer (Layer 5) is defined by ISO 8327 (based on X.410).

STAMINA applications profile and the Quadrilateral Profile (QP) are both military versions of CCITT X.400(MHS)-1984. The QP is being developed and used by four command and control system programs in FR, GE, UK and US. The QP has a single transport profile based on X.25. To understand some of the essential differences between STAMINA and QP, note that Layer 7 of X.400-1984 consists of the User Agent (UA), the Message Transfer Agent (MTA), and the Reliable Transfer Agent (RTA). The RTA serves as the liaison with the Session Layer protocols (in X.400-1984, the Presentation Layer is a null layer; i.e., there is no layer 6, so Layer 7 liaises directly with Layer 5). Both the UA and MTA use peer (e.g., UA-to-UA) protocols to communicate to distant UAs and MTAs. The peer protocol for the UA is the Interpersonal Messaging Protocol (P2), while the peer protocol for MTA-to-MTA communication is the Message Transfer Protocol (P1). Thus, P1 defines the relaying of messages among MTAs, while P2 defines the service elements of the interpersonal messages exchanged by UAs. The STAMINA profile provides military features by extending P2 (using a "superset" approach), permitting these features to be mapped into similar commercial features in the P1 protocol without affecting lower layer protocols, whereas the QP changed both P1 and P2 in such a way that the changes affected services in lower protocol layers as well.

16.7.2 STAMINA Transport Profiles

STAMINA includes selection of CCITT and ISO standards--along with allowable options and parameters--necessary to attain interoperability among the end systems. STAMINA is based on profiles defined in the SPAG User's Guide [Ref. SPAG 1987]. The STAMINA transport profiles are:

- Permanent Telephonic Circuit Providing Connection-Oriented Network Service, T/21(M)
- Telephonic Switched Circuits Providing Connection-Oriented Network Service, T/22(M)
- Permanent Access to Packet Switched Data Network (PSDN), OSI Connection-Mode Services, T/312(M)

Table 54 identifies the standards specified for the STAMINA transport profiles. The current standard for STAMINA is Version 4.0, April 1990 [Ref. STAMINA 1990].

Table 54. Standards for STAMINA Transport Profiles

Layer	Transport Profiles T/21(M)	T/22(M) T/312(M)	T/312,
4. Transport	ISO 8072 ISO 8073[a]	ISO 8072 ISO 8073[a]	ISO 8072 ISO 8073[a]
3. Network	ISO 8348 ISO 8208 ISO 8878 STANAG 4214 STANAG 5046 CCITT V.25 CCITT V.25bis	ISO 8348 ISC 8208 ISO 8878 STANAG 4214 STANAG 5046	ISO 8348 ISO 8208 ISO 8878 STANAG 4214 STANAG 5046
2. Data Link	ISO 7776[b] CCITT V.25 CCITT V.25bis	ISO 7776[b]	ISO 7776[b]
1. Physical	CCITT V.24 CCITT V.11 ISO 2110 ISO 4902 CCITT V.25bis MIL-STD-188C	CCITT V.24 CCITT V.11 ISO 2110 CCITT V.25 ISO 4903 MIL-STD-188C CCITT X.21bis	CCITT X.21 CCITT V.11 ISO 2110 ISO 4902 MIL-STD-188C

[a] Class 0 (Simple) and Class 2 (Multiplexing) are mandatory; Class 4 (Error Detection and Recovery) is optional.

[b] Options 2 and 8 of ISO 7809 (Balanced Asynchronous Class) are mandatory; Option 10 may be included under bilateral agreement.

16.7.3 STAMINA Development Activities

One current activity is addressing the need to add functionality required to support relays between X.400 and ACP-127 message domains, as recommended by TSGCE and recommended by the *NATO C3 Architecture* and the *NATO C3 Master Plan.* In addition, STAMINA is building a database of the interoperability parameters (e.g., speeds for communications lines) chosen by implementors of STAMINA specifications. Some parameters must be identical for interoperability and others must fall within certain ranges. The database will also track some parameters that do not affect interoperability.

A conformance test suite has been developed, and a file transfer functional profile (based on FTAM) has been defined. A new transport profile is being developed for digital circuit switch connections for communications supporting the SHAPE and CR Mobile Alternate War HQ. The current STAMINA application profile will be implemented in the STC testbed.

The Configuration Management Board (CMB) for STAMINA has agreed [Ref. US 1988] to add the additional military features to the X.400 specification, making it identical to MMHS(84). Version 4.0 of STAMINA should be reviewed for such compliance. The

CMB has decided to omit one part of STAMINA, the Transport Profile for Analog Circuit Switch, which was seen as high risk and for which no interest has been expressed from implementors. There are plans to develop another transport profile for STAMINA for digital circuit switched communications. NACISA is interested in studying the compatibility of STAMINA with the 1988 standards, with an orientation to migrate toward a 1988 base or, alternatively, define an interface module between the 1984- and 1988-based systems.

Some STAMINA parameters are left to be determined by the implementors of an interface, and some of these must be the same on both ends of the interface. NACISA has developed a database in which to record the parameters used on all STAMINA implementations. NACISA has begun to develop a new project called the Automatic Message Processing System (AMPS). It appears at this early stage that it will have two aims [Ref. NACISA 1990]:

- To provide individual ACE HQs with automated message handling capability internal to each HQ for generation of outgoing messages and to provide the processing of incoming messages. Initially, the messages will be transmitted via the existing TARE system using TARE-unique protocols. Where possible, the internal processing will be based on X.400 oriented systems.
- To use the AMPS at each HQ as the platform for the eventual replacement of the TARE with an X.400 oriented network.

The interface standards to be used with ACE are expected to migrate from TARE-unique protocols via STAMINA/MMHS-84, through MMHS-88, and eventually to X.400 commercial standards.

An ACE ACCIS Integrated Testbed is planned to support NATO CCIS development efforts, e.g., the BICES Pilot Study (BPS) effort, with NACISA serving as the host nation and STC providing scientific expertise and the home of one of the testbed nodes.

17. NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS

This appendix identifies national initiatives that make or plan to make significant use of OSI standards in military applications. Major bilateral and multilateral initiatives are discussed in the main body of this working paper; these include the Quadrilateral Interoperability Programme (Section 16.3.5) and STAMINA (16.3 6).

Quick Reference	
Topic	Page
France	373
Netherlands	378
Norway	379
Performance Evaluation	400
United Kingdom	379
United States	382

The primary purpose of this review of national initiatives is to identify the ways in which military features are being addressed in national systems. In some cases, there may be fully-compliant use of OSI standards. In other cases, there may be defined some extensions to the standards that could be considered by international bodies as candidates for new options to the commercial standards, so that in the time frame of ATCCIS (and other NATO CCIS projects) the military features (e.g., a secure local area network) may be specified by civil standards. On the other hand, analysis of national initiatives may lead to conclusions that some features may need to be specified as deviations from civil standards and, in these cases, the relevant STANAGs may need to have similar deviations.

National initiatives discussed in Section 17.3 are addressed, where possible, in terms of requirements, profiles, and transition strategies that have been recommended or adopted. A short review is provided in Section 17.2 of work being done to evaluate the performance of civil standards for military applications. Several initiatives that have led to fielded operational capabilities are discussed in Appendix C in some detail.

17.1 Overview of National Initiatives to Implement OSI Standards in Military and Related Systems

17.1.1 France

Army Tactical CCIS Systems. Army tactical CCIS systems in France are using or are projecting to use more and more components based on OSI standards. The Army is following the general recommendations of standards organizations such as AFNOR, SPAG, CCITT, and CEN/CENELEC (see Appendix F), and would thereby try to use, wherever possible, the products (hardware and software) built upon these standards.

One example of the implementation of OSI standards in Army tactical systems is the use of ETHERNET™ (ISO 8802.3) to link cells within a command post. In addition, tactical networks, such as RITTER and RETINAT, are based on CCITT X.25 packet switched standards. Table 55 identifies the international OSI standards that the Army intends to use in its standardized MHS Gateway, based on QTIDP specification.

Table 55. French Army Standardized MHS Gateway

OSI Layer	International Standard	Brief Title of Standard
Application (Layer 7)	CCITT X.400:1984 ISO 9066/1:1987 (c1/2) ISO 8649:1986, ISO 8650:1986	MHS RTSE ACSE
Presentation (Layer 6)	CCITT X.409:1984	Abstract Syntax Notation
Session (Layer 5)	ISO 8326:1986, ISO 8327:1986	Basic Service and Protocol
Transport (Layer 4)	ISO 8072:1985, ISO 8073:1984	Class 2 Service and Protocol
Network (Layer 3)	ISO 8208:1985	Basic Service and Protocol
Data Link (Layer 2)	ISO 7776:1985	HDLC LAP B
Physical (Layer 1)	CCITT X.21:1984	

Source: Private communication from M. Romann, Section d'Etudes et Fabrications des Telecommunications (SEFT), Direction des Armements Terrestres/DGA, Ministere de la Defense, France, 13 January 1992, NATO UNCLASSIFIED.

RETINAT. RETINAT is a data communications system for the French Army. The network operates 33 switches of two types (one for military districts and one for military regions). The network accommodates 1,400 synchronous and 600 asynchronous ports and supports data rates from 300 bps to 64 Kbps. The switches are interconnected with 64-Kbps trunks and use X.75 gateways for interoperability with other data networks. [Ref. Cassese 1990]

Real Time Transport Service (RTTS). The French MOD has developed an architecture and implementations of that architecture for a Real Time Transport Service (RTTS). GAM-T-103 is a specification for an implementation of this architecture [Ref. GAM 1987]. RTTS results from more than 15 years of experience in the design and realization of real-time data networks for military systems. RTTS provides not only data communication services but also synchronization and management services. RTTS was described at the June 1990 Military OSI Symposium at STC [Ref. STEI 1990]. The paper addressed the ISO Transport Service, real-time constraints, and a proposed real-time Transport Service. It presented the classes of service, the models used for data transfer, the connection-oriented and connectionless modes for communication services, the

synchronization services, and the management services. RTTS has been proposed in draft STANAG 4254 (Annex E) as the basis for defining real-time services for NATO CCISs (see Section 10.4.4).

There are two current releases of the Real Time Transfer Protocol specification:

- GAM-T-103B, available in French only, is interfaced with a data link service near to the MAC service to support the STANAG 1553 Military Bus (with the STANAG 3910 extension). GAM-T-103B is used for the Rafale aircraft weapon and navigation system.
- GAM-T-103C, available in French and English, is interfaced with a LLC1 data link service to support the Recital bus (deterministic Ethernet). GAM-T-103C is used for the new French aircraft carrier weapon and navigation system.

Public Message System. ATLAS 400 is a public messaging system based on CCITT MHS X.400-1984 and is a good illustration of the national implementation of X.400 standards. Administration and design of ATLAS 400 is under the responsibility of TRANSPAC, a public company that is a subsidiary of FRANCE TELECOM. The ATLAS 400 services can be provided to private companies or administrations, and different kinds of systems can be built:

- A large company can get its own "private" messaging system, and all the nodes can be split throughout the country at the different company's locations.
- It is also possible to get a system that allows different organizations (public or private) to exchange messages between them. This can be useful, for example, to exchange documents between provider and client. Such an implementation would be used to exchange information between different companies.

The ATLAS 400 functional profile is defined in *Specification Technique d'Utilisation et de Raccordement (STUR) ATLAS 400,* which defines Layers 1 to 7. This document also derives from an early effort of the Centre National d'Etude des Telecommunications (CNET) to promote the X-Series standardization (this work, named ARCHITEL, is described below).

ATLAS 400 is only an interpersonal messaging system, and so uses only the Interpersonal Messaging Protocol from the X.400 Series. ATLAS 400 can also be adapted to the size of the company's computer equipment. For example, the Message Transfer Agent may be locally implemented or derived from the ATLAS 400 implementation. Thus, the User Agent and the Message Transfer Agent are not necessarily co-resident. This illustrates the possibilities of tailoring the system to client use.

ARCHITEL. Historically, ARCHITEL is a group effort within CNET. Its purpose was to promote the use of X-Series standards for the widespread use of FRANCE TELECOM and telecommunications companies, in particular by the CNET contractors. ARCHITEL defined X-Series profiles in the early 1980s. ARCHITEL implemented these profiles, specifically those for the lower five layers, to validate the parameters and options used for interoperation and also to clarify the standards where necessary. In some cases,

ARCHITEL identified and developed recommendations to address portions of the standards that were judged to be imprecise. The profiles defined in ARCHITEL specified Class 0 and Class 2 for the Transport Layer and the connection-oriented network service for CCITT X.25. (X.25 is used in the public packet switched network, TRANSPAC.)

The ARCHITEL profile is a complete specification that precludes at Layer 3 such capabilities as adding user data to a packet call, using nonstandard packet sizes, etc. All the parameters and options for each layer needed to ensure interoperation are addressed.

ARCHITEL has published the reference document, *STUR ARCHITEL*, which states all the functional profiles for the lower five layers of the CCITT OSI Reference Model (e.g., X.215 and X.225 for the Session Layer). STUR ARCHITEL is informative, not mandatory. It was one of the earliest functional profile descriptions for the industrial community and was therefore instrumental in providing proof of concept of the use of OSI standards on a national scale. Thus, historically, STUR ARCHITEL was the basis for the development for OSI implementations now in use by the military. The military implementations have also included Transport Class 3.

SICF. SICF is the French Army battlefield CCIS designed to provide ADP facilities at the First Army, Corps, and Division HQs, in addition to the headquarters of the Rapid Deployment Force.

- Functional Units
  - Each command post has several computers connected to a LAN.
  - Each computer can serve:
    - -- 12 alphanumeric terminals in any chosen role, such as manoeuver, intelligence, or logistics
    - -- 4 high-resolution graphic cells for manoeuver and intelligence
    - -- 4-auto-dial devices linking into the RITA communications network.
  - Each screen can play any role for the user (G2, G3, etc.).
  - The first-generation uses civil hardware protected by reinforced boxes.
  - Application software has been developed in C language and uses the UNIX operating system.
- Timescale
  - First generation
    - -- 1988 Stage 1 - Army, Corps and Rapid Deployment Force HQ
    - -- 1990 Stage 2 - Down to division level
    - -- 1991 Stage 3 - Additional functions such as command post flip flop, ISO communication software on the bases of the Quadrilateral Technical Interface Design Plan
  - Second generation
    - -- 1996 - Integration of environment constraints, decision supports, and ruggedization.
- Functions
  - Communications: Computers can be connected to those at other command posts to exchange data, including graphics, via RITA.

- User Assistance: Computer-assisted message preparation for LANDREP and STANAG 5621 messages; message transmission via RITA and distribution within command posts; automatic production of graphics and situation reports from stored data.
- Database Management: Distributed relational database.
- Specific functions: nuclear, biological, and chemical; engineer; intelligence; manoeuver; logistics; fire support; and air-space management.

17.1.2 Germany

HEROS. HEROS-2/1 is the German Army CCIS that supports staff work at the corps, division, brigade, and battalion echelons. The HEROS-2/1 hardware is mounted in TEMPEST-proof shelters that can be moved by vehicles.

- Functional Units. The command post consists of the computer communications shelters (Re/KK), the graphic shelter, and the workstations which are all connected via a local area network (LAN). Each command post on corps and division level is duplicated in order to provide to the commander high availability of the system due to the development of the leap-frogging concept. Each workstation can play any role for the user (G2, G3, etc.). Communications to the command posts are provided by wide area networks (WAN) that consist of AutoKo, Bundeswehrgrundnetz, and will include combat net radio in the future.
- Timescale
  - Field trial — III 1989 - IV 1990
  - Fielding of the three Corps — II 1992 - IV 2000
- Functions
  - Graphic. The staffs of the corps, division and the brigade echelons are also equipped with graphic shelters (GK). The graphic shelters contain workstation and digital equipment with which it is possible to draw up situations and plans and generate them from the data base.
  - Applications
    -- Message formats according to STANAG 5500
    -- Message reporting based on STANAG 5621, Edition 2
    -- Orders according to STANAG 2014
    -- War Diary
    -- Mail Box
  - Military Message Handling System
  - Communication architecture allows the automatic use of the following communications links:
    -- LAN (command post communications)
    -- WAN:
    --- Bundeswehrgrundnetz (connection to the Army Staff and NATO)
    --- AutoKo (connection to corps, division and brigade)
    --- VHF Radio (connection to battalions and other command posts)
    --- QIP-Interface (connection to MCS, SICF and WAVELL)
  - Database Management. The data held by all command posts is consistent. The data management concept is, therefore, designed to continually update the database.

- Leap Frogging. The database management mentioned above fully supports the command post leap frogging concept.

17.1.3 The Netherlands

ZODIAC. A program is on-going which will provide an upgrade of the Royal Netherlands Army (RNLA) common message handling system [Automatic Telegraph System (ATS), ACP 127 based] within the tactical ZODIAC communication system. The new ATS will be fielded in 1995.

ABDIS. A local message distribution system [Abonnee Distributie Systeem (ABDIS)] was introduced in the 1 NL corps command post in 1990. This system provides a local message switch (ACP 127 based) which forwards messages by "Subject Indicator Code." The current plan is that the systems for division command posts will be fielded in 1993. The ABDIS systems can be seen as an interim system until the introduction of the "Command Post Communication Network" in 1995. See Figure 20.

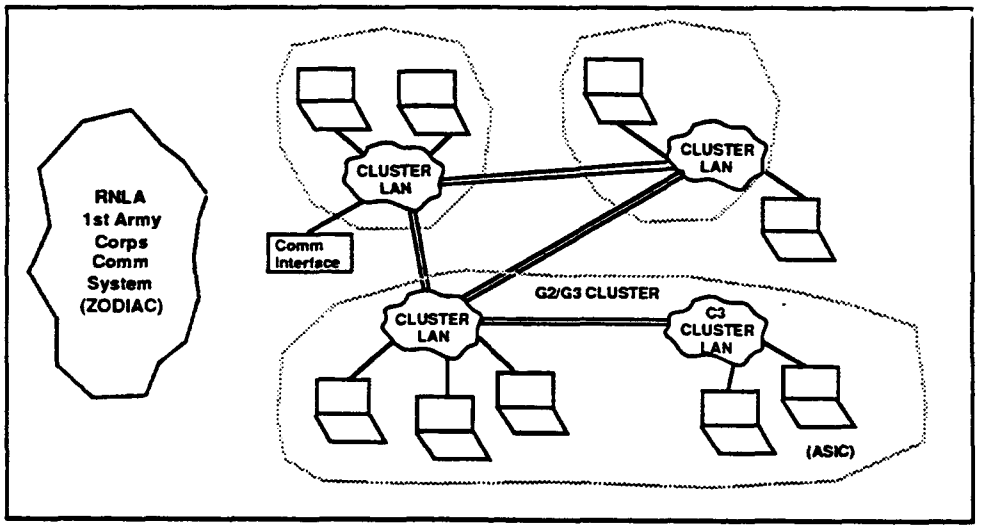


Figure 20. RNLA Command Post Communication Network

CPCN. The RNLA started a program for the development of a "Command Post Communication Network (CPCN)" in December 1991. The CPCN will be used as the common data communication infrastructure for the division- and corps-level command posts. The CPCN is the core system on which the new tactical information systems will be developed in the near future. The CPCN involves an integrated telephone- and data communication- infrastructure based on OSI standards. Data communications protocols: (Probably DECNET phase 5). See Figure 21. The first (corps level) system will be fielded in 1995. (The name of this new project is still a point of discussion.)

C2 Programme Evolution. The RNLA is following the general recommendations of civil and NATO standards organizations. (Ethernet to link C3

elements within cells; FDDI to link cells within the command post; X.25 to link command posts; ACP127 on the gateways). The Army intends to use (future) standardized ATCCIS specifications.

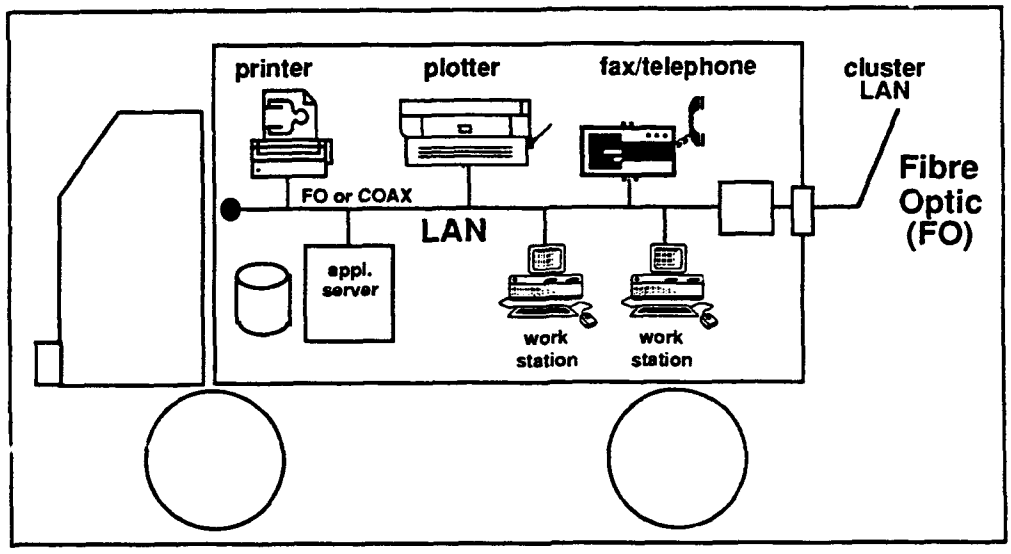


Figure 21. RNLA C3 System Architecture

17.1.4 Netherlands, Norway, France, United Kingdom

Four NATO nations are participating in a project entitled "Cooperative Prefeasibility Studies for Tactical Communications Systems for the Land Combat Zone--Post 2000." In this study, candidate subsystem architectures are being developed on the basis of current and near future communications technologies as ISDN, EUROCOM, FDDI, PABX, packet radio and cellular telephony. From these technologies six subsystem architecture alternatives were derived each with either a nodal (centralized) or a nodeless (distributed) characteristic. (See Section 4.4).

From this set, subsystem architectures are selected on the basis of military operational requirements and threat expectations to form one system architecture for the entire Land Combat Zone. The chosen system architecture to cover the intermediate and the rear zone of the land combat zone. The wide area communications subsystem consists of a backbone of distributed Local Area Communications Subsystem (LACS) elements with centralized LACS elements providing access to the backbone. [Ref. van der Voort 1990]

17.1.5 United Kingdom

Robust Protocols Research Programme. The U.K. MOD and NATO has established the Robust Protocols Research Programme at RSRE to quantify and minimize the risks associated with the U.K. MOD and NATO policies for procuring future CCISs to

ISO OSI standards. The approach being taken is to take commercial off-the-shelf protocols that are as near as possible to the perceived military requirement. The performance of these protocols is being established under ideal and degraded conditions in the laboratory.

Initial work has concentrated on the X.400 and FTAM standards. A protocol stack, using X.400 or FTAM, Transport Service Class 4 (TP4), and connectionless network service (CLNS) over X.25(1984) has been selected. These were selected to give a worst case scenario for evaluating the protocol standards. Early results have provided an upper bound to the overheads that may be experienced under ideal conditions. This result will be used for the design and sizing of messaging networks. Some measurements on the performance of FTAM over degraded links have also been obtained. These have shown how a more "intelligent" implementation of the data link protocol could provide optimum throughput over a range of degraded conditions. [Ref. Price 1990]

Defence Fixed Telecommunications System (DFTS). MOD central Defense staffs are establishing a Defence Packet Switched Network (DPSN). This project is a major element of a wider Defence-wide communications infrastructure covering all communications services: the DFTS. Over time, the present MOD and Armed Forces communications systems will integrate to DFTS. Profiles that have been recommended for the DFTS are of three types: end-system services, common application services, and basic communications services. End-system services, together with the proposed standards, are electronic trading (based on EDI), revisable document exchange (based on ODA), general file transfer (based on FTAM), remote terminal access (based on VT), inter-personal messaging (based on MMHS), and inter-organizational messaging (also based on MMHS). Common application services include message handling (MMHS), Directory, ACP 127 interworking (MMHS), shared file store (FTAM), and shared database (RDA and SQL). The basic communications service profiles are T.31(M) for WAN access, T/611 and T/613 for LAN access, R.131(M) for WAN-to-WAN relay, and R/21 for LAN-to-LAN relay. [Ref. Bailey 1990]

The U.K. MOD has a commitment to provide its Single Service strategic communications needs via a common communication network (DFTS). It is also MOD policy that such provision should, to the greatest extent possible, be procured from the civil market to standards recognized by the international community. Progress in implementing the DFTS has been slow as the priority of each of the Single Services has been to deploy their own systems, leaving convergence to DFTS until a later date. However, one subset of DFTS. the packet switched data communications network (DPSN), was identified as requiring common provision to satisfy immediate operational needs.

The DPSN procurement has been guided by the DFTS Architecture and Procurement Working Group (DAPWG), which recommended that (1) the network be based upon the internationally recognized X.25 standard for network access; and (2) potential candidate network systems should be mature, have considerable expansion

capability, and be supported by a manufacturer with a total commitment to the product and development of the relevant standards. The procurement has been distinguished by the short time scale between statement of requirement and in-service operation, and being both within the financial provision and satisfying the operational requirement. For the future some significant issues have to be developed and resolved, not the least being interworking with other systems, e.g., ISDN, multilevel security and management across the boundary between DPSN and end-user systems. [Ref. Dibble 1990]

Wavell. Wavell is a battlefield ADP system, built to full military specifications including TEMPEST and NBC. It is designed primarily to assist G2/G3 staff cells in headquarters at corps, division, and brigade levels. It has limited G1/G4 functionality. Full deployment to 1 (Br) Corps was completed in 1987 and the latest software upgrade (Version 5) will be tested at the end of 1991, after which no more changes to the existing Wavell will be made. A study into an enhanced Wavell has begun, and full production is currently planned to start in mid-1993 and is geared to coincide with the formation of the British-commanded ACE Rapid reaction Corps. This will also include integral interoperability functionality after evaluation of the 1993 Quadrilateral Interoperability Programme field trials. International functionality up to the field trials will be procured as a support facility and co-exist with Wavell. The in-service date for enhanced Wavell is 1995. Many options regarding the use of standards are being considered, some of which are identified below [Ref. TSGCE 1991n]:

- Four classes of functionality
  - STANAG message preparation and generation
  - STANAG-to-Wavell message exchange
  - International system management
  - Communications interconnection
- Some or all of the following components:
  - X.25 gateway units (as in current Wavell)
  - Quadrilateral MHS (QMHS) based on X.400-88 on international side of message exchange gateway
  - X.400-88 MHS on national side of gateway
  - International system management capability
  - Message store capability (absent in the current QMHS)
  - X.500 Directory services capability
  - Staff workstations with X.400-88 and "IRIS" STANAG message preparation application programme
- Consideration of X.400-92 for future designs.

WAVELL Risk Reduction Exercise. Proposed architecture and configuration options to be adopted for the Wavell Risk Reduction Exercise (WRRE) Demonstrator System will shortly be agreed.

The WRRE Demonstrator System (WDS) will be assembled and integrated at DRA Fort Halstead as a major part of the process of demonstrating that the Wavell Enhancement

System (WES) can be implemented at low risk from Commercial Off-the-Shelf (COTS) equipment and software which will meet the user requirement, and which will possess inherent flexibility to adapt to a wide range of scenarios, to extend to other functional areas of military activity, and which will provide a simple and smooth transition path towards a battlefield-wide CIS which meets the principles set forth in a UK Army policy paper.

The architecture to be described is a set of standards that provide the infrastructure facilities recommended to be implemented as part of the staff terminals and other processing units within the WES, on top of which the selected user functionality will be supported. In terms of the model developed under the UK Goal Architecture study, these infrastructure facilities are the communications sub-system, the data management sub-system, the human-computer interface sub-system and the appropriate binding provided by the operating system. In terms of the model developed by the ATCCIS study, these infrastructure facilities are the transfer facility, the data management facility, the service control facility and the MMI service facility.

Both these studies recommended that their respective architectures be implemented in terms of internationally agreed commercial standards, supplemented where essential with military-specific features to meet essential military requirements which could not be satisfied by the commercial standards. The full repertoire of such standards will not be completely defined for some years as yet, but the direction in which the commercial standardization bodies are heading is now sufficiently clear in all important respects to allow a choice of "intercept" standards to be made with a high degree of certainty that only minor adjustment will be subsequently required. The WDS will be constructed on that basis.

The configuration issues relate to the physical disposition of equipment, the allocation of functions to those equipments, the implications of such choices on the underlying communication bearer systems, and the constraints place by both the current configuration of those bearer systems and the present disposition of equipments on the proposed initial deployment proposals for the Wavell Enhancement System. These interactions are now being investigated.

17.1.6 United States

DoD Transition to GOSIP. The US DoD intends to adopt OSI protocols as a full co-standard with DoD protocols, specifically for message handling and file transfer (MIL-STDs 1777, 1778, 1780, and 1781). OSI protocols are expected to "become the sole mandatory interoperable protocol suite" [Ref. ASDC3I 1987]. The Defense Communications Agency (DCA) has been named as the DoD Executive Agent for Data Communications Protocol Standards, and in June 1988 this agency promulgated an OSI implementation strategy [Ref. DCA 1988]. The Services and Agencies have developed transition plans to comply with this strategy.

Corporate Information Management. The US DoD has initiated a major effort to transition the DoD's present information systems and associated information technology resources to a communications and computing infrastructure based on the principles of open systems architecture and systems transparency. The breadth of this work is for DoD-wide corporate information management (CIM) and includes in its scope both tactical and strategic CCISs. Architectural aspects of the CIM Technical Reference Model are discussed in Section 4.4.4. A summary of the CIM current (November 1991) assessment of the standards availability is given in Table 56. The table addresses all eight CCIS service areas (note that security and management standards are addressed within each of the other seven service areas where they apply). The column on standards status indicates whether adequate standards are now or in the future available for each service and if not, whether there is a gap (some but not sufficient standards) or a void (no standards). The table further shows the dates at which US federal standards (FIPSs) are expected.

Table 56. US DoD (CIM) Assessment of Standards Availability

				TIMEFRAME FOR STANDARDS AVAILABILITY			
SERVICE AREAS	SERVICE	STANDARDS STATUS	CIM	1 OCT 1991	1 OCT 1992	1 OCT 1993	1 OCT 1995
Operating System	Kernal	Now	●	FIPS Pub 151-1 (POSIX)	FIPS Pub 151-2		
	Commands and Utilities	Future		IEEE P1003.2 (Draft Standard)	Approved IEEE Standard	FIPS Addition	
	Security	Future		IEEE P1002.6 (Draft Standard)	Approved IEEE Standard	FIPS Addition	
	System Management	Future	●	Draft Government Network Management Profile (GNMP) FIPS	Approved FIPS Supplemented By MIL-STD-1813		
Programming	Programming Languages	Now	●	FIPS Pub 119 - ADA		FIPS Pub 119-1 (ADA-9X)	
	Case Tools and Environment	Future		ECMA Portable Common Tool Environment (PCTE) Specification 149			
	Security	Void					
User Interface	Data Stream Encoding	Now	●	FIPS Pub 158 (X Window System)			
	Data Stream Interface	Now	●	FIPS Pub 158 (X Window System)			
	Subroutine Foundation	Now	●	FIPS Pub 158 (X Window System)			
	Toolkit Components	Future		Future Standard - IEEE P1201.X	Final Draft - IEEE P1201.X	FIPS 158 Addition	
	Presentation	Future		Future Standard - IEEE P1201.X	Final Draft - IEEE P1201.X	FIPS 158 Addition	
	Dialogue	Future		Future Standard - IEEE P1201.X	Final Draft - IEEE P1201.X	FIPS 158 Addition	
	Security	Void					
Data Management	Data Dictionary - Directory	Now	●	FIPS Pub 156 (IRDS)			
	Data Management	Now	●	FIPS Pub 127-1 (SQL)		FIPS Pub 127-2 (SQL +)	FIPS Pub 127- 3 (SQL++)
	Distributed Data	Future		Draft ISO Standard - Remote Database Access (RDA)	Final Draft - IEEE P1201.X	FIPS Addition	
	Security	Void					

Key: ● Included in November 1991 CIM Standards Profile.

Table 56. (Continued)

				TIMEFRAME FOR STANDARDS AVAILABILITY			
SERVICE AREAS	SERVICE	STANDARDS STATUS	CIM	1 OCT 1991	1 OCT 1992	1 OCT 1993	1 OCT 1995
Data Interchange	Document Interchange	Future		Planned FIPS Pub (Office Document Architecture/ Office Document Interchange Format/Office Document Language ODA/ODIF/ODL)	Draft FIPS	Final FIPS	
	Document Interchange	Now	●	FIPS Pub 152 (SGML)			
	Graphics Data	Now	●	FIPS Pub 128 (CGM)			
	Product Data Interchange	Gap		Planned FIPS Pub (Initial Graphic Exchange Specification/IGES)	Draft FIPS	Final FIPS	
	Product Data Interchange	Future		Draft International Standard (Standard for the Exchange of Product Model Data - Step)	Final ISO Standard	Draft FIPS	Final FIPS
	Electronic Data Interchange	Future		FIPS 161 - Effective 30 Sept 1991		Convergence of X.12 and Edifact	
	Security	Void					
Graphic Services	Graphics	Now	●	FIPS Pub 120-1 (GKS)			
	Graphics	Now	●	FIPS Pub 153 (PHIGS)			
	Security	Void					
Network Services	Data Communications	Now	●	FIPS Pub 146-1 (GOSIP)		FIPS 146-2 (GOSIP)	
	Transparent File Access	Future		Draft IEEE Standard P1003.8			
	Personal/Micro Computer Support	Void					
	Distributed Computing	Future		Draft OSF Specification (NCS/RPC)	Draft FIPS		Final FIPS
	Security	Void					

Source: *Corporate Information Management (CIM) Technical Reference Model*, Version 1.0, US DoD CIM Standards Office, 4 November 1991, UNCLASSIFIED.

Key: ● Included in November 1991 CIM Standards Profile.

Packet Switching for DDN. The US Defense Communications Agency has implemented an X.25 packet-switched protocol for the Defense Data Network (DDN). This protocol includes the use of the US DoD-unique protocols for Layers 3 and 4, namely the Internet Protocol (IP) and the Transmission Control Protocol (TCP). DDN supports over 50,000 users of a DoD-unique electronic mail (E-Mail). DDN contains a set of physically, procedurally, and cryptographically secured packet switching segments for classified E-Mail in the Defense Integrated Secure Network (DISNET) (e.g., DISNET-1, DISNET-2, DISNET-3). There are additional segments for unclassified E-Mail [e.g., Military Network (MILNET) and Advanced Research Projects Agency Network

(ARPANET)]. Local area networks (LANs) are connected to the DDN by gateways or hosts using the DoD IP.

Defense Message System (DMS)--Upgrades for DDN. The US has initiated [Refs. DCA 1989c; MROC 3-88 1989] a project called the Defense Message System (DMS) that will eventually integrate DDN with the Automatic Digital Network (AUTODIN). DMS will phase in [Ref. DCA 1988a] such protocols and services as US GOSIP, CCITT X.400 Message Handling System, High-Level Data Link Control (HDLC) for subscribers, new asynchronous protocol(s) with reliable transfer for subscribers, and CCITT X.500 Directory Services. TCP/IP protocols will be phased out. Initially (Phase I) a US DoD-unique security program called BLACKER will be implemented at the host-to-host level, which will ultimately result in an integrated DISNET. Later (1993) DDN will consist of MILNET (unclassified) segments and DISNET (classified) segments connected by BLACKER-protected gateways.

The following general requirements have been validated by the DMS Multicommand Required Operational Capability (MROC) in 1988:

- Connectivity and interoperability
- Guaranteed delivery and accountability
- Timely delivery
- Confidentiality and security
- Sender authentication
- Integrity
- Survivability
- Availability and reliability
- Ease of use
- Identification of recipients
- Message preparation support
- Store and retrieval support
- Distribution determination and delivery.

In November 1991, DISA prepared a draft DMS Required Operational Messaging Characteristics (ROMC) document to specify the messaging characteristics that are derived from the thirteen general requirements identified above. The ROMC is solution independent and develops quantitative characteristics based on baseline DMS requirements and from engineering estimates. [Ref. DISA 1991]

An OSI Transition Plan has been prepared for the DMS. The April 1991 draft of this plan defines transition goals, constraints, activities, dependencies, and schedule for the transition of the DMS to an architecture and supporting environment that employs the US GOSIP. It documents the activities necessary to transition DMS hardware and software

components, protocols, formats, and procedures to an OSI-based capability, while providing for interoperability between the baseline capability and the OSI-based capability during the transition period.

Beginning with the Baseline in 1989, the plan identifies three transition phase (1990-94, 1995-2000, and 2001-2008). The major capabilities and changes included in the plan are X.400 messaging, X.500 Directory Services, management capability, AUTODIN-to-DDN interconnectivity, Allied interoperability, tactical interoperability, and AUTODIN phase out. Phase I augments the 1989 Baseline with initiatives to bridge the gap between AUTODIN and the DDN and to improve base-level automation.

Phase II will include X.400/X.500 individual and organizational messaging with the SDNS Message Security Protocol (MSP) protection (vice distinct AUTODIN and E-Mail in the first phase). The Base Information Transfer System (BITS) will begin to be deployed at the base level in Phase II. Most but not all of the Baseline and Phase I components will be phased out. This evolution continues and is completed in Phase III. [Ref. MITRE 1991]

C4I for the Warrior. The US Joint Staff (J6J) has developed a concept to intelligently and uniformly apply information technology to facilitate the command, control, communications, computers, and intelligence (C4I) support to the warrior. The concept is standards based and focuses on exchange of information between existing C4I systems. Briefly, the capability of this concept is described as "a fused, real-time, ground truth picture of the warrior's battle space and the ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute the warfighting mission in the battle space." Each step of the interoperability transition process would involve the warrior with the technicians to ensure the result is what is really needed. Following refinement of the concept, the next step is development of a joint interoperability architecture. This architecture would fashion the Service architectural concepts (some are discussed below) into an integrated whole, coordinated with the CIM initiatives (see Section 4.5). The standardization underlying the architecture would specify services in the form of a joint interoperability standard for the common interfaces. Included in the concept is a "database in the ether, which would have common access protocols and make it unnecessary for the user to have knowledge of the physical location or nature of distribution of the information elements being accessed." [Ref. J6J 1991]

WWMCCS ADP Modernization (WAM) Architecture. A modernization program for the Worldwide Military Command and Control System (WWMCCS) that ends about 1995. An standards-based architecture has been developed by DISA to guide the long-term development of WWMCCS beyond 1995 (see Section 4.6). The initial documents for the WAM Architecture are:

- *A Generic and Target Architecture for Command and Control Information Systems*, Prepared by IDA for DISA, IDA Paper P-2490, September 1991, UNCLASSIFIED.
- *Survey of Technical Standards for Command and Control Information Systems*, Prepared by IDA for DISA, IDA Paper P-2457, September 1991, UNCLASSIFIED.[82]

ATCCS Architecture. The Army Tactical Command and Control System (ATCCS) is the US Army's tactical system-of-systems concept. As shown in Figure 22, the tactical systems are grouped into five battlefield functional areas (BFAs): maneuver control, fire support, air defense, intelligence and electronic warfare (IEW), and combat service support (CSS).

Each functional area for the US Army is planned to have a single BFA control system and a number of subordinate automated and manual BFA systems. The objective control systems are:

- Maneuver Control System (MCS). MCS has been fielded on militarized hardware called the Tactical Computer Terminal (TCT) and nondevelopmental item computers called the Tactical Computer Processors (TCP). Fielding with the ATCCS Common Hardware Software (CHS) is planned with the next version (V11) of the evolutionary development program, planned for FY93. A theater-level maneuver control system, U.S. Army in Europe (USAREUR) Tactical Command and Control System (UTACCS), has been fielded in Europe.
- Advanced Field Artillery Tactical Data System (AFATDS). AFATDS completed concept evaluation (CE) in 1989 and began full-scale development in 1990. When fielded with ATCCS CHS beginning in FY94, AFATDS will replace the Tactical Fire Direction System (TACFIRE), now being used in the heavy divisions, and the Lightweight TACFIRE (LTACFIRE) now being fielded to the light divisions.
- Forward Area Air Defense (FAAD) Command, Control, and Information (C2I). FAAD C2I is a tactical data system being developed with ATCCS CHS that will develop and distribute a low-altitude air defense (LAAD) air picture and C2 information across a division front. Its IOC is planned for FY94.
- All Source Analysis System (ASAS). ASAS was developed in the Joint Tactical Fusion program with the Air Force, whose system was called Enemy Situation Correlation Element (ENSCE). A limited capability configuration (LCC) for ASAS is planned for FY93). When fielded, ASAS will replace the Technical Control and Analysis Center (TCAC, AN/TSQ-130) that is being used in some heavy divisions in the United States and in Europe. Initially ASAS will not be fielded with ATCCS CHS.

---

[82] There is intentionally a strong overlap between WP25 and the WAM standards document, since they both seek to support a standards-based architecture for CCISs in the post-1995 timeframe. As noted in the Preface, much of the WAM standards document was derived from Edition 2 of WP 25 and much of the new material in Edition 3 of WP 25 was derived from the WAM document.

- Combat Service Support Control System (CSSCS). CSSCS will provide a tactical interface to CSS systems deployed to the Continental United States, used in garrison, and fielded for tactical employment. A prototype CSSCS is now under development, but full-scale development of the objective system has not yet begun. IOC with ATCCS CHS is planned for FY94.

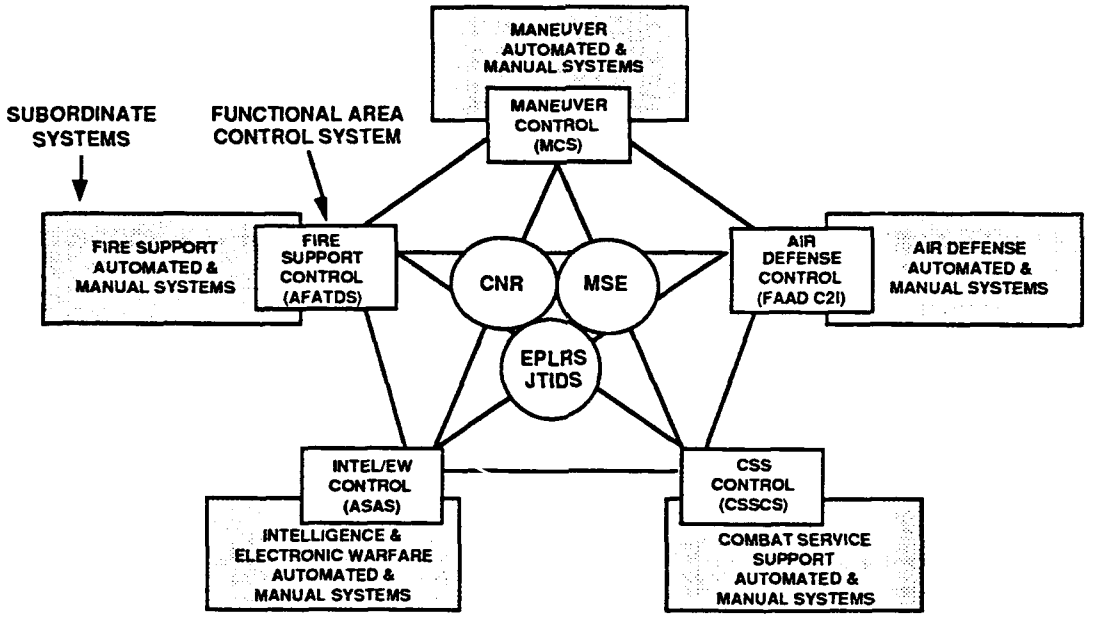


Figure 22. US Army Tactical Command and Control System (ATCCS)

Supporting ATCCS are three types of communications systems. The first is single-channel combat net radio (CNR). The Army has fielded VHF/FM radios such as the AN/PRC-77 and AN/VRC-12 family of radios and is developing the Single-Channel Ground-Air Radio System (SINCGARS). The second type is a switched system called the Mobile Subscriber Equipment (MSE), a military version of cellular radio based on the French-developed RITA system. A packet-switched data communications overlay for MSE has been approved as a preplanned product improvement, but is not funded. The third type of communications is called the Army Data Distribution System (ADDS) and consists of the Enhanced Position Location Reporting System (EPLRS) and the Joint Tactical Informations Distribution System (JTIDS). The data rate for EPLRS will be 2,400-3,600 bits/sec.

A key feature of the ATCCS program is the goal of using common hardware and software (ATCCS CHS) for the five tactical BFA control systems wherever possible. Figure 23 identifies the primary hardware components and identifies in some detail the objective concept for the layers and modules of common software. Modules for all layers would be candidates for automated systems other than BFA control systems as these are developed or improved during the 1990s.

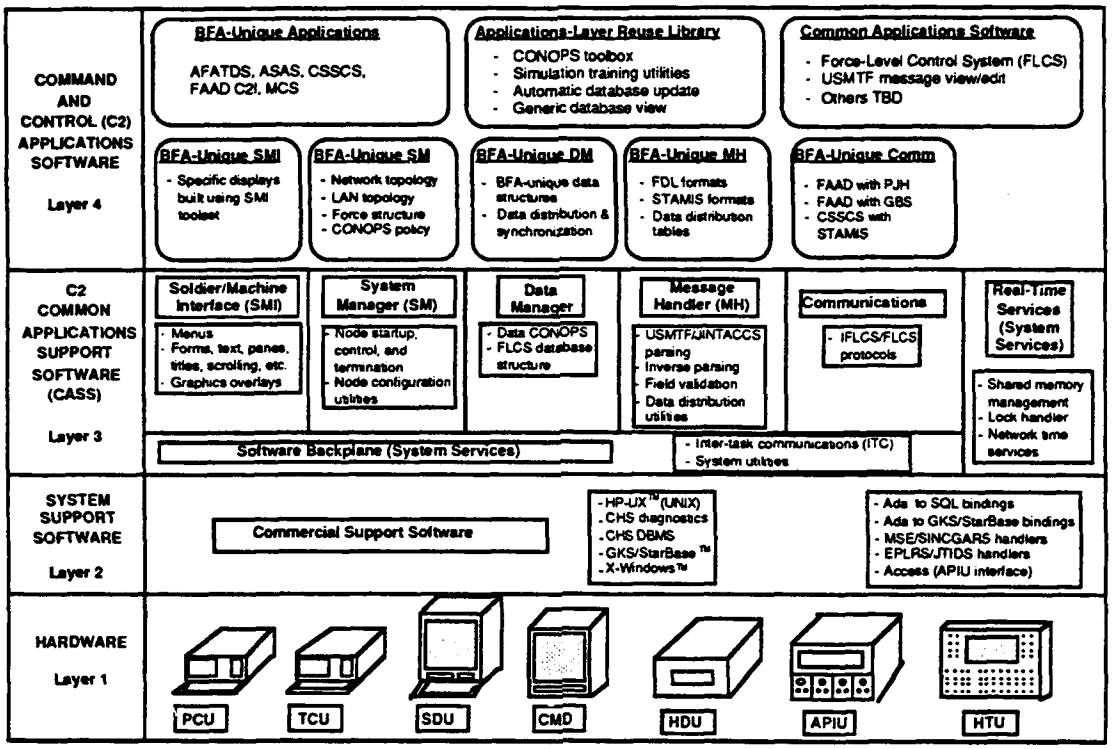


Figure 23. US Army ATCCS Layered Software Reference Model

Layer 1 is the common hardware. The ATCCS computers--the Portable Computer Unit (PCU) and the Transportable Computer Unit (TCU)--are based on a 32-bit Motorola 68020 microprocessor,[83] a 32-bit, 5 Mbits/s data bus, a 3.5-in floppy disk drive, and a 40- or 100-Mbyte removable hard disk cartridge. The PCU supports 1-2 million instructions per second (MIPS) and 4-20 Mbytes of random access memory (RAM), whereas the TCU supports 2-4 MIPS with 4-16 MBytes of RAM. The Standalone Display Unit (SDU) is a 16-in monitor with two[84] configurations: monochrome display with a direct (RS-232) connection to a PCU or TCU or color monitor device (CMD) with keyboard and connection to the standard (ISO 8802.3) local area network (LAN). The PCU has a 25-line (9-in) built-in display. The stand-alone Hard Disk Unit (HDU) is a 152-Mbyte disk drive with an Institute of Electrical and Electronics Engineers (IEEE) 488 interface. The Adaptive Programmable Interface Unit (APIU) provides four modems with multiple interface options (e.g., wire, RS-232, RS-449, COMSEC, combat net radio, packet switching). The Handheld Terminal Unit (HTU), designed as a digital entry device for forward units, weighs 7-10 lb and supports up to four modems.

---

83 A 68030 microprocessor is optional, supporting up to 8 MIPS (at a 33 MHz clock rate).

84 Other options include 16- or 19-in high-resolution color monitor with eight planes (the standard is six planes). A 12-in, four-plane option is also available.

Common software is planned for system support (Layer 2), common applications software support (CASS, Layer 3), and C2 applications software (Layer 4). Layer 2 software is provided with the NDI hardware and includes both UNIX and MS DOS environments (HTU supports only MS DOS). Layer 2 has an Adaenvironment with programming support tools and standard tools accessible via bindings in Adafor graphics [e.g., Graphics Kernel System (GKS) and database management (e.g., Starbase and SQL query interfaces)]. Layer 2 also provides handlers and access codes for the communications hardware and software (e.g., APIU, LAN).

The CASS making up Layer 3 has not yet been developed, although there are a number of promising candidates already coded in MCS and AFATDS. A high-level working group has been formed by the Program Executive Officer, Command and Control Systems (PEO-CCS) to advance CASS specification and development. Work is currently focused on requirements for Inter-Task Communications (ITC), using the design and software from the AFATDS Concept Evaluation (CE) as a baseline. Work is also ongoing in the Soldier-Machine Interface (SMI) and System Manager (SM) areas. The goal of the PEO-CCS is to have as much CASS in the next versions (in 1993) of MCS and AFATDS as possible.

Most of the C2 applications software in Layer 4 could be unique to a battlefield functional area (BFA), but these would be designed with the goal of being able to use the modules at any workstation. This would enable any properly configured CHS workstation to execute modules from two BFAs where required (such as for modules for both fire support and maneuver or for both fire support and force level control). Modules such as tools to support continuity of operations (CONOPS), training, database update, and database views could be used by several, if not all, the functional area control systems.

MTACCS Architecture. The Marine Tactical Command and Control System (MTACCS) concept is shown in Figure 24. One of the tactical C2 systems is specifically assigned the role of a force-level control system to support MAGTF-level C2. Central to MAGTF C2 is ADP support for a MAGTF Database developed from information provided in the four functional areas. These are Ground C2, Aviation C2, CSS C2, and Intelligence. MAGTF C2 provides support to the Commander for information fusion, dissemination, and display; planning; assessment; and tasking. The Marine Corps has developed a Common Application Support Software architecture, similar to the one illustrated in Figure 23 (above) for the Army.

The Ground C2 functional area includes maneuver control and fire support, as well as integration of position location information (PLI). Aviation C2 includes offensive and defensive air support, to include fixed-wing and rotary wing vertical takeoff and landing (VTOL) assault support and antiair warfare (AAW). In addition, Aviation C2 includes control of aircraft and missiles, electronic warfare, and air reconnaissance. CSS C2 provides visibility to the MAGTF and other functional areas as required on logistic assets

and manpower. Intelligence supports MAGTF C2 by providing information on enemy positions, orders or battle, and maneuver indicators.

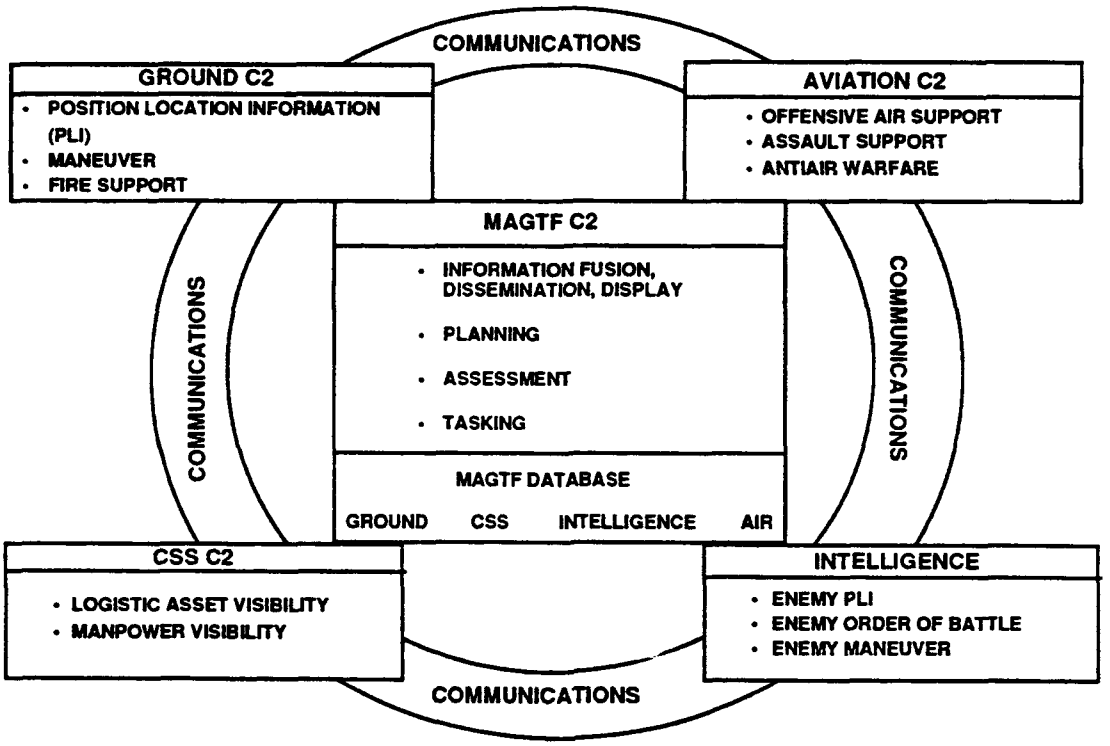


Figure 24. US Marine Tactical Command and Control System (MTACCS)

Copernicus Architecture. Tables 57 and 58 illustrates the Copernicus architecture developed by the US Navy for strategic and tactical systems. Copernicus is a "seamless" information management architecture for Navy command, control, communications, computers, and intelligence (C4I) consisting of four pillars: eight Global Information Exchange Systems (GLOBIXSs), the Command-in-Chief (CINC) Command Center or Complex, four Tactical Data Exchange Information Systems (TADIXSs), and the Tactical Command Center.

Table 57. US Navy Copernicus Architecture--Pillars, IERs, and Functions

Information Management Ashore		Information Management Afloat	
GLOBIXSs A. SIGINT Mgmt B. ASW Mgmt C. SEW Mgmt D. HICOM E. Imagery Mgmt F. Database Mgmt G. RDT&E Coord H. Navy-Wide Administration	**CINC COMMAND COMPLEX** 1. Unified Commands 2. Other Services 3. Navy • FOSIC • FIC • CSG • ASW • SEW • Watch • Research • C2 Center	**TADIXSs** A. Command B. Support C. Direct Targeting D. Force Operations	**TACTICAL COMMAND CENTER** 1. Composite Warfare Coordinator 2. Antiair Warfare Center 3. Anti-Submarine Warfare Center 4. Anti-Surface Warfare Center 5. Space & Electronic Warfare Center 6. STWC
Information Exchange Requirements • Voice • File Transfer • Imagery • Interactive • Messages • Real-Time Data • Video	• Receive & process info • Maintain C2, intelligence, strategic & tactical info • Generate command displays • Support query & response • Provide models & other C2 decision aids • Generate & monitor orders, plans, & related information • Support operator training • Provide system monitoring & control	Information Exchange Requirements • Voice • File Transfer • Imagery • Interactive • Messages • Real-Time Data • Video	• Receive & process info • Maintain C2, intelligence, & tactical information • Generate command displays • Support query & response • Provide models & other C2 decision aids • Generate & monitor orders, plans, & related information • Afloat adaptability • Shipboard training support • Provide system monitoring & control

Sources: *Fleet Communications in the Copernicus Architecture,* Final Draft, 20 June 1991, UNCLASSIFIED; *The Copernicus Architecture,* Briefing to IDA, Space and Electronic Warfare Directorate OP-094 (Capt J.R. Wood), 7 October 1991, UNCLASSIFIED.

Copernicus capabilities will be implemented in a building block approach. Each GLOBIXS will be a global, virtual (not necessarily physically dedicated) network of the Defense Communications System (DCS). Each GLOBIXS will be an afloat virtual network of variable duration (minutes, hours, or days), depending on the information exchange load. The CINC Command Complex consists of workstations; local ares networks; the Base Information Transfer System (BITS--a wideband, local, and metropolitan area network) with network management, security, standards, and protocols; database; and communications servers. The Tactical Command Center has similar capabilities using the newly developed Communications Support System (CSS) instead of BITS.

Table 58. US Navy Copernicus Architecture--Functional Architecture

Model	Component of Architecture	Planned Building Block
Open Systems Architecture	Common Human-Machine Interface	
Common Message and Data Transmission Formats	Software Applications and Utilities	• Data compression software • Sensor-specific data • Cross-correlation data • Data robots • Copernicus tactical software • Common decision support software • Environmental analysis software • Trans-sanitization software • INFOSEC (COMPUSEC, COMSEC) software • Network and system management software
	Application Portability Interface (POSIX Standard)	
Open Systems Standards and Communications Protocols (GOSIP)	Operating Systems	• COTS operating systems (e.g., UNIX, VMS, DOS)
Standard BUS architecture and Hardware Interfaces	Hardware	• Desktop engines (e.g., personal computers) • Workstation engines (e.g., DTC-2, TAC-3) • Communications servers • Data File servers • Display devices • Modular embedded cryptographic devices • STU III COMSEC devices • Interchangeable modems • Standard storage devices
Nondevelopmental Items (NDI) (Commercial off the shelf and government off the shelf)	Network Services from Common User Backbones	• GLOBIXSs (using DDN, DSN, DCTN, TelCo, etc.) • TADIXSs (using CSS: SATCOMs, HF, LOS, etc.) • LANs (e.g., (IC)2, SAFENET, etc.)

Source: *The Copernicus Architecture*, Briefing to IDA, Space and Electronic Warfare Directorate OP-094 (Capt J.R. Wood), 7 October 1991, UNCLASSIFIED.

The Copernicus architecture for the information systems (CINC Command Complex and Tactical Command Center), specifically to address interoperability, has three parts: (1) standards and protocols, (2) security, and (3) network management. As with ATCCIS, the US Navy has determined that homogeneity is not practical and that "users need open systems that provide interoperability of products and portability of people, data, and applications across heterogeneous computing environments." The standards will include POSIX and GOSIP, but these have been determined as "not sufficient to address the full spectrum of needs, even in their range of applications." As a result, the Navy has adopted the APP/OSE developed by NIST to facilitate rapid prototyping, evolutionary acquisition, implementing various computer architectures, refocusing research and development, leveraging research and investment, and achieving the goal of scalability of hardware and software capabilities and standards that will be required in the future. [Ref. COPERNICUS 1991]

For security, Copernicus will use the capabilities development for the DoD ICA, including both end-to-end and multi-level security devices. For network management, Copernicus will use MIL-STD-1813, *Network Management for DoD Communications,* 10 June 1991, developed by NIST.

Air Force Computer-Communications Architecture. The architecture currently addresses base-level applications that are stove-piped and are hosted on a standard base-level computer, but these concepts are evolving to a local information transfer environment with support from regional processing centers. An Air Force Corporate Data Dictionary is being developed. The Air Force software architecture is illustrated in Table 59.

Table 59. US Air Force Software Architecture

User Interface				GOSIP
X-Windows				
Applications				
Commercial Off the Shelf	Tools		Developed	
Word Processors Graphics	CASE Data Dictionary		Ada SQL Data Standards	
POSIX				
Hardware				
Micro-computer	Mini-computer	Mainframe	Supercomputer	

Source: *Air Force C4 Architecture*, Briefing to JTC3A's Objective Architecture Conference, HQ USAF/SCX (LtCol J.M. O'Meally), 19 September 1991, UNCLASSIFIED.

Coast Guard Information Systems Architecture. The Coast Guard has a diversity of requirements stemming from the need to communicate and interoperate with many government agencies. The Coast Guard has developed a standards-based architecture with eight aspects: network standards, hierarchical structure, decision support systems, sensor sub-architecture, information security, public data interface, radio navigation mapping, and command center mapping.

US Army Initiatives. The US Army has a number of initiatives underway that address tactical implementations of OSI standards. The initiatives are under the direction of the Interoperability and Standards Directorate of the Communications-Electronics Command. The Army has an initiative to evaluate OSI protocols (including possible enhancements) in the newly developed Single-Channel Ground/Air Radio System (SINCGARS) combat net radio (VHF-FM). Specifically, the Army is examining options to provide an automatic voice/data contention resolution protocol at the Medium Access Control (MAC) sublayer of the data link layer (Layer 2). Some investigation of a forward error correcting Layer 2 protocol is also ongoing. In addition, an OSI profile is being developed for a local area network (T.LAN). Further, the Army has procured with its

Common Hardware and Software (ATCCS CHS) nondevelopmental item (NDI) program a number of commercial OSI implementations, including ISO 8802.2 and 8802.3 for the local area network (TCP/IP and other DoD protocols will be used initially at layers above Layer 2). CHS has CCITT X.25 switched protocols for wide area networks (these also are used in conjunction with TCP/IP). Finally, the CHS has a standard graphics interface and plans in the next procurement phase to obtain, if possible, a POSIX-conformant operating system.[85]

US Marine Corps Initiatives. The Marine Corps has adopted a Technical Interface Design Plan (TIDP) for Marine Tactical Systems (MTS) [Ref. MTS TIDP 1987] that mandates the use of bit-oriented messages and two functional profiles for protocols in all its command and control systems. One profile for broadcast mode is designed to be used in combat net radio. It has been implemented in the AN/PSC-2 Digital Communications Terminal (DCT). The second profile of protocols is for switched mode and was developed from the Joint Tactical Communications Program (TRI-TAC) Interface Control Documents. This profile has been implemented with the Unit Level Tactical Data Switch (ULTDS). The switched profile is also being implemented with the Tactical Air Operations Module (TAOM) and a developmental system for air operations--Advanced Tactical Command and Control Center (ATACC). Although not fully OSI conformant, the two MTS profiles are based on several OSI standards (ISO 3309, ISO 7809, and ISO 4335). The Marine Corps' approach to data communications standards and profiles follows the OSI seven-layer model and incorporates military features not covered within the ISO standards.

DoD Protocol Suite. Figure 25 shows the DoD Internet protocol suite.[86] The upper layer protocols providing user functionality support file transfer [File Transfer Protocol (FTP),[87] MIL-STD-1780]; electronic mail [Simple Mail Transfer Protocol (SMTP), MIL-STD-1781]; and remote system access [TELNET Protocol,[88] MIL-STD-1782]. The middle layers provide a reliable host-to-host transport protocol [Transmission Control Protocol (TCP) MIL-STD-1778] on top of a connectionless (CL) internetworking protocol [Refs. Internet Protocol (IP), MIL-STD-1777].

---

85 Discussions with staff from the Information Systems Directorate, CECOM, March 1989, UNCLASSIFIED.

86 The figures and information for this section and the following sections on US GOSIP and proposed mixed stacks for Army CCISs is taken from Use of OSI Protocols for US Army Tactical Command and Control Applications, Richard Nieporent and Brajesh Mishra, The MITRE Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

87 FTP provides a simple application for transfer of ASCII, EBCDIC, and binary files.

88 TELNET Protocol provides a simple scroll-mode terminal capability.

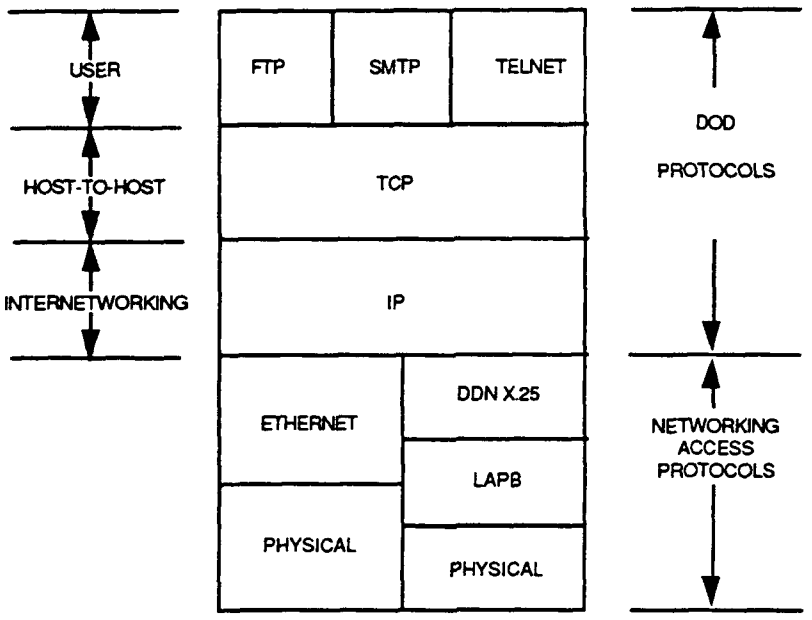


Figure 25. DoD Protocol Suite

No lower layer protocols are specified in the DoD protocol suite--it uses whatever protocols are required to access the network to which it is attached. Thus, for example, the DoD protocol suite uses the Ethernet™ (ISO 8802.3 CSMA/CD Media Access Control for a coaxial cable 10-Mbps LAN) protocol to operate of a local area network and the DDN implementation[89] of the CCITT X.25 protocol (X.25 Packet Level Protocol, ISO 8208) and the HDLC LAPB (ISO 7776) procedures to operate over a wide area packet switching network. Although DoD protocols are not international standards, they have become a de facto open standard in the US--almost every vendor provides the DoD protocols in their version of the UNIX operating system. The DoD protocols are also included in the ATCCS Common Hardware and Software (CHS) procurement and are specified for use over the CHS IEEE 802.3 (ISO 8802.3) tactical LAN. Finally, the DoD protocols are used by the MSE packet switched network (PSN).

The DoD protocol suite has two drawbacks for their use in tactical CCISs:

- They are not US GOSIP compliant. It would be necessary for implementations of the DoD Protocols to undergo an expensive and time-consuming transition to satisfy the GOSIP mandate. In particular, the battlefield functional area (BFA) applications will have to be modified to use the functionality of the GOSIP protocols.
- GOSIP Application Layer protocols provide more functionality than the DoD protocols. Moreover, more effort is now being committed by the nations for the OSI protocols than by the US in the DoD arena. As new OSI protocols are

[89] The DDN implementation of X.25 was provided by Bolt Beranek and Newman. It is also planned for use in the Mobile Subscriber Element (MSE) for Army area communications.

developed that meet tactical communication requirements, they are expected to be incorporated in GOSIP. Thus, future versions of GOSIP are expected to provide considerably more functionality than the DoD protocol suite.

Version 2 of US GOSIP. Figure 26 summarizes the US GOSIP protocol suite for Version 2 (see Figure 21 in Section 14.4.3 for the complete diagram). The applications supported are the same as the DoD protocols: file transfer (FTAM, ISO 8571), electronic mail (MHS, CCITT X.400-series 1984 recommendations;[90] and MOTIS, ISO 10021 and 9066], and the Virtual Terminal Protocol (VTP, ISO 9040 and 9041). Also, like the DoD protocol suite, a transport protocol (Transport Class 4, ISO 8073) is specified that will provide reliable host-to-host communications, and a CL network protocol (CLNP, ISO 8473) is specified for internetworking. Unlike the DoD protocols, US GOSIP provides for the Layer 7 Association Control Service Element (ACSE, ISO 8650), connection-oriented protocols for the Presentation Layer (ISO 8823, Layer 6), and connection-oriented protocols for the Session Layer (ISO 8327, Layer 5).

However, unlike the DoD protocol suite, GOSIP explicitly specifies a number of network access protocols, including IEEE 802 (Logical Link Control, ISO 8802.2; CSMA/CD, ISO 8802.3; Token Bus, ISO 8802.4; and Token Ring, ISO 8802.5) for communications over a LAN and the X.25 protocol for wide area packet switch network communications.

There is one major disadvantage to using GOSIP in Army CCISs now. The MSE PSN internetworking capability for tactical area communications can not be used with GOSIP, since GOSIP has a different internetworking protocol (CLNP) than the DoD protocol suite (IP). Access to the MSE PSN will still be possible using a direct interface to the tactical LAN.

Mixed Protocol Stacks for Future Army CCISs. The US Army is developing an automated Army Tactical Command and Control System (ATCCS) for the tactical battlefield. Communications connectivity for the ATCCS will be provided by the US Army's local and wide area tactical communications networks. A protocol suite must be selected for the ATCCS that can interface to these tactical networks and support a wide range of tactical communications applications. A mixed protocol suite, consisting of OSI upper layer protocols operating of the US DoD transport and internetworking protocols (TCP/IP), has been recommended to support the required ATCCS functionality and interoperability and provide a direct migration path to US GOSIP and the NATO militarized OSI protocols.

---

90 US GOSIP 1.0 and 2.0 mandate use of X.400(MHS)-1984. US GOSIP 3.0 is expected to require X.400(MHS)-1988.

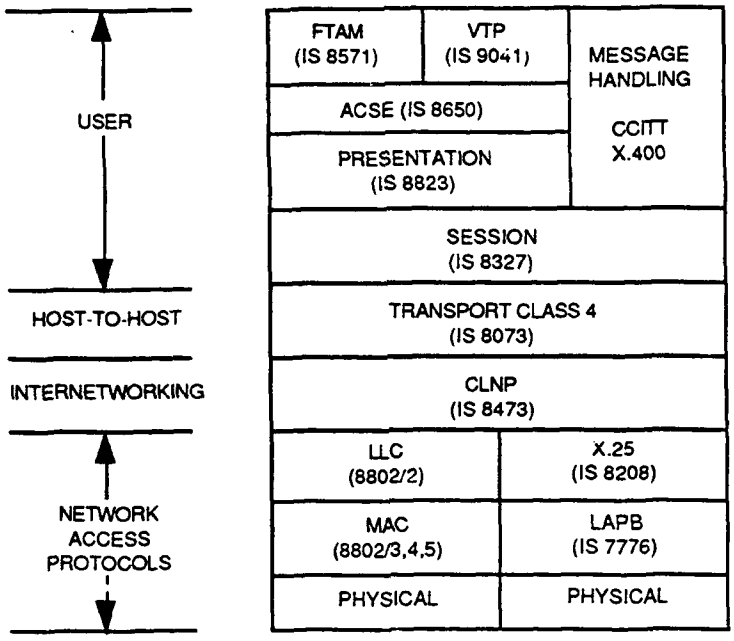


Figure 26. US GOSIP Protocol Suite, Version 2

Figure 27 shows a proposed mixed suite of protocols for ATCCS. The upper three layers consists of the GOSIP Session, Presentation, and Application Layers. The same FTAM, X.400, and VTP Application Layer protocols are specified as in GOSIP. The middle protocol layers are the same as in the DoD protocol suite: TCP and IP. Also, as in the DoD protocol suite, the lower layer protocols (Physical, Data Link, and Network Layers) are unspecified.

The mixed protocol suite has the increased functionality of the GOSIP Application Layer protocols, without sacrificing compatibility with the MSE PSN. No changes will be necessary in BFA applications, when ATCCS transitions to GOSIP, since they would already use the GOSIP Application Layer protocols. [Ref. Nieporent et al. 1990]

A Convergence Protocol [Request for Comment (RFC) 1006, *ISO Transport Service on Top of the TCP*, Version 3, 1987] is needed to interface the GOSIP upper layer protocols to the DoD internetworking protocols. The Convergence Protocol provides OSI Transport Class 0 (TP0) along with a packetization protocol.[91] This protocol is commercially available in Version 6.0 of the ISO Development Environment (ISODE).

[91] Since TCP is a stream-oriented protocol and TP0 is a block-oriented protocol, the packetization protocol is needed to preserve the OSI packet boundaries.

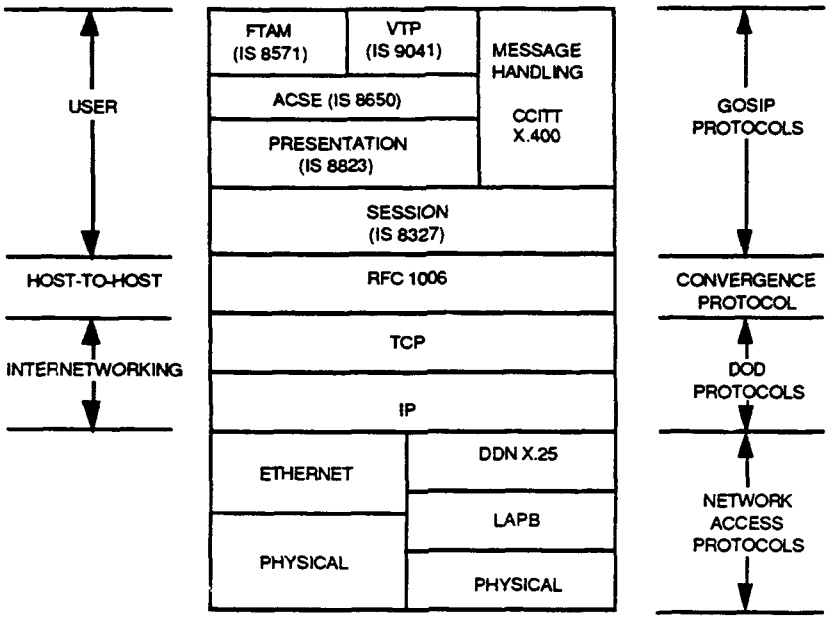


Figure 27. Proposed Mixed Protocol Suite

17.2 Identification of Efforts to Evaluate the Performance of Civil Standards for Military Use

This section identifies a number of papers submitted in June 1990 to the Military OSI Symposium at SHAPE Technical Centre that describes analytical and demonstration efforts to evaluate the performance of OSI and other protocols for use in military systems. These papers should be consulted for detailed results.

17.2.1 Sources of Reports on Performance Evaluations

Practical Evaluation of OSI Protocols. This paper summarizes work being done under the Robust Protocols Research Programme at the Royal Signals and Radar Establishment (RSRE) in the U.K. MOD. As noted in Section 2.3, the work has concentrated on X.400 and FTAM over TP4, CLNS, and X.25. [Ref. Price 1990]

User Performance of Tactical Networks in the ITDN. User performance experiments were conducted in 1989 on portions of the Integrated Tactical-Strategic Data Network (ITDN) Demonstration that simulated tactical areas at echelons corps and below. The performance of four tactical links [Fleet Satellite Communications (FLTSATCOM), MSE line-of-sight radio, Tactical Satellite Communications (TACSATCOM), and Very Small Aperture Terminal (VSAT)] was measured at the protocol level that most directly affects the network user. The results, though preliminary, can help predict the performance of applications in tactical nets. US DoD protocols were measured; however, the results may provide the basis for informed conjectures about the user-level performance of OSI protocols. [Ref. Reichlen 1990]

Transport Protocols and Internetworking in Low Bandwidth Tactical Networks. This paper examines the impact of packet size on end-to-end functionality (including reliable delivery, packet resequencing, segmentation, and flow control). Tradeoffs between a small packet size required because of the unreliable media and a large packet size required to minimize the header overhead are considered using standard transport protocols. The choice of ULP depends on the application required to run over the network; for instance, military messaging application could use X.400 and its supporting presentation and session layers as specified in US GOSIP or the enhanced versions proposed in STANAGs 4265-4269. The paper also assess the impact of the transport protocol selection on the network architecture in an internetwork configuration. [Ref. Bahnji 1990]

(This page intentionally left blank.)

18. CONCLUSIONS AND RECOMMENDATIONS

This section summarizes the gaps in current and planned standards coverage and identifies possible courses of action for addressing these deficiencies. In addition to the four Basic Facilities, Table 60 depicts other elements of the ATCCIS architecture and shows their relation to the five groups of standards:

- Application-level facilities (ALFs)--provide automation support for command and control key tasks.
- Man-machine interface (MMI) service facility (MSF)--provides the functionality for a generalized interface between ALFs and users, irrespective of the particular devices used to interact with users and the human-computer interface they implement.
- Input-output facilities (IOFs)--provide an interface between an ATCCIS-conformant system and a particular class of non-ATCCIS-conformant systems. Example profiles for an IOF are the STAMINA profile and the Quadrilateral Interoperability Programme profile, both discussed in Chapter 16.

Table 60. Summary of Standards in the Eight Service Areas and Their Relation to ATCCIS Basic and Other Facilities

Data Manage -ment	Network	Operating System Interface	Security & OSI System Management	Data Inter-change	User Interface	Graphics	Program-ming
ATCCIS DMF	ATCCIS TF & IOFs	ATCCIS SCF	ATCCIS SMF & Others	ATCCIS DMF	ATCCIS MSF	ATCCIS DMF & MSF	ATCCIS ALFs
Chapter 5	Chapter 6	Chapter 7	Chapter 8	Chapter 9	Chapter 10	Chapter 11	Chapter 12
SQL SQL2 SQL3 IRDS RDA ISAM TP ODP Data Elements	OSI RM X.400 MHS FTAM X.500 Dir. JTM ACSE CCR ROSE RTSE RPC ASN.1 BER PROFILES GOSIP EPHOS	POSIX OSCRL	NOSA SANISI ISO 7498-2 Security Frameworks Sec. Protocols P1003.6 SDNS BLACKER Systems Mgmt. Mgd. Objects CMIS CMIP Conf. Testing Estelle SDL LOTOS Reg. Authorities	ODA ODIF SGML EDI DTAM DFR RDT	HCI X-Windows Drivability UIMS Toolkit VDT TM MOTIF VT	GKS PHIGS	Ada Pascal C COBOL BASIC FORTRAN LISP Bindings CASE Tools CAIS PCTE PCIS IEEE Software Engin. Stds

18.1 OSI Technical Standards

While TSGCE has identified and assessed eight military features that need to be incorporated in commercial OSI standards for use in military systems, little detail has yet been released (e.g., in drafts of STANAGs 4251-4266) to show how these features can actually be addressed in military versions of OSI standards. WG1 and WG2 of TSGCE SG9 are continuing to progress drafts of such standards, but it is too early to assess the degree to which the military features will be provided. TSGCE SG9 has an ambitious 18-month plan for progressing the NATO OSI data communications standards, but without increased support from the Nations it does not appear that all the stated objectives will be reached. It appears unlikely that a stable set of NATO OSI standards addressing the full range of OSI options will be approved before the mid-1990s. Also, efforts to incorporate military requirements in civil standards and initiatives to obtain commercial products with the desired military features may not be successful until the late 1990s. Clearly, with limited resources, an evolutionary plan is needed that reflects carefully analysed priorities for progressing NATO technical standards for OSI and other open systems capabilities.

There is a need to reassess and revalidate the military features that are the basis for the work by TSGCE and the Nations to ensure military requirements will be met by the standards to be adopted. The initial views on the required military features developed in the early 1980s were based, to some degree, on concepts to support manual communications centers. Experience since that time with automated communications facilities could lead the reassessment to different results on what military features are not yet supported by civil standards. As an example, fewer levels of precedence might be acceptable than were previously determined, and different measures of quality of service might be defined.

There is a need to identify additional resources and possibly new approaches to expedite the completion of the initial OSI data communications STANAGs. The scope and diversity of the applicable OSI and OSI-related standards activities in the civil sector is expanding rapidly. Some features needed by the military are already being addressed by existing and emerging international standards. Initial OSI data communications STANAGs are needed as soon as possible to provide a concrete step in the transition strategies for the NATO nations and agencies. The work plans by TSGCE SG9/WG1 and SG9/WG2 address many of the important technical areas, but these groups are having difficulty in maturing the full set of draft STANAGs in a timely fashion.

A significant issue regarding military features for OSI technical standards is whether these features can be specified as extensions or options to the commercial standards or, alternatively, whether some of the features mandate deviations and hence noncompliance with the base commercial standards. Whenever military features can be provided through extensions or new options to existing commercial standards, the specifications for the services and protocols could be offered to the international standards bodies and the nations could seek to have these changes made part of the standard. In such

cases, commercial implementations of the military features could be expected at a much lower cost than if military-unique deviations had to be supported.

If NATO and the nations are not successful in defining the military features or if they are not fully addressed by the international commercial standards, as either extensions or options, then the following actions should be considered, presumably by TSGCE:

- Assess the functionality of the ISO/CCITT standards against the proposed military requirement
- Assess the operational impact of not meeting the requirement in CCISs for data communications
- Identify cost(s) associated with implementing a nonconformant, military-unique standard
- Refer the results back to an operational body within NATO to determine if the added functionality is cost-justified in accordance with memorandum of agreement procedures.

18.2 Other Technical Standards

Data standardization is needed to support the development of ATCCIS. Since data standardization addresses the representation of data as well as data management, data element standardization, and naming conventions, it requires not only technical but also procedural and operational standards. Data standardization issues and recommendations are addressed in WP 7L, *Operational and Procedural Requirements for Data Management and Standardization.*

18.3 Recommendations

The following recommendations are made in the area of progressing the technical standards:

a. TSGCE SG9 should continue the current efforts to reassess and revalidate the military features that do not appear to be provided by existing and emerging civil standards.

b. TSGCE should identify additional resources and possibly new approaches to expedite the completion of the initial OSI data communications STANAGs. As examples, the nations could increase the resources provided to TSGCE SG9 and more active participation by civil agencies and contractors could be considered.

c. The nations should seek wherever possible to influence the international and national standards bodies to incorporate the military features identified by TSGCE SG9 into the civil standards. Specifically, the nations should support initiatives in ISO to expand work in areas of interest to the military. Examples are the ISO questions on whether to continue architectural work on multipeer data transmission and on quality of service.

d. The military organizations of the nations should actively participate in international and national civil standards bodies to ensure that military requirements are addressed by the emerging open systems standards.

e. TSGCE should adopt International Standardized Profiles whenever possible and should seek international recognition of additional profiles where they are needed for military systems.

f. TSGCE should develop and adopt a plan to ensure that a set of NATO OSI STANAGs is available in the mid-1990s, even if adopting this plan means postponing the incorporation of some low priority requirements. This plan, including a schedule for the release of the OSI STANAGs, should be included in the next draft of the *NTIS Transition Plan* developed by TSGCE SG9.

g. The *NTIS Transition Strategy* should be expanded to include additional standards and specific profiles of standards recommended for use by ACCS, ACE ACCIS , ATCCIS, BICES, and other major NATO projects until a complete set of NATO OSI STANAGs have been promulgated.

   (1) The profiles should include support for the exchange of information through database-to-database transfers as well as for STANAG 5500 messages and the data link to replace Link 1 (as required by ACCS).

   (2) The profiles should include support for ISDN.

   (3) The standards should include those for graphics interfaces and language bindings, document and picture interchange, remote data access, the reference model for data management, transaction processing, and open distributed processing.

APPENDIX A

THE USE OF INTEROPERABILITY PARAMETERS TO ENSURE STANDARDS COVERAGE

THE USE OF INTEROPERABILITY PARAMETERS TO ENSURE STANDARDS COVERAGE

1. INTEROPERABILITY PARAMETER METHODOLOGY

1.1 General

This section describes a methodology for ensuring adequate standards coverage through detailed analysis of the parameters that are required to achieve interoperability against specific standards that control these parameters.

1.2 Description of the Methodology

An Interoperability Parameter (IP) is a system or design parameter whose control is required to achieve interoperability. These parameters are identified in system specifications, interface control documents, and other requirements documents prior to or very early in the system development process. In many cases, the interoperability parameters are controlled through the specification of a range of standards. The assembled parameters act as a checklist for interoperability, since each IP must be controlled by a suitable standard. The purpose of an analysis using IPs is to recognize and examine all relevant quantities and characteristics in a direct manner, instead of assuming that existing or draft standards will provide adequate coverage of the quantities.

One of the underlying principles for the ATCCIS concept is that specifying standards is essential to ensuring interoperability. However, it cannot be emphasized too strongly that specifying standards alone will not guarantee interoperability. Indeed, every standard has a number of design parameters or IPs whose values may need to be fixed in the design phase of implementation. To ensure interoperability, each of these IPs must also be specified and controlled. Some IPs are very general and may be used to specify a class of options or mode of operation. Other IPs may be very detailed, such as restrictions on timing, format size, or bandwidth.

IPs can be identified and appropriately controlled in any stage of system development, from initial concepts and requirements to detailed design and as-built specifications. Parameters may simply be the identity of governing specifications (e.g., standards) for interface or other requirements. They could be the identity of options or specification of limits on performance requirements. They could include lists of services or routines that are mandated or that are denied for use. IPs may include logical or physical layouts that show such elements as sequences, relationships, interconnections, and logical block diagrams. IPs may include waveforms. They may include operating procedures, such as dial settings. In short, IPs include any information item that needs to be controlled at any stage of development to ensure interoperability.

Because each standard is a reflection of the degree to which agreement can be reached in a service area, many important attributes (i.e., IPs) are often left unspecified or unaddressed. As agreements are reached over time, the standards will improve by addressing more functionality and harmonizing conflicting approaches. In cases where standards identify extensions and other types of options, great care must be taken in standards specification and IP control to ensure that, whenever an extension or option is permitted, every implementation of the related service also supports this extension or option. This principle is especially important in achieving not only interoperability but also portability of applications from one implementation or environment to another, such as is needed when operating systems, data management systems, interface packages, and hardware are upgraded.

1.3 Examples of Interoperability Parameters

This section provides a brief introduction to interoperability parameters by examining portions of three sets of standards:

- Physical standards for 25-pin connectors (i.e., EIA RS-232D interface)
- Electrical characteristics of digital interface circuits (i.e., EIA RS-423A and QSTAG 594)
- Transmission characteristics for single channel radio (i.e., STANAG 4202).

1.3.1 Physical Standards for 25-pin Connectors

Table A-1 identifies a number of electrical and mechanical interoperability parameters controlled by EIA RS-232D for 25-pin connectors. The first two columns provide the definition of the interoperability parameter; the values specified in the standard, if any, are given in the third column.

Table A-1. Example Interoperability Parameters Based on Characteristics of Unbalanced Load Digital Interface Circuits, 25-Pin Interface Connectors

Description of Interoperability Parameter		Example Value of IP
EXAMPLE ELECTRICAL CHARACTERISTICS:		
Undefined condition	Minimum voltage Maximum voltage	-3 volts +3 volts
Marking condition (binary ONE)	Interface Voltage Maximum	-3 volts
Spacing condition (binary ZERO)	Interface Voltage Minimum	+3 volts
Restriction on use of hysteresis techniques to enhance noise immunity		None
Load impedance of the receiver side	Minimum for applied voltage ≤ 25 volts Maximum for applied voltage of 3 to 25 volts	3,000 ohms 7,000 ohms
Effective shunt capacitance of receiver	Maximum	2,500 picofarads
EXAMPLE MECHANICAL CHARACTERISTICS:		
Number of Pins		25
Cable length	Maximum	Not specified
Connector length (male contacts, female shell)	Minimum Maximum	38.84 mm 39.09 mm
Connector width (male contacts, female shell)	Minimum Maximum	8.23 mm 8.48 mm
Contact spacing, Pin #1	Longitudinal offset Lateral offset	+16.56 mm +1.42 mm
Contact spacing, Pin #2	Longitudinal offset Lateral offset	+15.19 mm -1.42 mm
Contact spacing, Pin #25	Longitudinal offset Lateral offset	-16.56 mm +1.42 mm

Table A-1. (Continued)

Description of Interoperability Parameter		Example Value of IP
Pin diameter	Minimum	0.98 mm
	Maximum	1.06 mm
Pin length, overall with mounting	Minimum	9.77 mm
	Maximum	10.03 mm
Pin mounting length	Minimum	1.57 mm
	Maximum	1.76 mm
Female contact length, overall with mounting	Minimum	9.27 mm
	Maximum	9.63 mm
Female contact socket depth	Minimum	7.37 mm
	Maximum	7.37 mm
Pin assignment	Pin #1	Shield
	Pin #2	Transmitted Data (BA)
	Pin #5	Clear to Send (CA)
	Pin #25	Test Mode (TM)
Female contact socket depth	Minimum	7.37 mm
	Maximum	7.37 mm

Sources:

(1) DIS 2110, *25-Pin DTE/DCE Interface Connector and Pin Assignments* (related to EIA RS-232C), November 1985.

(2) EIA RS-232D, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange,* 1986.

(3) EIA RS-449, *General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange,* November 1977.

(4) EIA Industrial Electronics Bulletin IEB-12, *Application Notes on Interconnection Between Interface Circuits Using RS-449 and RS-232C,* November 1977.

1.3.2 Electrical Characteristics of Digital Interface Circuits

Table A-2 identifies interoperability parameters of digital interface circuits that are controlled by QSTAG 594. These are all electrical characteristics.

Table A-2. Example Interoperability Parameters Based on Electrical Characteristics of Unbalanced Load Digital Interface Circuits

Description of Interoperability Parameter		Example Value of IP
Open circuit voltage, generator	Minimum magnitude Maximum magnitude	4 volts 6 volts
Test termination voltage, generator	450 ohm ±1% test load min	90% magnitude of open circuit voltage
Short circuit current, generator	Maximum magnitude	150 mA
Output leakage current, current, generator	Maximum magnitude with applied voltage from -6 V to +6 V	100 µA
Output signal waveform voltage	Minimum magnitude Maximum magnitude Variance between transitions	3.6 volts 6 volts Within 10% steady state
Output signal waveshaping	Rise time to 90% steady state at maximum signaling rate Minimum Maximum Rise time to 90% steady state at signaling rates below 1 kb/s Minimum Maximum	 0.1 unit interval 0.3 unit interval 100 µsec 300 µsec
High impedance state	Requirement Output voltage at high imped and 450 ohm ±1% test load	Optional Zero (nominal)
Wire or cable	Characteristics	Not addressed
Signaling rates		Not specified
Total load	Resistance minimum Required differential input voltage to achieve intended binary state	400 ohms 200 mV
Fail safe	Requirement	Optional

Sources:

(1) QSTAG 594, *Electrical Characteristics of Digital Interface Circuits*, 25 March 1981 (adopts MIL-STD-188-114).

(2) MIL-STD-188-114A, *Electrical Characteristics of Digital Interface Circuits*, 30 September 1985 (Revision of MIL-STD-188-114 dated 24 March 1976).

(3) CCITT V.10/X.26, *Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use With Integrated Circuit Equipment in the Field of Data Communications*, 1985 (related to EIA RS-423A, which is compatible with MIL-STD-188-114A).

(4) EIA RS-423A, *Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits*, December 1978.

1.3.3 Transmission Characteristics for Single Channel Radio

Table A-3 presents a nearly complete summary of the interoperability parameters controlled by STANAG 4202 for single channel radios. This standard is in use in NATO as the basis of interoperability for digital data transmission on combat net radio.

Table A-3. Example Interoperability Parameters Based on Single Channel Radio Standards (STANAG 4202)

Description of Interoperability Parameter		Example Value of IP
Frequency band	Minimum frequency Maximum frequency Channel spacing	Not specified Not specified Not specified
Transmission rates (1)	Preferred rate Other required rates	600 b/s 300, 1,200 (and 150 for HF)
Modulation	Type	FSK
Data	Character coding type	NATO 7-bit
FSK modulation	Mark (or 1) frequency Space (or 0) frequency Audio tone frequency accuracy, transmit Receiver accuracy	1575 Hz 2425 Hz ± 5 Hz (± 1 Hz desired) ± 20 Hz
FSK transition between mark & space	Maximum phase discontinuity	5 degrees
FSK timing	Minimum clock accuracy for synchronous data	± 1 part in 10**5
Keytime delay	Required Options Modulation applied	0.53333, 2.026676 sec Multiples of 0.10667 sec (2) Reversals ending in a zero
Bit synchronization preamble	Length Modulation	33 bits Reversals ending in a "1"
Character synchronization preamble	Length Modulation	63 bits Pseudo-random sequence generated by a (6,1) shift register starting with "111111"
Message preparation for transmission follows)	Initial character Message structure Message padding	"SI" or "NUL" (clear, respectively, encrypted text 7-bit bytes Up to 6 "1" bits
Cyclic redundancy check (applied to the entire input message)	CRC type Generator (mod 2) Conversion to 8-bit byte Size of check CRC padding	Polynomial x**16+x**12+x**5+1 0 in most significant bit Three 7-bit bytes NATO 7-bit end-of-text chars as required (up to 15) (3)
Envelope termination	Size	Four 7-bit characters NATO 7-bit end-of-text chars

Notes:

(1) STANAG 4202 (Appendix B) provides guidelines for interim use of 16,000 b/s channels that are not shown in this table.

(2) 0.10667 sec is the time to send 128 bits at 1,200 b/s or 64 bits at 600 b/s.

(3) The minimum message is 16x7 or 112 bits and requires 0.19 sec at 600 b/s.

Table A-3. (Continued)

Description of Interoperability Parameter		Example Value of IP
Error detection and correction coding (applied to 7-bit bytes)	ED&C type	Hamming (12,7), produces 12-bit coding for every 7-bit byte
Time dispersal coding	TDC interleaving array size	16x12, with sixteen 12-bit Hamming codes
Errors	Number of acceptable but uncorrectable errors	None (stop processing and send no NACK)

Source: STANAG 4202 EL (Edition 2), *Transmission Envelope Characteristics for High Reliability Data Exchange Between Land Tactical Data Processing Equipment Over Single Channel Radio Links*, Military Agency for Standardization, NATO, 25 May 1988.

1.3.3 Interoperability Parameters for X.25 Packet Switching

Table A-4 provides the interoperability parameters for the Implementor's Agreements on the X.25 packet switching protocol as defined in the 1989 NIST Workshop stable agreements that apply to U.S. GOSIP Version 1.0.[1] The NIST Workshop understands that agreement to these interoperability parameters will ensure interoperability of implementations of the X.25 protocols.[2]

2. USING INTEROPERABILITY PARAMETERS TO CHARACTERIZE MILITARY FEATURES IN OSI-RELATED TACTICAL STANDARDS

This section is intended to be expanded to demonstrate the use of interoperability parameters to describe how some fielded tactical data systems are implementing military versions of OSI standards to achieve interoperability. The descriptions here extend the tables provided in Chapter 9 to describe the Quadrilateral Interoperability Program and STAMINA. Examples will also be taken from Appendix C, National Initiatives for Military Use of OSI Standards.

---

1 *Stable Implementation Agreements for Open Systems Interconnection Protocols*, Version 2, Edition 1, NIST Special Publication 500-16, National Institute of Standards and Technology, December 1988, UNCLASSIFIED.

2 Private communication with Director, Systems and Network Architecture Division, NIST, 25 May 1989.

Table A-4. Interoperability Parameters for X.25 Packet Switching

ISO Layer & Function		Standards Cited	Notes on Interoperability Parameters
-	General	CCITT X.25	• Defines procedures required to describe the DTE side of a CTE/DCE interface for systems attached to subnetworks providing an X.25 interface shall be as defined in ISO 7776 and ISO 8208 as indicated below. • These procedures shall also apply to a DTE operating on a DTE/DTE interface.
3	Network Layer	ISO 8208 (X.25 PLP)	• The elements of ISO 8208 applicable for use depend on the OSI role of ISO 8208 (i.e., provision of CONS, support of CLNP): a. When ISO 8208 is used to support CONS, the optional user facilities in Section 5.1 of ISO 8878 shall be supported. b. When ISO 8208 is used to support CLNP (when providing the CLNS), Permanent Virtual Circuit may be used. • Virtual Call Service is required. • Any mutually agreed window and packet size may be used; however, all DTEs must be capable of supporting a window size of 2, a packet size of 128 octets, and a sequence number modulus of 8. • The Basic RPOA Selection Facility shall be implemented and its use or non-use selectable on a per virtual call basis. (1)
2	Data Link Layer	ISO 7776 (HDLC Procedures-- X.25 LAPB)	• The address assignments are: DTE = A (=11000000 binary) DCE = B (=10000000 binary). On a DTE/DTE interface, one of the DTEs, by a prior agreement, shall use the DCE address. • The modulus shall be 8. • A window size (k) of 7 shall be supported. In addition, other window sizes may also be supported. • The Multilink Procedures are excluded.

Notes:

1. Agreement on the Basic RPOA Selection Facility parameter is an ongoing, not a stable, implementation agreement.

References:

1. *Stable Implementation Agreements for Open Systems Interconnection Protocols,* Version 1, Edition 1, NIST, December 1988.

2. *Ongoing Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements*, NISTIR 88-3824-2, NIST, February 1989.

(This page intentionally left blank.)

APPENDIX B

FUNCTIONAL PROFILES IDENTIFIED IN THE NTIS TRANSITION STRATEGY

FUNCTIONAL PROFILES IDENTIFIED IN THE NTIS TRANSITION STRATEGY

1. INTRODUCTION

The *NATO Technical Interoperability Standards (NTIS) Transition Strategy* is developed by the Tri-Service Group on Communications and Electronics (TSGCE) and promulgated by the Conference of National Armaments Directors (CNAD). This appendix identifies the functional profiles identified in the November 1991 *NTIS Transition Strategy* (Sixth Edition). All are based on existing or emerging recommendations developed by international or regional standards bodies. Most are based on recommendations from the European Workshop for Open Systems (EWOS).

The notation used to identify and distinguish the functional profiles is that currently being used by EWOS. This notation will be changed in future editions of the *NTIS Transition Strategy* to the taxonomy developed by ISO in TR 10000. The ISO taxonomy is described in Section 6.4.2.

2. APPLICATION PROFILES

There are six functional profiles identified in Figure B-1:

- AFT11, Simple File Transfer (unstructured)
- AFT12, Positional File Transfer (flat)
- AFT22, Positional File Access (flat)
- AFT3, File Management
- AMH21, Message Handling Service: Interpersonal Messaging (IPM): IPM End System to IPM End System
- AMH22, Message Handling Service for IPM: User Agent (UA) to Message Store (MS).

7	ISO 8571 ISO 8650
6	ISO 8823 ISO 8824 ISO 8825
5	ISO 8327

(a) A.111, Simple File Transfer

7	CCITT - T.60
6	CCITT - T.61
5	CCITT - T.62

(b) A.221, Basic Teletex

7	IPM service MT service MT protocol Reliable transfer Association control	ISO 10021-7/X.420 ISO 10021-4/X.411 ISO 10021-6/X.419 ISO 9066-2 ISO 8650
6		ISO 8823 ISO 8824 ISO 8825
5		ISO 8327

(c) A.331, Message Handling Service: Interpersonal Messaging: IPM End System to IPM End System

7	MS service IPM service MT service MT protocol Remote Operations Reliable transfer Association control	ISO 10021-5/X.413 ISO 10021-7/X.420 ISO 10021-4/X.411 ISO 10021-6/X.419 ISO 9072-2 ISO 9066-2 ISO 8650
6		ISO 8823 ISO 8824 ISO 8825
5		ISO 8327

(d) A.332, Message Handling Service: Interpersonal Messaging: UA to MS

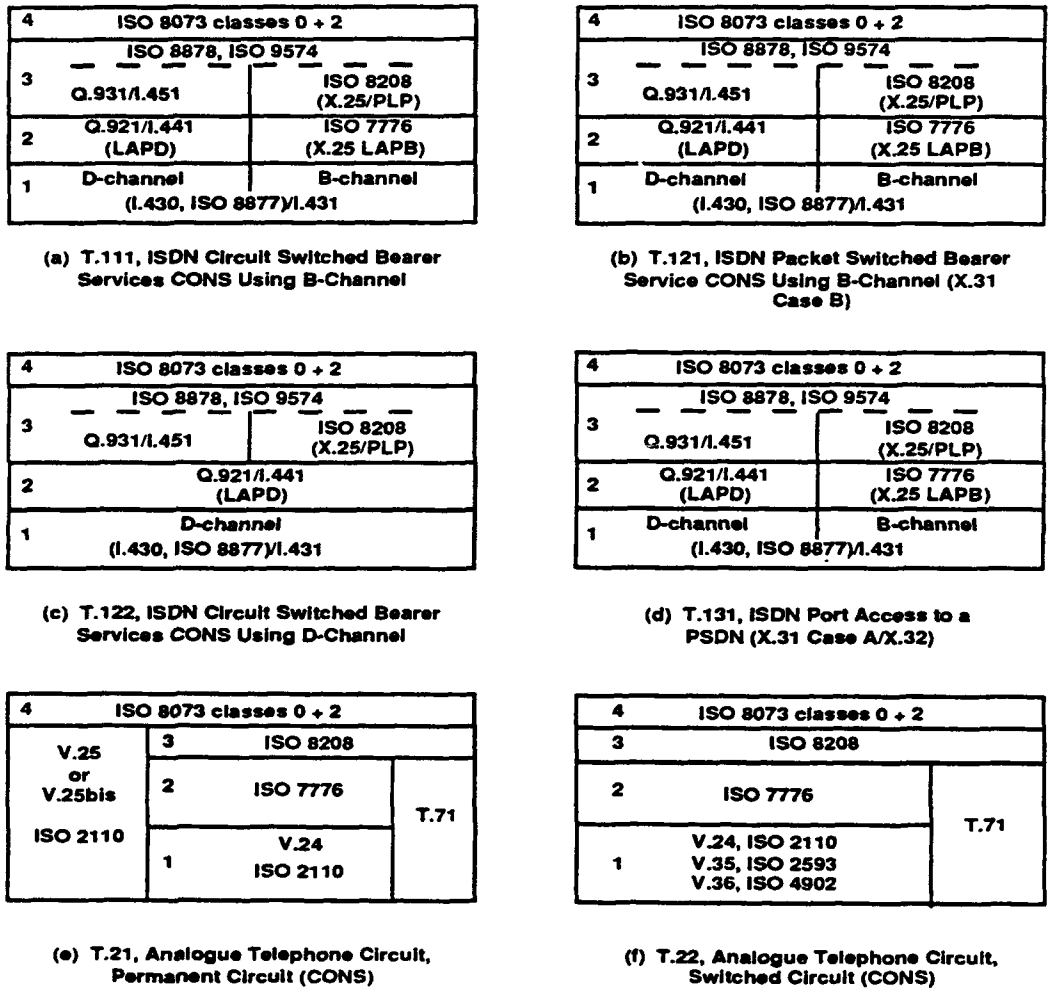
Figure B-1. Application Functional Profiles

3. TRANSPORT PROFILES

Figure B-2 identifies 20 transport profiles. T-profiles use the connection-oriented transport service (COTS): TA involves the use of the connectionless network service (CLNS); TB, TC, and TD all involve

the connection-oriented network service (CONS) and differ as to the required classes (TP0, TP2, TP4) of the COTS. [U-profiles (no examples given) use the connectionless mode transport service (CLTS)]. The first four transport profiles [B-2(a) to B-2(d)] are for a packet-switched digital network (PSDN) :

- TC11xy,[1] Permanent Access to a PSDN Using COTS) and T.70/CONS
- TD11xy, Permanent Access to a PSDN Using COTS and T.70/CONS
- TC113x, TD113x, TC1231, TD1231: ISDN Port Access to a PSDN, X.31/X.32 (X.31 case A/x.32)
- TC1211, TD1211, TC1221, TD1221: Switched Access to a PSDN Using COTS and T.70/CONS.



(a) T.111, ISDN Circuit Switched Bearer Services CONS Using B-Channel

(b) T.121, ISDN Packet Switched Bearer Service CONS Using B-Channel (X.31 Case B)

(c) T.122, ISDN Circuit Switched Bearer Services CONS Using D-Channel

(d) T.131, ISDN Port Access to a PSDN (X.31 Case A/X.32)

(e) T.21, Analogue Telephone Circuit, Permanent Circuit (CONS)

(f) T.22, Analogue Telephone Circuit, Switched Circuit (CONS)

Figure B-2. Transport Functional Profiles

[1] In the ISDN profiles, x=1 for the Permanent case and x=2 for the Switched case.

4	ISO 8073 classes 0 + 2
3	ISO 8208
2	ISO 7776
1	X.21 X.21bis

(g) T.31x, Permanent Access to a PSDN, T.70/CONS

4	Draft STANAG 4264 classes 0 + 2
3	Draft STANAG 4263
2	Draft STANAG 4262
1	Draft STANAG 4261

(h) T.312M, Permanent Access to a PSDN, CONS (Military)

4	ISO 8073 class 0	
3	ISO 8208	X.32
2	ISO 7776	
1	X.25 level 1	

(i) T.321, Switched Access to a PSDN, CONS, Telephone Circuit Access

4	ISO 8073 classes 0,2	
3	ISO 8208	X.32
2	ISO 7776	
1	X.25 level 1	

(j) T.322, Switched Access to a PSDN, CONS, Digital Data Circuit Access

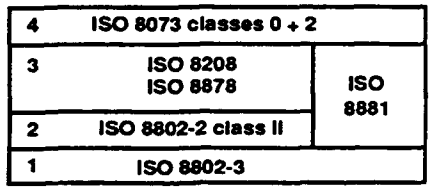
4	ISO 8073 classes 0 + 2	
X.21	3	T.70
	2	T.70
1	CCITT X.21	

(k) T.41, Digital Data Circuit, Telematic End Systems, T.70 Case

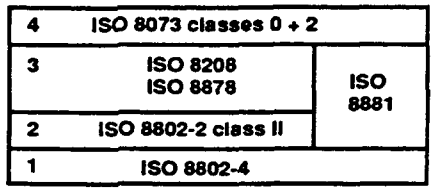
4	ISO 8073 classes 0 + 2	
X.21	3	ISO 8208 ISO 8878
	2	ISO 7776
1	CCITT X.21	

(l) T.42X, Digital Data Circuit, CONS

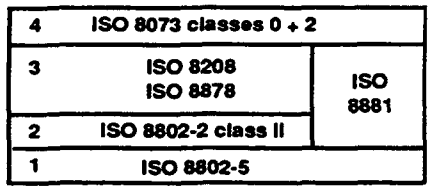
Figure B-2. (Continued)



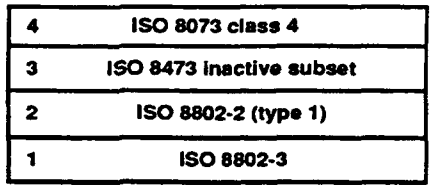
(m) T.611, Local Area Network CSMA/CD, CONS



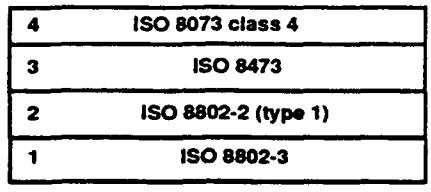
(n) T.612, Local Area network Token Bus, CONS



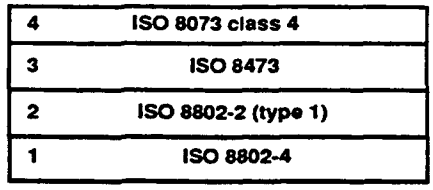
(o) T.613, Local Area Network Token Ring, CONS



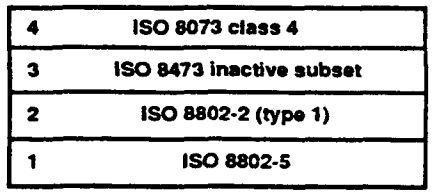
(p) T.6211, Local Area Network CSMA/CD, CLNS Single-LAN Environment



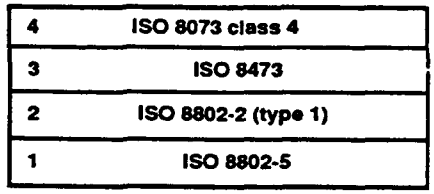
(q) T.6212, Local Area Network CSMA/CD, CLNS Multiple-LAN Environment



(r) T.622, Local Area Network Token Bus, CLNS Multiple-LAN Environment



(s) T.6231, Local Area Network Token Ring, CLNS Single-LAN Environment



(t) T.6232, Local Area Network Token Ring, CLNS Multiple-LAN Environment

Figure B-2. (Continued)

Two of the transport profiles [B-2(e) and B-2(f)] are for analog telephone circuits:

- T.21, Permanent Circuit with CONS
- T.22, Switched Circuit with CONS.

Four PSDN transport profiles [B-2(g) through B-2(j)] are shown in Figure B-2:[2]

- T.31x, Permanent Access to a PSDN, Using T.70 (T.311) or CONS (T.312)
- T.312M, Permanent Access to a PSDN with CONS (draft STANAG for military use)
- T.321, Switched Access to a PSDN, Telephone Circuit, Using Transport Protocol Class 0 (TP0) over CONS
- T.322, Switched Access to a PSDN, Data Circuit, Using TP0 and TP2 over CONS.

Two digital data circuit transport profiles [B-2(k) and B-2(l)] are shown in Figure B-2:

- T.41, Digital Data Circuit for Telematic End Systems Using T.70
- T.42x, Digital Data Circuit Using CONS (T.421 for Permanent Circuit and T.422 for Switched Circuit).

The final six transport profiles [B-2(m) and B-2(t] are for local area networks (LANs):[3]

- T.611, CSMA/CD LAN with CONS
- T.612, Token Bus LAN with CONS
- T.613, Token Ring LAN with CONS
- T.6211, CSMA/CD LAN, CLNS Single-LAN Environment
- T.6212, CSMA/CD LAN, CLNS Multiple-LAN Environment
- T.622, Token Bus, CLNS Multiple-LAN Environment
- T.6231, Token Ring LAN, CLNS Single-LAN Environment
- T.6232, Token Ring LAN, CLNS Multiple-LAN Environment.

4. RELAY PROFILES

Figure B-3 identifies 11 relay profiles. These are:

- Relaying the CONS:[4]
  - R.11, LAN to LAN
  - R.12, LAN to X.25 (PSDN)
- Relaying the CLNS:
  - R.21, LAN to LAN
  - R.22, LAN to X.25 (PSDN)
- Relaying the X.25 Packet Layer Protocol:
  - R.31, LAN to LAN
  - R.32, LAN to X.25 (PSDN, Virtual Call)
  - R.33, X.25 (PSDN, Virtual Call) to X.25 (PSDN, Virtual Call)

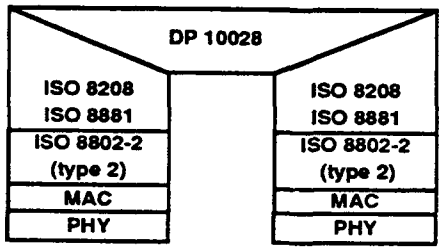
---

2 All the T-profiles provide the Connection-Oriented Transport Service (COTS). U-profiles would use the Connectionless Transport Services (CLTS)--no U-profiles have been identified in the 1989 *NTIS Transition Strategy*.

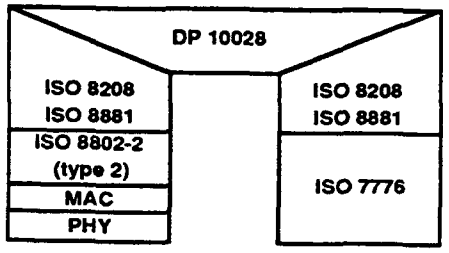
3 No T-profiles are given in the 1989 *NTIS Transition Strategy* for T.614, Fiber Distributed Data Interface (FDDI) LAN with CONS or for T.624, FDDI LAN with CLNS.

4 The 1989 *NTIS Transition Strategy* also identifies (without specifying the protocol stacks) a military profile being developed in SG9 WG1 for R.131(M), Relaying the CONS, WAN/PSDN to WAN/PSDN Using X.75.

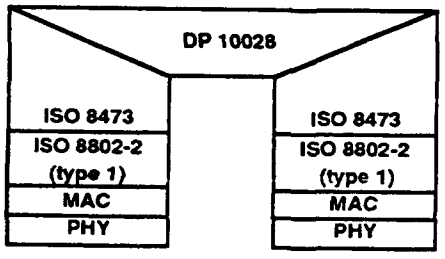
- Relaying the Media Access Control (MAC) Service:
  - R.41, CSMA/CD to CSMA/CD
  - R.42, CSMA/CD to Token Ring
  - R.43, Token Ring to Token Ring
  - R.44, CSMA/CD to Fiber Distributed Data Interface (FDDI).



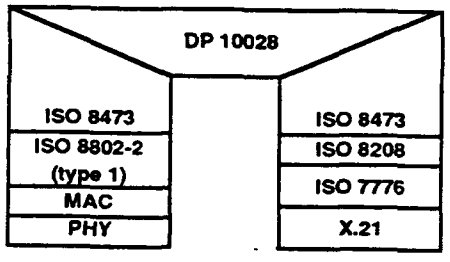
(a) R.11, Relaying the CONS, LAN-LAN



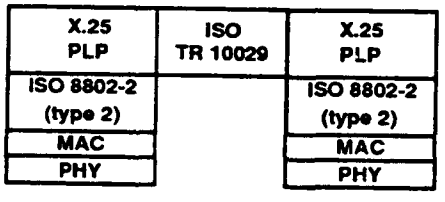
(b) R.12, Relaying the CONS, LAN-X.25 (PSDN)



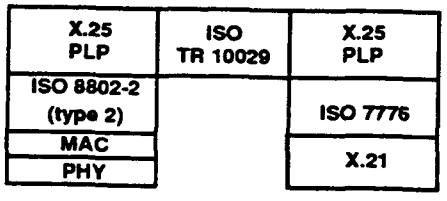
(c) R.21, Relaying the CLNS, LAN-LAN



(d) R.22, Relaying the CLNS, LAN-X.25 (PSDN)

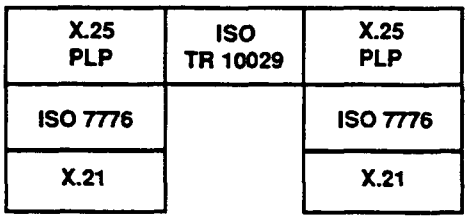


(e) R.31, Relaying the X.25 Packet Layer Protocol, LAN-LAN

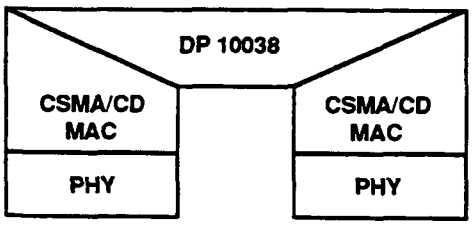


(f) R.32, Relaying the X.25 Packet Layer Protocol, LAN-X.25 (PSDN, Virtual Call)

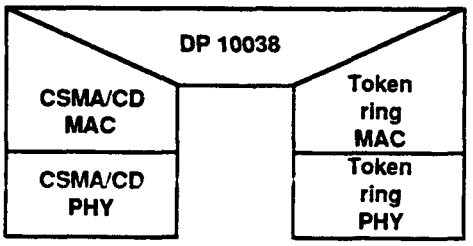
Figure B-3. Relay Functional Profiles



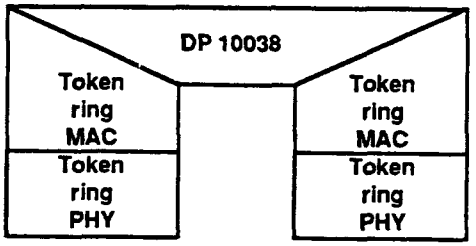
(g) R.33, Relaying the X.25 PLP, X.25 (PSDN Virtual Call)-(PSDN, Virtual Call)



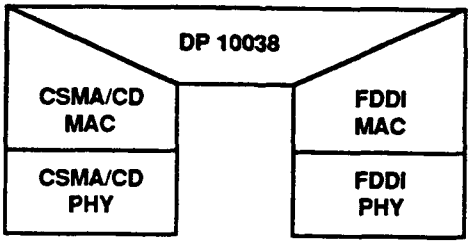
(h) R.41, Relaying the MAC Service, CSMA/CD-CSMA/CD



(I) R.42, Relaying the MAC Service, CSMA/CD-Token Ring



(j) R.43, Relaying the MAC Service, Token Ring-Token Ring



(k) R.44, Relaying the MAC Service, CSMA/CD-FDDI

Figure B-3. (Continued)

(This page intentionally left blank.)

APPENDIX C

NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS

NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS

1. INTRODUCTION

This appendix identifies profiles being used in national initiatives that make or plan to make significant use of OSI standards in military applications. The purpose is to provide detailed information on profiles that are planned for evolving tactical CCISs in the nations. Additional contributions to this appendix (as well as other parts of WP 25) are welcome.

NATO work on OSI is discussed in Chapter 15. Major bilateral and multilateral NATO initiatives are discussed in Chapter 16; these include the Quadrilateral Interoperability Program and STAMINA. Many national initiatives are discussed in Chapter 17.

2. CCIS PROFILES FOR INTEROPERABILITY

2.1 Details of Standards for French National Initiatives for Enhanced Interoperability

The Army will use standardized products based on the following standards:

- Programming language: LTR3 (Language Temps Reel), Ada, C
- Database: Relational database management systems, SQL
- Operating System: UNIX
- Development methods: Based on the French military standard GAM-T-17.

2.2 Overview of Data Communications for US Army's ATCCS

The Army Tactical Command Control System (ATCCS) architecture is discussed in Chapter 17 (Section 17.1.5). This section highlights the organization of data communications services planned for ATCCS.

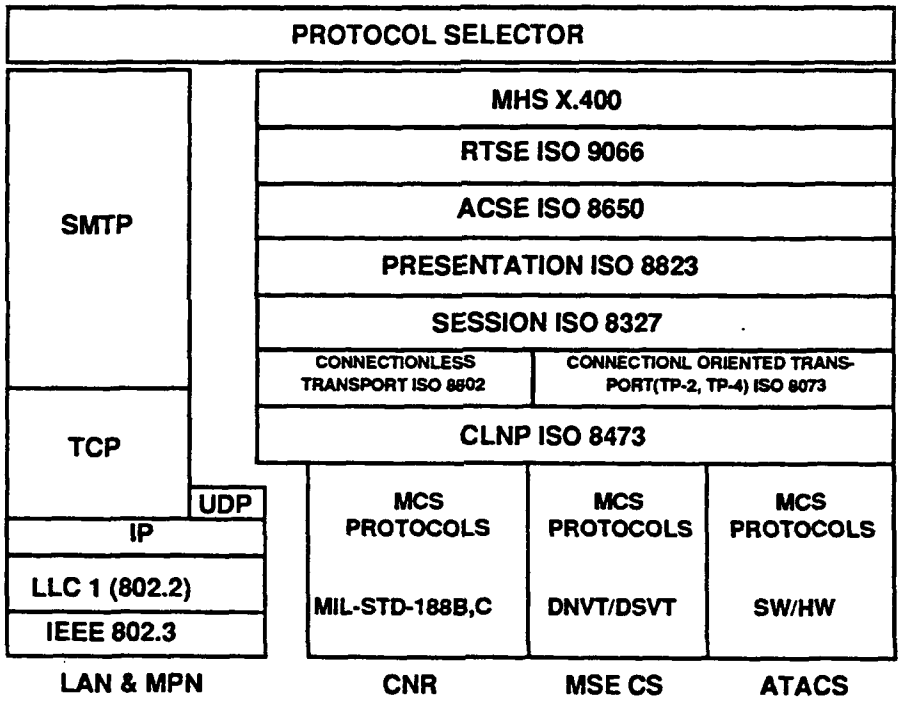
Figure C-1 identifies the protocol stacks specified in the Initial Baseline, and Figure C-2 identifies the protocols for the next stage [termed "Effectivity A1.1" and planned for the Follow-On Test and Evaluation (FOT&E) milestones] for ATCCS.[1]

- The local area network (LAN) interface is defined by TCP/IP, IEEE 802.2 (LLC 1) and IEEE 802.3 (CSMA/CD).
- The MSE Packet Network (MPN) uses TCP/IP, CCITT X.25, HDLC LAPB (ISO 7776) and four-wire conditioned diphase (CDP) or fiber-optic Thin LAN.
- US DoD Internet protocols used over TCP/IP are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), and TELENET. The standards for those protocols are listed in Appendix H.
- The UDP is provided to permit stacks over the Connectionless Network Protocol (CLNP) to use the MPN and LAN communications.
- Combat Net Radio (CNR) interfaces are defined by MIL-STD-188 B and C, STANAG 4202, and MIL-STD-188-114A.
- The ATCSS Common Hardware/Software (CHS) will provide protocols at Layers 2, 3, and 4 (in part).
- The MSE Circuit Switch (CS) interface is through the Digital Non-Secure Telephone (DNVT) and Digital Secure Telephone (DSVT).

---

[1] Cross-Functional Area Interface Specification for ATCCS, ACCS-A3-400-12, U.S. Army CECOM.

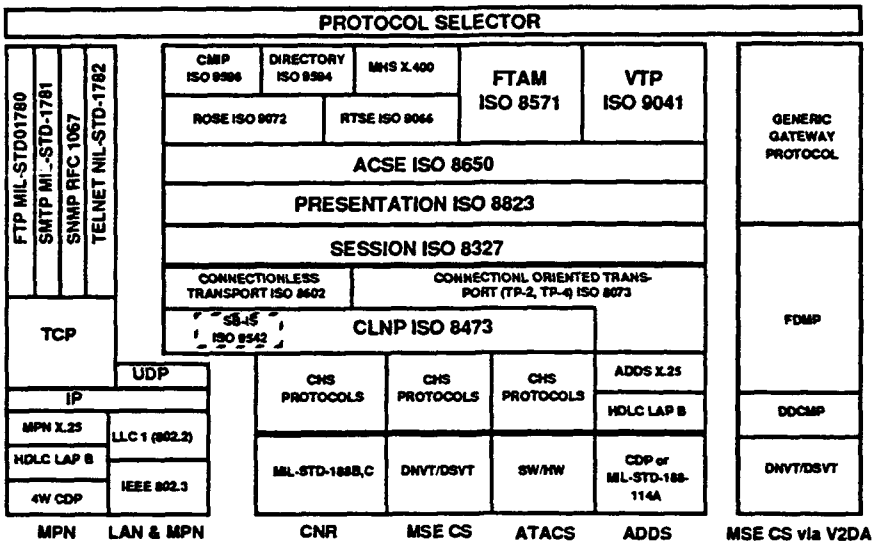
- The CHS provides physical interfaces to the Army Tactical Communications System (ATACS).
- Except for the Air Defense Functional Area, which also uses the Joint Tactical Information Distribution System, the ATCCS users will use only the Enhanced Portion Location Reporting System (EPLRS) portions of the Army Data Distribution System (ADDS). EPLRS uses a CDP or MIL-STD-188-114A interface, HDLC LAPB, and an ADDS version of X.25.[2]
- An alternate MSE CS Generic Gateway is provided by use of the DNVT/DSVT, WDCMP and Full Duplex Message Protocol (FDMP). This uses the MSE Version 2 Data Adapter (V2DA), currently only in use by the All Source Analysis System (ASAS).
- Not shown is the optional use of BLACKER with the MPN stack.
- Not shown is the Quadrilateral stack used with MCS (see Chapter 16). This stack uses TP2 and a variant of MHS-84.
- Not shown are options for LAN and MPN to use an address resolution protocol (ARP) and a reverse address resolution protocol (RARP).



Source: Cross-Functional Area Interface Specification for ATCCS, ACCS-A3-400-12, U.S. Army CECOM.

Figure C-1. ATCCS Inter-BFA Communications Protocols (Initial Baseline)

2 ADDS X.25 and MPN X.25 are not identical and not reported to be interoperable.



Source: Cross-Functional Area Interface Specification for ATCCS, ACCS-A3-400-12, U.S. Army CECOM.

Figure C-2. ATCCS Inter-BFA Communications Protocols (Effectivity)

2.3 Advanced Field Artillery Tactical Data Systems (AFATDS)[3]

AFATDS is the Fire Support (FS) functional area control system of the Army Command and Control System (ACCS) and Marine Tactical Command and Control System (MTACCS).

2.3.1 System Overview

AFATDS will provide an automated command, control, and coordination system that satisfies the Fire Support requirements generated by AirLand Battle doctrine. AFATDS equipment will be employed worldwide in support of the U.S. Army Fire Support Battlefield Functional Area (BFA) and Marine Corps fire support requirements. AFATDS software development will be accomplished in successive versions, each implementing additional functionality and interfaces, beginning with Version 1; Versions 2 and 3 will expand AFATDS functionality through development on its predecessor version.

AFATDS Version 1 will include component elements provided by the Army Tactical Command and Control System Common Hardware and Software (ATCCS CHS) program and the Standard Integrated Command Post System (SICPS) program.

AFATDS is a multi-service United States Army/United States Marine Corps (USA/USMC) automated command and control (C2) system for Fire Support Operations (FSOP). The initial fielding of AFATDS will be Version 1 (V1), which will be capable of managing field artillery (FA), air fire support (AFS)/Marine Air naval gunfire (NGF) and mortar attack systems at all echelons from corps to platoon level. AFATDS will provide the capabilities to process, analyze, and exchange combat information within the AFATDS architecture and with other Army BFA systems, selected NATO systems, and MTACCS component systems in Marine Amphibious Air-Ground Task Forces (MAGTFs).

AFATDS will be a system of mobile, dispersed, multi-functional nodes providing automated planning and execution capabilities to fire support operational facilities (OPFACs) and Independent User Centers (IUCs). OPFACs will operate at Fire Support Elements (FSEs) of the supported maneuver force, field artillery command posts, and other FA elements throughout the command structure. IUCs are remote terminals that allow commanders and selected fire support personnel to monitor fire support operations and issue guidance and directives from widely dispersed battlefield locations. The operational context for AFATDS is given for the Army in Figure C-3 and for the Marine Corps in Figure C-4.

---

3 This section is based on the following contribution: *AFATDS Data Communications*, Draft, Henry Saphrow, OPM AFATDS, U.S. Army CECOM, January 1992, UNCLASSIFIED.

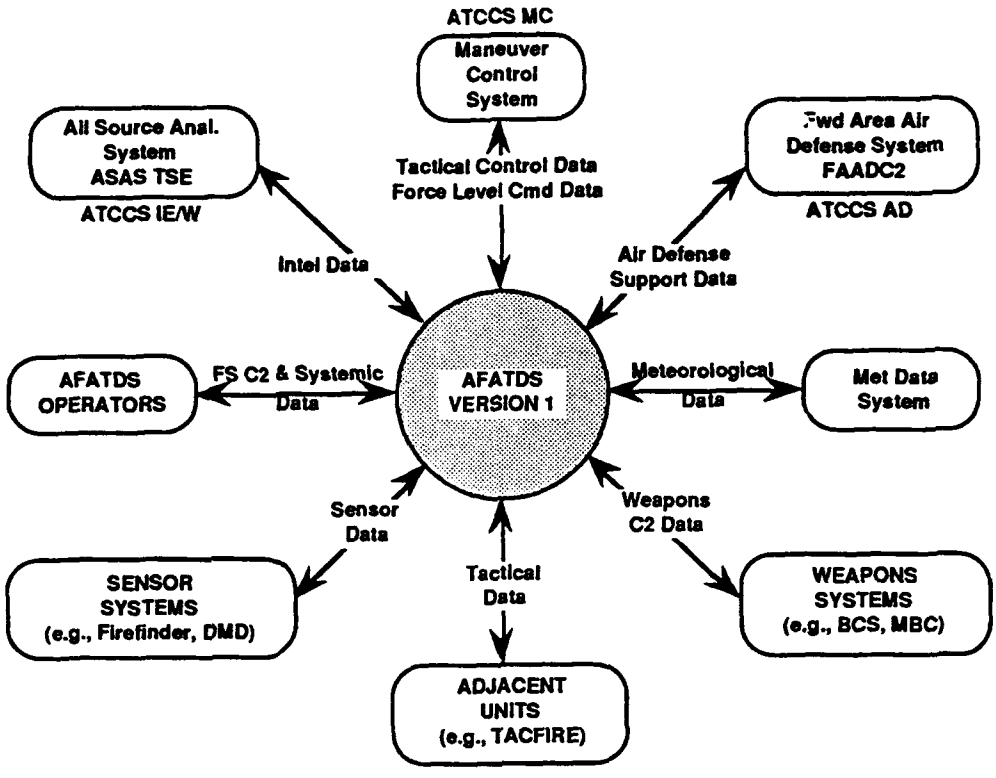


Figure C-3. AFATDS (US Army) Operational Context

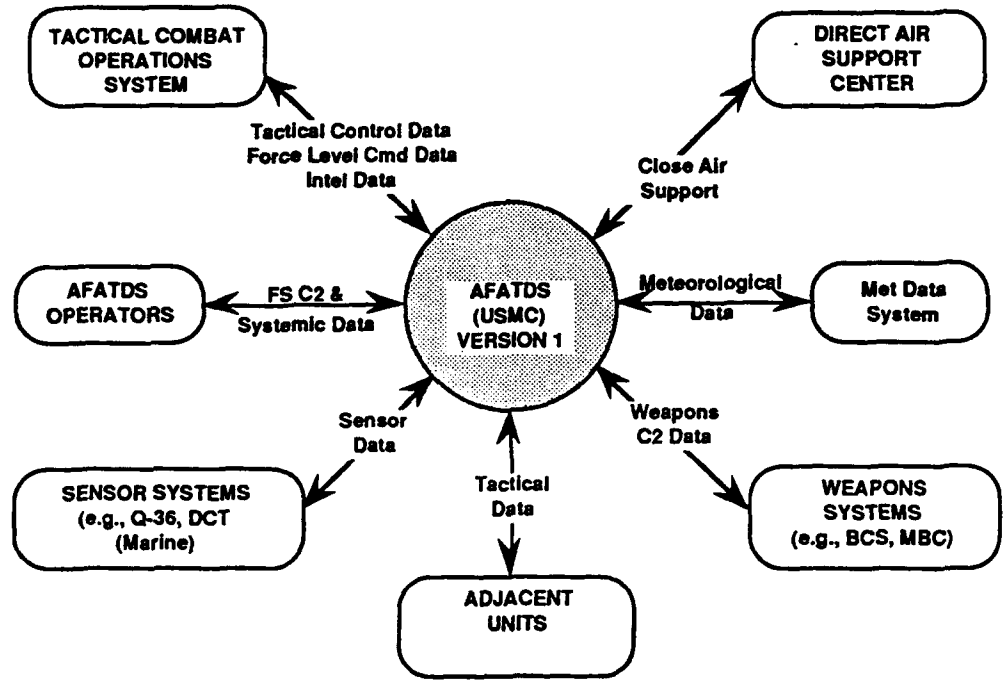


Figure C-4. AFATDS (USMC) Operational Context

Note: AFATDS will be a system of mobile, dispersed, multi-functional nodes providing automated planning and execution capabilities to fire support operational facilities.

The AFATDS V1 contract was awarded in May 1990 with IOT&E planned for FY94. AFATDS V2 and V3 are parallel efforts starting in FY92 for Version 2 and FY94 for Version 3. Initial fielding of production version (V2) is planned for FY95.

2.3.2 FS Operational Capabilities

AFATDS OPFAC capabilities within FA units will be for the command, control, and support of organic and attached FA assets (i.e., target acquisition means, operation centers, fire direction centers, weapons, and FA mission support elements). OPFAC capabilities located with maneuver units (FSE) will support the advising of the maneuver force commander on the use of available fire support assets, planning their employment, and integrating them into the scheme of maneuver. Marine Corps requirements are identified in the FIREFLEX Required Operational Capability. Automated capabilities will also be provided within any designated OPFAC for performing the fire support execution and movement control functions.

AFATDS FS operational capabilities are contained in five general operational need categories. These categories are the following:

a. Fire Support Planning (FSP) - provides the overall planning capabilities for integration of field artillery, air fire support, naval gunfire, and mortars into the force's scheme of maneuver.

b. Fire Support Execution (FSX) - provides automated support for target processing, attack systems analysis, and tactical fire direction.

c. Movement Control (MC) - provides for the movement control of field artillery units, prepares movement requests, coordinates those requests with the appropriate force level headquarters, and maintains movement data.

d. Field Artillery Mission Support (FAMS) - provides for logistical support for the field artillery system.

e. Field Artillery Fire Direction Operations (FAFDOPS) - maintains the current status of fire missions, fire support, and field artillery units.

2.3.3 Interoperability Capabilities

AFATDS will interoperate with existing tactical systems in order to serve as an integral element in the overall command and control structure. These systems consist of those FS systems directly engaged in execution of the Field Artillery mission and those other control systems that form the ATCCS. The following list summarizes the principal Version 1 AFATDS interfaces.

a. FS Sensor Systems (e.g., Firefinder, DMD, DCT, ATHS)

b. FS Weapons Control Systems (e.g., BCS, MBC, FDS)

c. Adjacent Systems [e.g., TACFIRE, ADLER, LTACFIRE, AFATDS (USMC)]

d. Maneuver Control System (MCS) - BFA and Force Level Control (FLC)

e. All Source Analysis System TOC Support Element (ASAS TSE) - Intelligence/ Electronic Warfare (I/EW) Data

f. Forward Area Air Defense Command and Control (FAAD C2) - Air Defense Support

g. Met Data System - Technical fire control meteorological data

h. AFATDS Operators.

2.3.4 AFATDS Communication Requirement

AFATDS primary method of communication is via the Combat Net Radio (CNR). Other communication capabilities includes Area Common User System (TRI-TAC, Mobile Subscriber Equipment, and Unit Level Switch), Army Data Distribution System (ADDS) and Position Location and Reporting System (PLRS), field wire (2W, 4W) and local area network (IEEE-802.3). AFATDS communication requirements include: operation on the move; continuity of operations (CONOPS); alternate net routing; communication channel reconfigurability while system is operational; operation with four programmable communication channels; and receive, transmit, and process over 2,000 messages per hour over secure links. Additional requirements include: detection reduction by the enemy, multiple destination communication, network loading and balancing, and automatic relays. To meet heavy traffic

demand and reliable communication over the CNR, AFATDS design implemented a communications architecture described in the next section.

2.3.5 AFATDS Communications Architecture

Figures C-5 and C-6 illustrate the organization of communications protocols used between Fire Support Workstations (FSWs) with regard to the ISO OSI Basic Reference Model, ISO 7498. Applications processes utilize one or more Application Service Elements (ASEs) that embody the functions of the ISO/OSI model's application, presentation, and session layers. Examples of ASEs are file transfer, message exchange, and X-Windows. ASEs rely on the data transfer services of transport and lower layer protocols that are common to all FSWs to facilitate their peer relationships.

Physical Layer. Connections to the following devices are provided in the Physical Layer.

- UHF: SINCGARS Radio, VRC-12, AN/PRC-77, AN/PRC-68
- HF: AN/PRC-104, AN/GRC-213, AN/GRC-193, AN/GRC-106
- MSE: DNVT, DSVT, EPLRS, PLRS, and ULS.

Data Link Layer. The data link is based upon Joint VMF-TIDP-TE Vol IV. Presently this standard only supports Type I services. AFATDS/VMF CPS (AFATDS Variable Message Format Communications Protocol Standard) supports both Type I and Type II services. Type I is based on MTS Broadcast standard with enhancements agreed by the Joint Message Standard Working Group. The Type II services are based on IEEE 802.2 and HDLC LAPB protocols with some enhancements for Combat Net Radio (CNR). The following enhancements are part of AFATDS/VMF CPS:

- Multi-Frame Transmissions
- Uncoupled Acknowledgements
- Use of Poll/Final (P/F) Bit
- Implementation of "Windowing" for Multi-Frame Transmissions

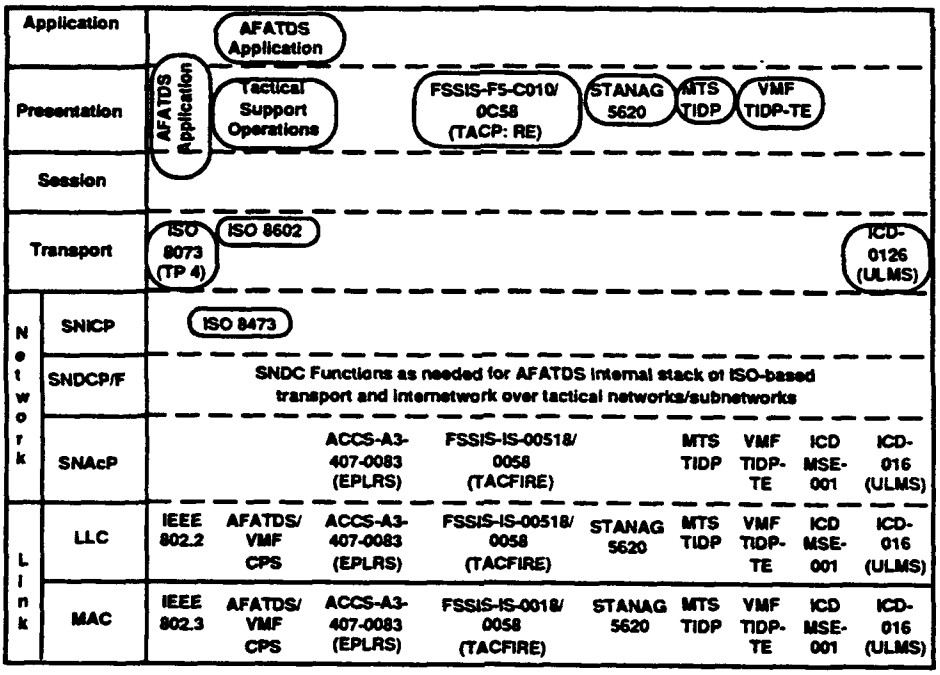


Figure C-5. Organization of Communications Protocols in AFATDS

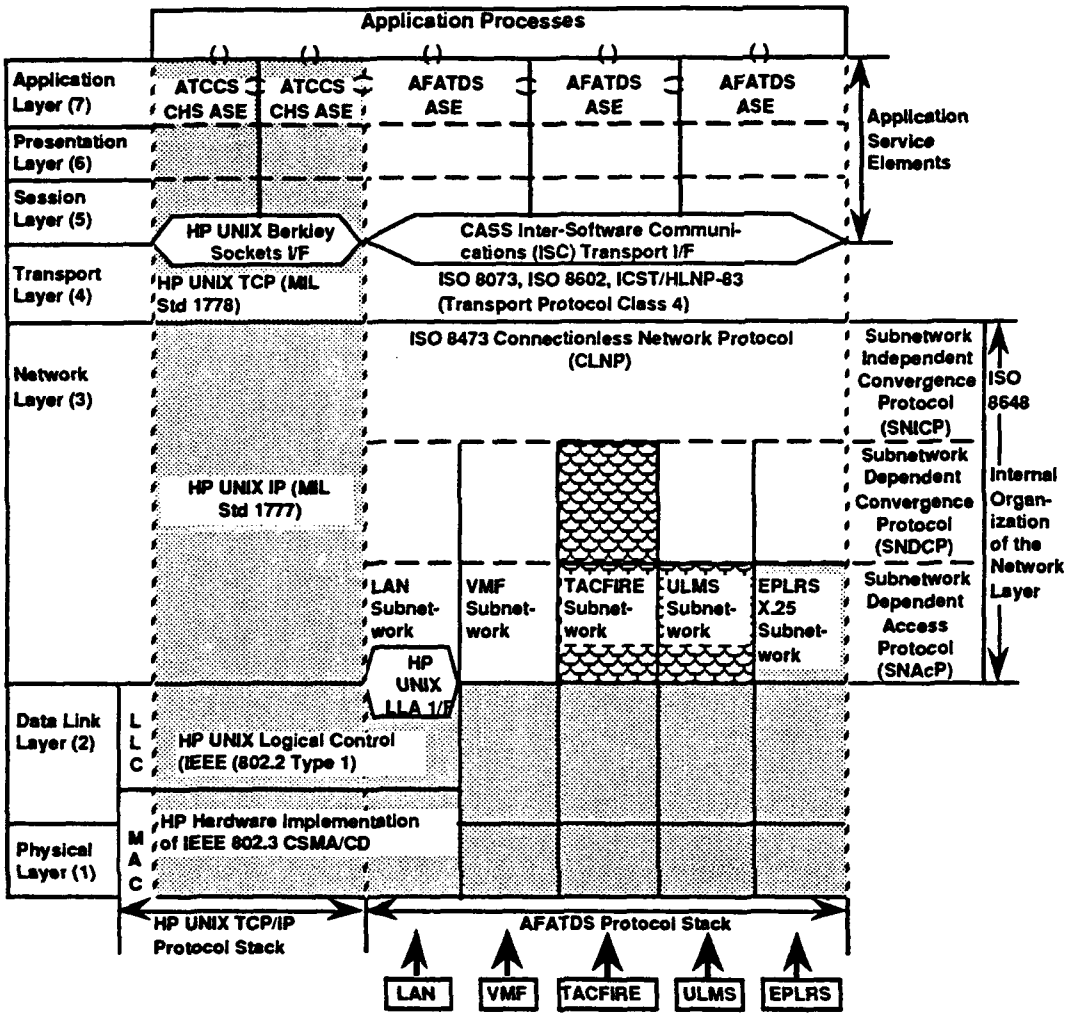


Figure C-6. AFATDS Protocol Stacks

- Use of Sequence numbers for State Variables
- Selective Rejection Balanced Mode Extended (SABME) Frame
- Frame Reject (FRMR) Frame
- Reset (RSET) Frame
- Disconnect (DISC) Frame.

Network Layer. The following network layer functions, which have been derived from the AFATDS SSS requirements and CEP experience, will be supported for AFATDS Version 1.

- Interconnection of Subnetworks
- Addressing
- Routing
- Error Control
- Flow Control
- Subnetwork Independent Convergence Protocols (SNICPs)
- Subnetwork Dependent Convergence Protocols (SNDCPs)
- Subnetwork Access Protocols (SNAcPs).

The network layer implementation for AFATDS will be based on the DIS 8473 (CLNP), ISO 8648, ISO 8348, and ISO 8348/ADD 1 network layer standards. Due to the unique FS requirements

and the FS operational environment, these standards will be extended and modified as necessary for AFATDS use. The AFATDS CLNP-based internet protocol will be utilized as the SNICP over five distinct subnetworks: the LAN provided as part of the ATCCS CHS, tactical networks employing the VMF-TIDP-TE data link protocol, tactical networks employing TACFIRE protocols, Enhanced Position Location Reporting System (EPLRS) X.25-based networks, and Unit Level Message Switch (ULMS)-based networks.

ISO 8473: *Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service.* This is the standard that AFATDS has adopted in which to base the internetwork layer. The AFATDS CLNP functionality will use multiple SNDCPs to access the diverse suite of subnetworks available to it and required of it to gain the connectivity needed in the Army's limited channel/bandwidth environment. Currently, the inactive Network Layer protocol subset will not be used even within an OPFAC LAN in order to support the dynamic (re)configuration capability required in AFATDS. The Non-Segmenting protocol subset may or may not be utilized awaiting results from yet-to-come performance trade-offs. Given the multiplicity of subnets with their varying packet sizes, a segmenting capability would seem appropriate in an absence of realizing the reliability of the subject subnets.

Session Layer. The Session Layer is null for AFATDS data communications.

Transport Layer. The following Transport Layer functions, which have been derived from the AFATDS System/Segment Specification (SSS) requirements and Concept Evaluation Phase (CEP) experience, will be supported for AFATDS Version 1.

- Connected Data Transfer
- Acknowledged Unit Data Transfer
- Unacknowledged Unit Data Transfer
- End-to-End Acknowledgement
- Retransmission on Time Out
- Segmenting and Reassembly
- Data Sequencing/Resequencing
- Explicit Flow Control
- Transport Addressing
- Inactivity Control.

The Transport Layer implementation for AFATDS will be based on ISO 8073 (TP 4), ISO 8072, ISO 8072/DAD 1, ISO 8602, and ICST/HLNP-83 Transport Layer standards. Due to the unique Fire Support requirements and the FS operational environment, these standards will be extended and modified as necessary for AFATDS use.

ISO 8073: *Information Processing Systems - Open System Interconnection - Connection Oriented Transport Protocol Specification;* also ISO 8073/DAD 2: Addendum 2: *Operation of Class 4 over Connectionless Network Service.* These are the standards which AFATDS has adopted to base the transport mechanism on. AFATDS CEP developed a transport mechanism based on NIST recommendations for implementing TP4 as promulgated in ICST/HLMP-83-3: *Proposed FIPS - Specification of a Transport Protocol for Computer Communication,* vol. 3: *Class 4 Protocol.* The primary extension to TP4 adopted from the NIST document was the modification of UNIT_DATA from unacknowledged/unreliable to acknowledge/reliable. This extension was developed by NIST to support military application and coincidentally served AFATDS CEP well. Additionally specializations to the TP4 protocol were made in CEP to meet the requirements of its clients and the diverse nature of the subnetworks (IEEE 802.5 to CNR) it was used over. Timer durations were modified to account for service delays perceived on different nets and to account for non-responsiveness of clients in reacting to service indications (e.g., connection offers). An adaptive retransmission timeout mechanism was developed. Segment sizes were adjusted per the servicing networks ability (non-segmenting network used in CEP). New state transitions and protocol data units were introduced to account for AFATDS specific anomalies or needed utilization improvements. An example was the inclusion of large amounts of user data in CR TPDUs in FIPS type UNIT_DATA to limit the number of TPDUs required to complete an acknowledged "datagram" especially over CNR. This AFATDS CEP implementation of a transport layer (in Ada) has been ported to AFATDS V1 for use as a protocol communication system in support of the AFATDS Inter-Software Communication (ISC)

prototype, and portions will be used where possible in the AFATDS V1 objective system design and implementation.

ISO 8062: *Information Processing Systems - Open System Interconnection - Protocol for Providing the Connectionless-Mode Transport Service.* Despite having needed and adopted NIST FIPS-style acknowledged UNIT_DATA, AFATDS still intends on availing itself of the more original ISO unacknowledge UNIT_DATA mechanism. This is useful especially in support of multicast. In AFATDS CEP this same standard was adopted (in draft form) and mechanisms were developed to allow multiple endpoints, or TSAPs, within a single workstation to receive copies of a single, multi-cast on the LAN.

Presentation Layer. The Presentation Layer is handled by the Tactical Support Operation (TSO) function in AFATDS. The TSO is a computer software configuration item (CSCI) in AFATDS V1 that embodies the presentation functions necessary to afford AFATDS applications the ability to interoperate with multiple different end systems, many of which have different transfer syntaxes (i.e., message formats/sets). TSO acts as a translation filter on transmission from AFATDS applications, proper, which can be destined to AFATDS and non-AFATDS systems alike, and proxies the transmission request on the correct procedural interface: inter-software communication (ISC) for intra-AFATDS transfer or the appropriate external system (XC) interface for non-AFATDS transfers. In the intra-AFATDS case, the ISC delivers the transmission to the destination application software entity directly, which receives it via TSO proxy routines again. In the non-AFATDS case, TSO invokes the XC function which RPCs (remote procedure call) the transmission request via the ISC to its agent XC entity at the respective external system "communication gateway" entity, which in turn acts as a gateway between the AFATDS internal stack, accessed via ISC, and the external stack required to interact with the non-AFATDS system.

TSO fills the classical role of application gateway as well. On reception of a message transmission from an external system, the appropriate "communications gateway" entity passes the message off to TSO, which then translates the message to AFATDS internal format and forwards it on to the application entity within the OPFAC which must process it. This hand-off on reception is done because external systems do not address their transmissions to the level of granularity that the AFATDS does. In essence, the other systems utilize a one-level address space where addressing consists of identifying the fire support unit. However, AFATDS utilizes a two-level name-space where each intra-AFATDS transmission is addressed not only to the unit, but also to the specific software entity within the unit, which, by the way, may be configured to be anywhere within a multi-workstation OPFAC. This is because AFATDS is the first distributed system in the US fire support inventory coupled with the engineering capability to extend transport end-to-end reliability over internetted tactical networks, whereas in the past it was all done with link protocols. At any rate, TSO is required to determine the final destination based on message content because the data transfer mechanism was not given complete address information by the external system per AFATDS standards.

Application Processes. AFATDS applications processes are composed of ASEs that can be classified into two types: Common ASEs and Specific ASEs. Common ASEs are those that provide capabilities which are generally useful to more than one application process. Specific ASEs are those that provide capabilities to satisfy the particular needs of a single application process. An ASE may invoke the services of another ASE within the same application process. Therefore, Common and Specific ASEs are combined in various ways to create different applications processes. Individual ASEs employ Application, Presentation, and Session Layer functions as necessary based on the service that the ASE is providing. Therefore, it is not possible to identify a single set of application, presentation, and session protocols, but rather these layers must be discussed for each ASE employed by an application process. The specific application processes and ASEs they employ are described below.

Application Layer employs two services. In the classic case, software entities access the data transfer mechanism directly (ISC in AFATDS, Berkley Sockets, or TL1 in UNIX) and perform their own version of the required functionality typically associated with the upper layers. In effect, the applications use their own ASE. This is especially true when remote procedure call (RPC) paradigms are used. RPC is an underpinning of AFATDS given its distributed nature and non-deterministic configurability. In the second service, application level software entities access data transfer by utilizing Message Handler Services defined as Tactical Support Operation (TSO). TSO performs some application control functionality and presentation functionality, and to some extent handles sessions with external systems for AFATDS applications. The message definition effort will use the data elements and messages as defined in ACCS, DoD (Joint), and NATO standards.

2.4 Protocols Provided by US Army TCIM Hardware[4]

The US Army Common Hardware/Software (CHS) programs include a Tactical Communications Interface Module (TCIM), also known as the Adaptable Programmable Interface Unit (APIU).

Two versions of interfaces are provided. Supported by an external device using a SCSI interface version on a single channel (known as Channel 1). Channel 1 supports the Maneuver Control System (MCS) Version 10 Circuit Switch (CSW), the Marine Tactical System (MTS) Mode VII CSW, CCITT X.25, and the Army Data Distribution System (ADDS) X.25 for EPLRS. The Version 1 interfaces are:

- KY-68 (DSVT)
- TA-1035 (DNVT)
- KG-84 (DLED)
- AN/GYC-7 Unit Level Message Switch (ULMS)
- SB-3614 SB
- EPUU/JTIDS (32 Kbps)
- 4 Wire
  - FSK-188C&B
  - STANAG 4202 (Annex A)
  - Conditioned Diphase.

The second version of interfaces (known as Channel 1 and Channel 2) is supported by an internal SCSI circuit card for the Version 2 Laptop Computer Unit (LCU). The second version supports all the interfaces defined by Version 1, together with additional interfaces noted below, on two channels (Channels 1 and 2). The Version 2 capability supports combat net radio with the following added interfaces:

- Combat Net Radio
  - VRC-12 and PRC-77
  - SINCGARS
  - GRC-193, GRC-213
  - PRC-104
- KY-57
- 2 Wire
  - FSK-188C&B
  - STANAG 4202 (Annex A)
  - Conditioned Diphase.

The following requirements are being addressed as follow-on TCIM requirements in development for field tests in 1992:

- AFATDS:
  - TACFIRE protocol (6/9/11/8) software
  - NATO STANAG 5620 software
  - MTS switched software
  - ADDS interface software
  - VMF TIDP software
  - TCIM/TCU interface
  - KG-84C
- FAAD C2I
  - Multiple TCIM
  - ADDS interface
  - TCIM/TCU interface

---

4 This section is based on the following contribution: *CHS Communications Program*, Briefing, Draft, Stan Levine, OPM CHS, US Army CECOM, December 1991, UNCLASSIFIED.

- ADDS
  - ADDS interface software
    - -- 128 Kbps baud rate
    - -- 200 packages per second (pps) throughput
  - Two programmable PJH channels
  - TCIM/TCU interface
- Marine Corps
  - MTS switched software
  - MTS broadcast (Class I) software
  - ULS autodial interface software
  - KG-84C interface software
- MCS follow-on requirements
- FSAC follow-on requirements.

The overall architecture for the communications software interfaces between the physical device (SCSI Bus) and the Layer 3 services provided by the Unit Level Processor (ULP) is shown in Figure C-7.

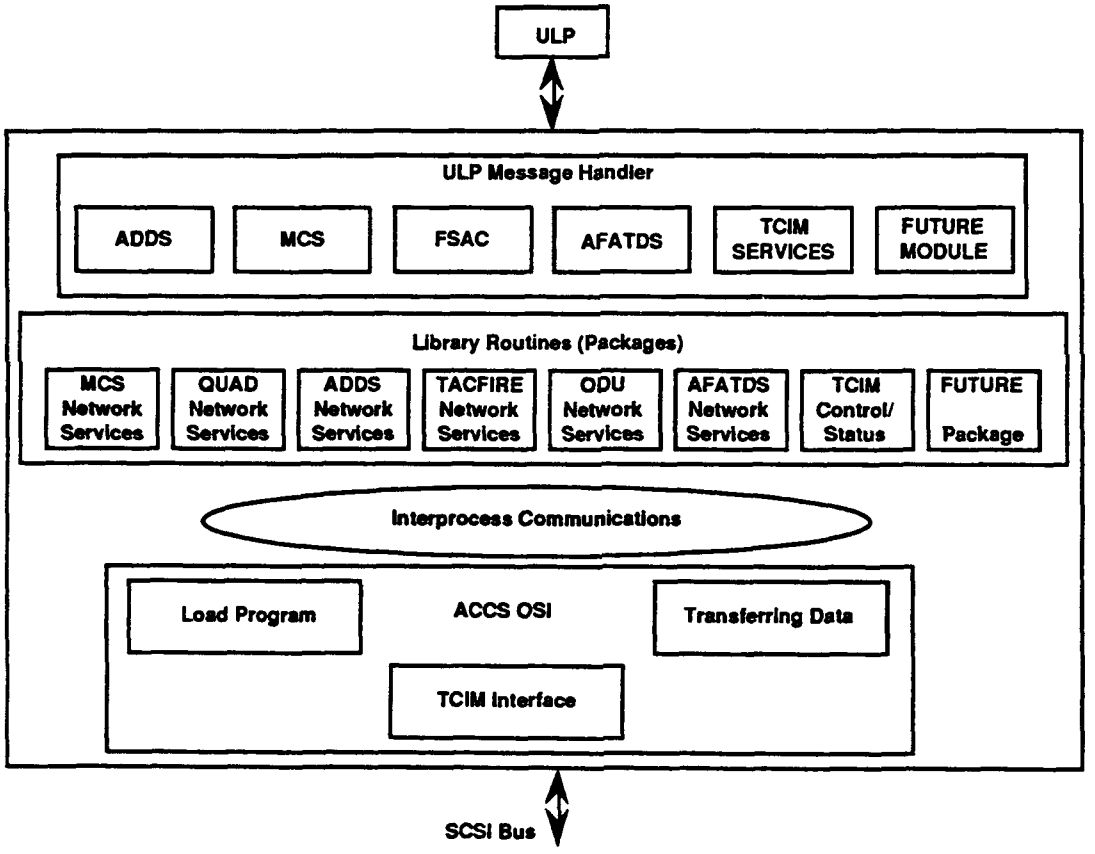


Figure C-7. Communications Software Interface Architecture

3. EXAMPLE PROFILES FOR BROADCAST MEDIA

3.1 Example of a Broadcast Profile for Data Communications Using Tactical Radios

This section uses the OSI Reference Model and interoperability parameters to identify interpretations, extensions, and deviations to OSI and other standards in the specification of a set of

protocols used to support data transmission over combat net radio by the U.S Marine Corps. These protocols are specified in Volume V of the Marine Corps MTS TIDP.

The MTS protocols were developed based on U.S. federal standards in the late 1970s. Many of the standards selected have become ISO standards, and the structure of the MTS protocols can be interpreted in terms of the seven-layer OSI Reference Model. The MTS broadcast profile, discussed in this section, is now being used by the Army and the Marine Corps as the basis for defining the initial protocol standards to be used in the TIDP now being developed for Joint Interoperability of Tactical Command and Control Systems (JINTACCS) K-Series Variable Message Format (VMF) bit-oriented messages. The K-Series messages and associated data communications protocols are being specified by the joint Fire Support Subgroup (FSSG) of the Joint Multi-TADIL Standards Working Group (JMSWG) under the auspices of the Joint Tactical C3 Agency (now the Joint Interoperability Engineering Organization).

Table C-1 highlights the features provided in the broadcast protocol, used in Marine Corps tactical data systems (TDSs), for each of the seven layers. It further identifies the standards used in each layer and notes the interpretations, exceptions, extensions, and deviations that were specified.

Military features supported by the broadcast protocol standard and identified in Table C-1 include:

- Multiaddressing (Layer 7, through the Message Header; and Layer 2, through the extended address field)
- Data integrity and, more generally, the capability to operate in a high bit-error-rate environment [Layer 2, through use of a 32-bit frame check sequence (FCS) for error checking and the (23,12) half-rate Golay error detection and correction coding (ED&C), together with 16x24-bit interleaving]
- Use of XID command and response (Layer 2)
- Control of emanations by senders and recipients through provisions for optional acknowledgements (ACKs) (Layer 7--request for ACK is part of the message) and for not sending ACKs even when requested (Layer 2), both under operator control
- Limit on the number of retransmissions permitted (Layer 2)
- Providing for net access (uses an international standard in Layer 2 for handling media access contention and collision detection[5] and defines an algorithm for wait times for reattempting access); net access algorithms could be extended to support precedence and preemption.

4. EXAMPLE PROFILES FOR TACTICAL SWITCHES

4.1 Example of a "Datagram" Switched Protocol Standard for Tactical Radios

This section summarizes a set of protocols used to support data transmission through tactical data switches by the U.S. Marine Corps. These are the MTS switched protocols that are specified in Volume V of the Marine Corps *Technical Interface Design Plan for Marine Tactical Systems.*

Table C-2 highlights the features provided in the switched MTS protocol for each of the seven layers. The table identifies the international and U.S. standards used in each layer, and notes the interpretations, exceptions, extensions, and deviations that are specified.

[5] The listen-before-talk contention method is called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Table C-1. A Functional Profile of Broadcast Protocols Used in Tactical Systems by the U.S. Marine Corps

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
7	Msg Header Msg Acknowledgment	None None	Supports multiple addresses, precedence, security classification, and message receipt compliance.
6	Msg Format	None	Uses the same flagging scheme as the syntax adopted for U.S. JINTACCS K-series messages.
	Information Field Size	None	Maximum message length is 3500 octets.
5	None	N/A	Null layer.
4	None	N/A	Null layer.
3	Message Segmenting	N/A	Messages are not segmented.
2	Frame Formatting	ISO 3309/7809 (HDLC) with Options 7 and 14	Opt 7=Extended Address Field; 2-17 octets, 1-16 destinations (base std is one octet; Opt 7 specifies no maximum on extended address field size). Opt 14=32-bit frame check seq (FCS) (base standard is 16-bit FCS).
	Frame Addressing	ISO 3309	
	Commands & Responses	ISO 4335/7809 with Option 1	Opt 1=XID. Does not support SABM, DISC cmds and FRMR,UA,DM resp (radio application).
	Media Access	No standard applies	Uses CSMA with unique algorithms for reattempting access to net.
	Data Link Initialization and Release	ISO 4335/7809 with Option 1 (XID)	XID is used during net establishment.
	Frame Transfer	ISO 4335/7809	Uses all 3 types of frames.
	Acknowledgment (ACK)	ISO 4335	ACK is optional; when invoked, it follows the standard.
	Retransmission	Not controlled by standards	Max 2 retries (under operator control) (no provision for setting a max in stds). Standards suggest use of P/F bit to control retransmission.
	ED&C--Error Detection	IS 3309/7809 w Opt 14	32-bit FCS (algorithm is ISO 3309, Sec 3.6.3).
	ED&C--Error Coding	Not controlled by standards	(23,12) half-rate Golay; 24th bit is zero filled (detects 6/corrects 3 errors in each 24-bit codeword).
	ED&C--Interleaving	Not controlled by standards	16x24-bit time dispersive coding (TDC).

Table C-1. (Continued)

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
1	--Electrical		
	--Voltage Levels	MIL-STD-188-114	[Similar to CCITT V.10/X.26]
	--Load Impedance	MIL-STD-188C	
		MIL-STD-188/24(Prt2)	
		MIL-STD-188-141	
	Mechanical		
	--Connectors	MIL-STD-242G(Prt8)	
		MIL-P-55149	
	Cable Lengths	MIL-STD-242G(Prt8)	
	Functional (pin assign)	MIL-STD-242G(Prt8)	
	Procedural		
	--COMSEC Pre/Postamble		
	Frame Placement	DCT Spec	
	--Keytime Delay	DCT Spec	
	--Bit Synchronization	DCT Spec	
	--Transmission Synch	DCT Spec	
	--Clocking Ctrl & Timing	N/A	

References:

1. Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP), Volume V, Protocol Standard, Headquarters, U.S.Marine Corps, July 1987, UNCLASSIFIED.

2. Discussions with Systems Integration Directorate, MCRDAC, and LOGICON/Eagle Technology, Inc., March 1989.

Table C-2. A Functional Profile of "Datagram" Switched Protocols Used in Tactical Systems by the U.S. Marine Corps

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
7	Msg Header Msg Acknowledgment	None [1] None	• Supports multiple addresses, precedence, and security classification.
6	Msg Format	None	• Uses the same flagging scheme as the syntax adopted for US JINTACCS K-Series messages
	Information Field Size	None	• Max is 40 segments, 260 octets per segment (message length)
5	None	N/A	• Null layer
4	End-End Sequence Control	None	• Transport layer accumulates and orders packets for users; uses 7 octets (vice 20-60 octets for TCP)
	End-End Congestion/ Flow Control	None found	• Connectionless-oriented layer, a variant of TP4
3	Network Routing/Switching	None found	• Connectionless-oriented with deterministic routing [2] • Supports "floating" host, using operator-initiated disconnect and reconnect, but requiring no change of address
	Message Segmenting	Not controlled by standards	• 260-octet maximum message segment
	Packet Addressing	None	• Uses unique 3-octet routing indicator and provides for multiple addressing for up to 16 destinations
	Packet Precedence	None	• Uses 3 classes of precedence (SysCom, Data1, Data2), in which military precedences (Y-Z-O-P-R) are handled as Data2
	Network FLow &	None found	• Traffic from subscribers can be limited on precedence; traffic in network is processed by packet precedence
	End-End Error Recovery (Message Accountability)	None	• Detects loss of message frames, with notificication for nonperishable messages
	Congestion Control Interneting	N/A	• Not supported
2	Frame Formatting	ISO 3309/7809 (HDLC) with Options 10 and 14 ANSI X3.66-1979 (ADCCP) (MIL188 TRI-TAC Mode VII)	• Opt 10 calls for extended control field (two octets) • U-frame is extended (two octets) [3] • Opt 14 calls for 32-bit FCS
	Frame Addressing	ISO 3309	• Station address varies [4]
	Commands & Responses	ISO 4335/7809 with addit'l Options 2,4,5,8,11 [5]	• SIM cmd may be initiated at both stations for link initialization • RIM response not implemented • Does not support poll-final (P/F) bit
	Media Access	N/A	• When established (initialized), full-duplex point-to-point link has no access contention
	Data Link Initialization and Release	ISO 4335/7809 ANSI X3.66-1979 (ADCCP) TRI-TAC IC[illegible]S	• Addresses security through use of UI-frames [6]
	Frame Transfer	ISO 4335/7809	• Uses all 3 types of frames
	Acknowledgment (ACK)	ISO 4335	• ACK or NAK is required
	Retransmission	ISO 4335	• Maximum of 5 retries • Retransmission is automatic if no ACK [7]

Table C-2. (Continued)

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
1	--Electrical		
	--Voltage Levels	MIL-STD-188-114	[Similar to CCITT V.10/X.26]
	--Load Impedance	MIL-STD-188C	
		MIL-STD-188/24(Prt2)	
		MIL-STD-188-141	
	Mechanical		
	--Connectors	MIL-STD-242G(Prt8)	
		MIL-P-55149	
	Cable Lengths	MIL-STD-242G(Prt8)	
	Functional (pin assign)	MIL-STD-242G(Prt8)	
	Procedural		
	--COMSEC Pre/Postamble		
	Frame Placement	DCT Spec	
	--Keytime Delay	DCT Spec	
	--Bit Synchronization	DCT Spec	
	--Transmission Synch	DCT Spec	
	--Clocking Ctrl & Timing	N/A	

References:

1. Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP), Volume V, Protocol Standard, Headquarters, U.S.Marine Corps, July 1987, UNCLASSIFIED.
2. Discussions with Systems Integration Directorate, MCRDAC, and LOGICON/Eagle Technology, Inc., March 1989.

5. COMPARISON OF TACTICAL PROFILES

5.1 Comparison of US Data Communications Broadcast Protocols Based on HDLC for Digital Entry Devices (DEDs)[6]

Note: STANAG 4202 is used for combat net radio to send STANAG 5500 message text formats. Its interoperability parameters are discussed in Appendix A.

Purpose. This paper compares Marine Tactical Systems[7] (MTS) and Variable Message Format[8] (VMF) broadcast data link layer protocols to High Level Data Link Control[9] (HDLC) and other data link protocols. All of these protocols are candidates for a Digital Entry Device (DED) protocol. This comparison identifies modifications to the base HDLC standard to accommodate a particular feature of a subnetwork technology. It provides insight to the reasons for deviations from the standard.

---

6 This section is based on a contribution from the US Marine Corps, *Comparison of the MTS Broadcast, VMF, and Other Data Link Standards Based on HDLC*, Draft, MCRDAC/Integration (Maj. M. Mascarenas), 15 November 1991, UNCLASSIFIED.

7 *Marine Tactical Systems Technical Interface Design Plan (MTS TIDP)*, Volume V, *Protocol Standard*, US Marine Corps, July 1987, UNCLASSIFIED.

8 *Variable Message Format TIDP*, Volume IV, *Protocol*, February 1991, UNCLASSIFIED.

9 ISO 4335, *High Level Data Link Control (HDLC) Procedures*, Third edition, 1987; ISO 3309, *High Level Data Link Control - Frame Structure*, Third Edition, 1984; and ISO 8885, *High-level Data Link Control Procedures - General-Purpose XID Frame Information Field Content and Format*, First Edition, 1987.

Background. The VMF data communication data link protocol (Layer 2 of the OSI Reference Model) is being developed for initial use as a broadcast protocol to operate with UHF, VHF, and HF single channel radios. VMF and Air Force Application Program Development[10] (AFAPD) are closely related to the Marine Tactical System (MTS) broadcast protocol. VMF, AFAPD, and MTS are based on ISO 4335 HDLC procedures and ISO 3309 HDLC frame structure.

The HDLC standard offers a range of option selections and operating modes that have been used for a variety of station and network types (e.g., point-to-point, multi-link, broadcast). Some of the flexibility built into HDLC includes the following:

- A broad set of commands and responses
- Procedures for primary, secondary, and combined stations
- Procedures for half and full duplex
- An extendable control field
- An extendable address field
- A variable information field
- Conventions to allow group and global addressing
- A set of 14 option functions.

Specialized data link standards have been created by selecting from the set of options or through modifications to the HDLC to provide special services. One such modification occurs in the address field. The address field of HDLC only allows one address that identifies the destination of a command and the source of a response. In broadcast type networks that have only combined stations, all stations receive the command or response and any station might have been the originator. Both the source and destination addresses are required to remove any ambiguity. For that reason, data link protocols for broadcast type networks modify the address field to allow at least two addresses, source and destination.

The following are the data link standards that are based on HDLC and used in this comparison:

(1) X.25 LAPB. X.25 LAPB uses the HDLC class of procedures for balanced asynchronous combined (BAC) stations and includes HDLC options 2, 8, and 10. It is intended for point-to-point or multipoint configurations.

(2) ISO 8802-2. ISO 8802-2, Logical Link Control[11] (LLC) defines two modes of operation, connection-oriented (CO) and connectionless (CL), both of which are based on HDLC for BAC stations in a broadcast network. It deviates from the HDLC standard frame format to provide both the source and destination addresses required in a broadcast network. It also uses a bit in the source address field to indicate whether the frame is a command or a response. The connection-oriented service uses the basic commands and responses for BAC and adds HDLC options 2, 7 and 10. The connectionless service is a reduced set of commands and responses, but adds HDLC options 1, 4 and 12.

(3) MTS Broadcast. The MTS data link broadcast protocol offers a connectionless service in a broadcast network. It is based on a reduced set of HDLC commands and responses and includes HDLC option 1, 7 and 14. MTS deviates in the address field to include multiple destination addresses for the broadcast network.

(4) ADAPD. AFAPD is based on the MTS broadcast protocol with a change in the address field to provide a mechanism for frame relay.

(5) VMF. VMF is a newly approved joint US DoD (under configuration management by JTC3A) protocol based on HDLC that is also closely related to both the MTS and ISO 8802-2. It provides both the connection-oriented and connectionless sets of procedures and modifies the definition of both the address and control fields. The connection-oriented set uses the BAC class of procedures and HDLC options 1, 2, 3, 7, 11, and 14. The connectionless operation is identical to the MTS operations.

---

10 *Program Design Specification for the Air Force Application Program Development (AFAPD) for the Digital Communications Terminal (DCT), AN/PSC-2*, US Air Force (TAC/DRI), May 1989, UNCLASSIFIED.

11 ISO 8802-2, *Logical Link Control*, First Edition, 1989.

Discussion. Table C-3 shows a comparison of frame formats and functions performed by the HDLC, X.25 LAPB, ISO 8802-2, MTS, VMF, and AFAPD data link protocols. The following paragraphs discuss each row of Table A-1 to highlight the areas of deviation and to explain the reasons for the deviation.

a. Frame Format. Only ISO 8802-2 varies from the HDLC frame format because it does not have the Frame Check Sequence (FCS) or Flag fields. This is primarily because 8802-2 is used with a Media Access Control (MAC) layer, which provides the FCS and Flag field functions, so the fields in ISO 8802-2 would be redundant.

b. Control Field Size. Only VMF for Type 2 service varies from the HDLC standard. A control field exists for each destination address to allow multiple addressing in the connection-oriented mode at the data link (there is no upper layer connection). The sequence windows are different for each of the destination addresses. Therefore, the control field contents are different for each destination. The control field size per destination is a fixed size, one byte.

c. Control Field Size Determination. Only VMF differs from the HDLC standard. In VMF, the size of the control field varies in relation to the number of destination addresses. The control field is composed of 1 to 16 one-byte control subfields. The other standards have control fields that are fixed by agreement to one or two bytes. The VMF variation accommodates multiple addressing in a connection-oriented environment. However, the control field size per destination is determined at initialization, since the VMF standard only allows the SABM (not the SABME) control format that designates the one byte control field.

d. Control Field Formats. All of the HDLC variants choose the formats from the complete set of HDLC formats according to the needs of the protocol. All of the connection oriented protocols (LAPB, and Type 2 services in ISO 8802-2 and VMF) use the basic set of control field formats and one or more from the optional formats. The connectionless mode protocols (MTS and Type 1 services in ISO 8802-2 and VMF) use a subset of the HDLC basic control field formats, because those pertaining to the connection set-up, maintenance, and disconnect are not required.

e. Address Field Size. A variance in this field is allowed by the basic HDLC protocol. While the size of the address can vary according to the HDLC standard, only one address is allowed. ISO 8802-2, MTS, AFAPD, and VMF have all extended the address field for the purpose of including the source address as well as the destination address. Those protocols are not point-to-point so the source is not obvious (as it is in the LAPB point-to-point protocol). MTS, VMF, and AFAPD have further extended the field to allow multiple destination addresses (an expansion of the group address). MTS, AFAPD, and VMF use the HDLC method [least significant bit (LSB) indicator] to extend the field. ISO 8802-2 uses the LSB for another purpose but has a fixed size address field. AFAPD further extends and modifies the address field to provide a frame relay function. The length of the field depends of the number of destinations and the use of the relay function.

- MTS, AFAPD, and VMF use the HDLC address extension method (LSXB) to lengthen the address field. Within the longer field, MTS and VMF identify subfields for the source and one or more destination addresses. ISO 8802-2 defines two address fields that are each one byte long. ISO 8802-2 does not use the LSB to indicate the extended address field. That bit indicates a group address in the destination address, and a command or response in the source address.
- VMF designates an address (value = 1) to have additional special significance within that protocol. The address equal to 1 is used to indicate the frame is in the Type 2 operation format. (ISO 8802-2 also allows both Type 1 and Type 2 operation. The service types are distinguishable in ISO 8802-2 because they contain exclusive sets of control field formats.)
- AFAPD address field content is identical to MTS if there is no relay destination. However, the address field has several additional subfields for the relay function. there are two source addresses instead of one (the originator and the current transmitting link address) and two destination fields (the final destination and a relay destination). There are three additional subfields (relay, flag, and hopcount) that are used in the relay process.

Table C-3. Comparison of Example Broadcast Protocols with HDLC, X.25 LAP B, and LLC

	HDLC 7809 BAC	X.25 LAP B	802.2 LLC	MTS BROADCAST	VMF	AFAPD
Frame Format	Flag Address Control Info CRC Flag	Same	DSAP, SSAP Control, Info	Same	Same	Same
Control Field Size	Extendable 1 or 2 Bytes for I PDU and S PDU. 1 Byte for S PDU	Same	2 Bytes for I PDU and S PDU. 1 Byte for U PDU.	1 Byte only	Type 1 1 Byte only Type 2 2 Bytes only	1 Byte only
Control Field Size Determination	At Link Set-Up	At Link Set-Up	Fixed	Fixed	Fixed	Fixed
Control Field Formats	(if no options) Comm Resp I I RR RR RNR RNR SABM UA DISC DM FRMR with options add: SABME XID XID SREJ SREJ UI UI REJ REJ SIM RIM UP TEST TEST RSET RD	Comm Resp I I RR RR RNR RNR SABM UA SABME DM DISC FRMR	Type 1 Comm Resp UI XID XID TEST TEST Type 2 I I RR RR RNR RNR SABME UA DISC DM REJ FRMR RSET REJ	Comm Resp I RR RR RNR RNR XID XID	Type 1 Comm Resp I RR RR RNR RNR XID XID Type 2 I I RR RR RNR RNR SABM UA DISC DM REJ FRMR SREJ RSET	Same as MTS
Address Field Size	Extendable 1 to XX Bytes	1 Byte	2 Bytes	2-17 Bytes	2-17 Bytes	3-20 Bytes
Address Field Formats	Source: None Destination: Global = 11111111 Group = by Agreement No Station = 0 Range = 0-255 or 0-127 if Extended	11000000 or 10000000	Source: 7 Bits 1-126 Destination: Global = 11111111 Group = 1XXXXXXX No Station = 0 Range = 0-127	Source: 7 Bits 1-126 Destination: Global = 11111111 No Station = 0 Range = 0-127	Source: Bits 2-95 Destination: Global = 11111111 Group = 96-126 No Station = 0 Special = 1 Range = 0-127	Source Originator Direct Destination Relay Flag Hop Count Relay Destination
Address Field Size Determination	LSB	Fixed	Fixed	LSB	LSB	LSB and Relay Function

Table C-3. (Continued)

	HDLC 7809 BAC	X.25 LAP B	802.2 LLC	MTS BROADCAST	VMF	AFAPD
Info Field Size Max	Any # of Bits	259 Bytes	Any # of Bytes	3500 Bytes	Negotiable Max = 3500	3500 Bytes
FCS	16 Bit or 32 Bits (Option #14)	16 Bit	None	32 Bit	32 Bit	32 bit
P/F Bit	P - One out-standing Re-quest F - Set in response to received P Bit	Same	Same	Same	Same	Same
Sequence Numbers	0-7 or 0-127	0-7 or 0-127	0-127	Not Used	Type 2 0-127	Not Used
Link Set-up Disc	SABM → UA SABME → UA DISC → UA	SABM → UA or SABME → UA DISC → UA	Type 1 Not Used Type 2 SABME → UA DISC → UA	Not Used	Type 1 XID Type 2 SABM → UA DISC → UA	Not Used
Network Control	XID	None	Type 1 XID Type 2 None	XID	XID	Not Used

g. Address field size determination. ISO 8802-2 deviates from HDLC because it defines two separate address fields of one byte each. It does not use the LSB to indicate an address field longer than one byte. AFAPD field size depends on the number of destination and if relay is requested.

h. Information Field Size Maximum. Each protocol adheres to the HDLC standard because HDLC allows any information field size.

i. FCS. ISO 8802-2 does not use the FCS field because the LLC is used with a MAC layer which provides the FCS functions. All of the other protocols use either the basic (16 bit) or optional (32 bit) FCS as allowed by the HDLC standard.

j. P/F Bit. Same.

k. Sequence numbers. ISO 8802-2 MTS, and VMF do not use sequence numbers in the connectionless-mode of service. Sequence numbers are used for flow control and sequencing that are not functions of the CL service. VMF Type 2 operation uses the extended sequence number range (0-127).

l. Link Set-up and Disconnect. All of the protocols that provide a connection-oriented service adhere to the HDLC standard for the link set-up and disconnect. The connectionless service mode in MTS, VMF, and ISO 8802-2 do not perform this function.

m. Link Control. The XID command is an optional command and response in HDLC. ISO 8802-2, MTS, and VMF use the XID format to pass link control information in the information field according to ISO 8885 - *HDLC Procedures - General Purpose XID Frame Information Field Content and Format*. AFAPD uses the XID with a one-byte information field for link initialization but does not follow ISO 8885 rules to identify the XID information field content.

5.2 Comparison of US Data Communications Broadcast Protocols Planned for Use in Land Warfare Fire Support CCISs[12]

Overview. MTS broadcast standard, VMF, and CPS[13] are all bit-oriented communication protocols that have a data link layer to support combat net radio, a broadcast communications medium. VMF and CPS were produced in parallel with the same Army and Marine Corps representatives and are based on the MTS protocol. In fact, the VMF specification was written using the MTS TIDP, Volume V, as the beginning text. This section compares the functional differences among the MTS, VMF, and CPS protocols and evaluates their ability to interoperate.

Functional Differences. Table C-4 lists the functions performed at each of the layers and briefly states the differences among the protocols.

a. Physical Layer. There are no functional differences among the protocols in this layer.

b. Data Link Layer. Listed below are three functional differences among the protocols.

- Media Access. The VMF protocol implements both a random and a prioritized method of calculating the net access delay (NAD) time. MTS only implements the random method, and CPS only implements the prioritized method and a hybrid scheme that is a mix of the random and prioritized schemes. Since VMF implements both schemes, the different media access schemes only create an interoperability problem between the MTS and CPS protocols. Since the VMF protocol was developed to provide Marine Corps and Army fire support interoperability, there is not a problem.
- Connection Establishment and Release. An XID exchange was developed for the VMF protocol that CPS and MTS adopted.
- Acknowledgement. MTS optionally acknowledges frames in a stop and wait method. VMF and CPS implement that method and also implement a connection-oriented service with a sliding window.

c. Network Layer. While the MTS broadcast protocol allocates space or the network header, it is not functional. For this layer only, the functionality of the MTS switched protocol will be compared to the other protocols. See Table A-2. The differences are listed below.

- Message Types. In the VMF and CPS protocols, the message type field defines a more expansive list of message types. Message format types include VMF, MTS, STANAG 5620, TACFIRE, and potentially IP. The same division of SYSCON, perishable, a non-perishable messages remains, however, so there is no related interoperability problem.
- Routing. VMF and CPS both allow a destination source list to be present in the network header. MTS switched protocol would interpret this list as multiple destinations rather than a routing list. MTS, VMF, and CPS are not interoperable when more than one destination address is present in the header. A change to MTS is proposed to adopt source list routing.
- Message Segmenting. MTS (broadcast) and VMF allow a system to optionally implement segmentation. CPS segments messages over 3,500 bytes. This is not currently a problem because the broadcast medium allows a frame size of 3,500 bytes, which accommodates the longest message. Segmentation is not necessary.
- Originator and Addressee. MTS and VMF use the principle of a 3-byte geographical or fixed hierarchical address. The description of its use is different because the routing function has been moved from the switches into end systems in the broadcast medium.

d. Transport Layer. There are no functional differences among the protocols in this layer.

---

12 This section is based on a contribution from the US Marine Corps, *Comparison of the Marine Tactical System (MTS(, Variable Message Format (VMF), and Army Fire Support Bit-Oriented Message (AFS-BOM) Protocols*, Draft, MCRDAC/Integration, 15 November 1991, UNCLASSIFIED.

13 Communication Protocol Standard (CPS), formerly known as Army Fire Support Bit-Oriented Messages (AFS BOM).

Table C-4. Comparison of Protocol Functions

FUNCTIONS	MTS	VMF	CPS
Physical Layer			
Electrical			
Mechanical			
Functional			
Procedural			
Link Layer			
Frame Formatting			
Frame Addressing			
Commands and Responses			
Media Access	Random	Random & Prioritized	Prioritized + Hybrid
Connection Establishment & Release	One XID exchange	2 new XID exchanges	?
Frame Transfer			
Acknowledgement	Verifies data pattern	Does not verify data pattern	Does not verify data pattern
Retransmission			
Error Detection & Correction			
Network Layer			
Header	* 3 message format types	9 message format types	9 message format types
Routing	* Directory	Directory & Source	Directory & Source
Message Segmenting	* Yes	optional	Yes
Packet Addressing	*		
Packet Precedence	* 3 precedence levels	3 precedence levels	3 precedence levels
Network Flow and Congestion Control	*		
End-to-End Error Recovery	* Yes	None	None
Transport Layer			
Null			
Session Layer			
Presentation Layer			
Message Formatting	Format 3	Format 3	Formats 1, 2, and 3
Application Layer			
Message Header			Different bit interpretation of message number field
Message Acknowledgement	Receipt/Compliance	Receipt/Compliance	Receipt/Compliance
System Management	*		

* Function is present in the MTS switched protocol, but not in the MTS broadcast protocol.
Blank fields indicate that all of the protocols implement the function the same.

e. Presentation Layer. MTS and VMF only allow VMF message Format 3, but CPS will also allow VMF message Formats 1 and 2. CPS will not send Format 1 or 2 messages to either MTS or VMF protocols, so this layer will be interoperable.

f. Application Layer. The message number field in the header contains a different data element structure in each of the protocols. In both MTS and VMF, message number is 17-bit field made up of a 7-bit functional area element and a 10-bit number element. MTS interprets the functional area as an ASCII character and VMF as a numeric. CPS divides the 17-bit message number field into a 3-bit format designator element, a 4-bit functional area element and a 10-bit number element. CPS will zero fill the 3-bit format designator element to achieve interoperability with VMF. MTS would not recognize VMF or CPS message numbers.

APPENDIX D

INTERNATIONAL CIVIL STANDARDS RELEVANT TO CCISs

I. OSI Architecture and General Standards
II. Layer 1: Physical Layer
III. Layer 2: Data Link Layer
IV. Layer 3: Network Layer
V. Layer 4: Transport Layer
VI. Layer 5: Session Layer
VII. Layer 6: Presentation Layer
VIII. Layer 7: Application Layer
IX. Miscellaneous Standards

INTERNATIONAL CIVIL STANDARDS RELEVANT TO CCISs[1]

I. OSI ARCHITECTURE AND GENERAL STANDARDS[2]

A. OSI Basic Reference Model and Conventions
B. Work Plans and Coordination Agreements
C. Formal Description Techniques (FDTs)
D. Security
E. OSI Management
F. OSI Registration Authorities
G. OSI Conformance Testing
H. Taxonomy and Profiles

A. OSI BASIC REFERENCE MODEL AND CONVENTIONS:

STANAG 4250[3] ♦	NATO Reference Model for OSI, April 1986	
	Part 1--General Description, Revised Draft, May 1990	
	Part 2--Security, Draft (SANISI Document)	
	Part 3--Naming and Addressing, Draft, December 1991	
	Part 4--Management, Draft, November 1990	
	Part 5--Military Features, Draft (Working Document)	
	Part 6--NATO Standardized Profiles, Draft, December 1991	
ISO[4] 7498 ♦	OSI Reference Model - Part 1: Basic Reference Model, General Aspects [SC21 N 3273]	
	Cor 1	Technical Corrigendum 1, 15 December 1988
	AD[5] 1 ♦	Connectionless-Mode Transmission
	PDAD[6] 2 ♦	Multipeer Data Transmission (MPDT) (work suspended; comments on reactivation of MPDT project have been requested [SC21 N 6197])
CD[7] 7498-1	OSI Reference Model - Part 1: General Aspects [Revision, November 1991 SC21 N 6152]	

---

1 Revised November 1991 based on multiple sources, including "Status of OSI (and Related) Standards," in *Computer Communication Review*, January 1991, pp. 111-131.

Two BSI documents (*ISO/IEC JTC1/SC21 Project File*, IST21 N 2933, 30 January 1991; and *Project Overview*, IST21 N 2844, 13 June 1991) were additional major sources for updating the list of standards.

2 The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

3 STANAG: NATO Standardization Agreement

4 ISO: International Standard with final approval from ISO.

5 AD: Addendum for ISO standard.

6 PDAD: Proposed or Preliminary Draft Addendum to ISO standard.

7 CD: Committee Draft for ISO standard [formerly Draft Proposal (DP)].

ISO 7498-2♦	OSI Reference Model - Part 2: Security Architecture
ISO 7498-3♦	OSI Reference Model - Part 3: Naming and Addressing
ISO 7498-4♦	OSI Reference Model - Part 4: Management Framework
TR[8] 8509♦	Service Conventions
DIS[9] 10731	Conventions for Definitions of OSI Services, August 1991 [SC21 N 6341] (IS status expected March 1992; will supersede TR 8509)
TR 9575	OSI Routing Framework, June 1990
DTR[10] 10730♦	Tutorial on Naming and Addressing, August 1991 [SC21 N 5335] (IS text expected June 1992)
WDTR[11] xxxx	Catalogue of PICS Proforma Notations, July 1991 (joint work of WG1 and CCITT SG VII; meeting scheduled for February 1991) [SC21 N 6160]
SC5 N 220[12]	Interim Report of the TCCA Rapporteurs' Group of Time-Critical Communications Architecture and Systems, 15 April 1991
SC6 N 4782	An Architectural Framework for Private Networks, Pre-Publication Version of ECMA TR 44, December 1987
SC21 SD-9[13]	Approved Commentaries on the Basic Reference Model for Open Systems Interconnection, SC21 OSI Reference Model Editor, July 1991 [SC21 N 6198]
SC21 N 2524	SC21/WG1 Overview - OSI Architecture, 29 January 1991
SC21 N 3207	Relationship Between Objects in Peer Open Systems, December 1988 [SC21/WG6]
SC21 N 3711	Requirements for Multipeer Data Transmission, July 1989
SC21 N 3906	Final Report to SC21 in Florence on the Reassessment of Project JTC 1.21.9.1 on Multipeer Data Transmission, October 1989
SC21 N 4647	Requirements for Service Conventions, May 1990
SC21 N 4681	User Requirements for Multi-Party Communications (MPC), Canada, May 1990
SC21 N 4682	Establishment of User Requirements, Canada, May 1990
SC21 N 4763	On-Going Multipeer Projects Within JTC1, ANSI, May 1990
SC21 N 5017	Relationship Between Concepts and Models for OSI and ODP, SC21/WG6, July 1990
SC21 N 5073	Final Answer to Q1/30.5 on Definition of the Term "Quality of Service," SC21/WG1, May 1990
SC21 N 5074	Final Answer to Q1/330.6 on Relay, Routing, and Network Management, SC21/WG1, May 1990
SC21 N 5081	Draft Answer to Q1/61 on Consistency Among ISO Standards Related to the OSI Reference Model, May 1990
SC21 N 5093	Status and Method of Operation for the Reference Model Revision, SC21/WG1, May 1990
SC21 N 5095	Liaison to SC6 on Revision of the Reference Model, May 1990
SC21 N 5096	Liaison to CCITT SG VII on Revision of the Reference Model, June 1990

8 TR: Technical Report for ISO.

9 DIS: Draft International Standard for ISO.

10 DTR: Draft Technical Report for ISO.

11 WDTR: Working Draft Technical Report for ISO.

12 Selected working drafts (e.g., SC6 N 4782) have been included from ISO/IEC JTC1 Subcommittee (SC) 5, SC6, SC18, SC20, SC21, SC22, and the Special Group on Functional Standardization (SGFS). These and other JTC1 standards organizations are discussed in Appendix F.

13 SD: Standing Document for an ISO subcommittee.

SC21 N 5099	Liaison Statement to CCITT SG VII(Q.25) on Service Conventions, SC21/WG1, May 1990
SC21 N 5105	Final Answer to Q1/56.6.1 on Positioning of Circuit Switched Networks, SC21/WG1, May 1990
SC21 N 5109	Liaison Statement to CCITT SG VII(Q23) on Naming and Addressing, SC21/WG1, May 1990
SC21 N 5110	Call to National Bodies and Liaison Organizations for Contributions on Technical Structure of Quality of Service (QoS) Architecture, May 1990
SC21 N 5196	Report of the Special Meeting on User Requirements, SC21, 7 June 1990
SC21 N 5197	Report of the Standards Maintenance Group, SC21, 4 June 1990
SC21 N 5501	Working Draft of Revised ISO 7498-1 Clauses 7.1 - 7.3, Information Transfer, Retrieval and Management for Open Systems [SC21/WG1, November 1990]
SC21 N 5840	Comments on the Relationship Between Concepts and Models for OSI and ODP, USA, April 1991
SC21 N 5848	Request for Documenting Requirements for More Performant Association Establishment, 4 April 1991
SC21 N 5849	USA Requirements to Reactivate the Multipeer Data Transmission Project (JTC 1.21.09.01), USA, April 1991
SC21 N 5933	Conventions for the Definition of OSI Services, DIS 10731, 1991
SC21 N 5934	Collection of Definitions of OSI Vocabulary (April 1991 Version), Rapporteur on Q17: OSI Vocabulary, June 1991
SC21 N 6069	Proposed New WG6 Question Q6/2 on the Relationship Between the OSI Upper Layer Architecture and ODP, 24 July 1991
SC21 N 6070	Working Draft Answer to the Proposed WG6 Question on the Architectural Relationship Between OSI and ODP, 25 June 1991
SC21 N 6157	Answer to CCITT SG VII Q 23 on OSI Reference Model Regarding ISDN, May 1991
SC21 N 6158	Final Answer to Q1/62 (Quality of Service Architectural Issues), WG1, May 1991
SC21 N 6159	Framework on Quality of Service, WG1, May 1991
SC21 N 6160	Catalogue of PICS Proforma Notations, WG1, July 1991
SC21 N 6197	WG1 Position on the Reactivation of Project 1.21.9.1 (Multi-Peer Data Transmission), WG1, July 1991 (national body comments requested by 31 March 1992)
SC21 N 6198	Approved Commentaries on the OSI Basic Reference Model [SC21 SD-9], July 1991
SC21 N 6346	Liaison Statement to JTC1/SC21 on Data Link Layer Security, 16 August 1991
SC21 N 6348	Liaison Statement to JTC1/SC21 Regarding a NP on "Framework for CIM Systems Integration", 16 August 1991
SC21 N 6494	Revised OSI Reference Model - Working Group Version Q56 Rapporteur, 24 October 1991
CCITT X.200	Reference Model of OSI for CCITT Applications
CCITT X.210	OSI Layer Service Definition Conventions
IST18[14] N 2694	Final Report on the Framework for Open Systems, July 1990
IST21 N 2508	PICS Proforma Notations, January 1991
IST21 N 2551	UK Response to SC21 N 5110 on the Technical Structure of Quality-of-Service (QOS) Architecture, February 1991
IST21 N 2552	Proposed UK Contribution on QOS, Joint Meeting on QOS, January 1991

[14] IST: Committee of the British Standards Institute (e.g., IST21 is associated with SC21).

IST21 N 2860	EWOS Technical Guide Routeing in the Context of OSI, EWOS-EGLL9172, Final Draft, 27 May 1991
IST21 N 2433	EWOS/TA/PT N004 Final Report on the Framework for Open Systems

B. WORK PLANS AND COORDINATION AGREEMENTS:

JTC1 N 1260	SC21 Request to Modify its Programme of Work, ISO/IEC JTC1, March 1991
JTC1 N 535	Directives for the Work of ISO/IEC Joint Technical Committee 1 (JTC1) on Information Technology, Secretariat, August 1989
JTC1 N 598	JTC1 Strategic Plan, Editing Team, November 1989
JTC1 N 1387	Contribution from JTC1/SC21 on Proposed Changes to JTC1 Organization, 10 June 1991
JTC1 N 1562	ISO/IEC JTC1/SC21 Contribution to the JTC1/SWG on Procedures Regarding Maintenance and Correction of Defects, 9 September 1991
SGFS[15] N 151	CCITT Liaison Statement on Work of SGFS, November 1989 (includes X.220)
SGFS N 225	Resolutions of JTC1 Advisory Group, June 1990
SGFS N 229	Resolutions of the 3rd Regional Workshop Coordinating Committee Meeting; AOW - EWOS - NIST OIW, June 1990
SGFS N 236	EWOS Organization and Activities, June 1990
SGFS N 282	Resolutions of the 4th RWS-CC Meeting, 18-19 October 1990, January 1991
SGFS N 300	List of documents (N 182 - N 300), Secretariat, February 1991
SGFS N 373	Output from the 5th Regional Workshop Coordinating Committee (RWS-CC), March 18-19, 1991, 13 June 1991
SC21 SD-1	Report of the Secretariat to the Plenary Meeting of ISO/IEC JTC1 SC21, 5-6 June 1990, Seoul, Republic of Korea, SC21 Secretariat, April 1990 [SC21 N 4588] (provides terms of reference and points of contact for working groups)
SC21 SD-2	ISO/IEC JTC1 SC21 Programme of Work (POW) - Target Date Summary for All Active and Published Projects, SC21 Secretariat, April 1990
SC21 SD-7	Security Management Plan, 4 June 1990 [SC21 N 5130]
SC21 SD-8	Schedule of Meetings, SC21, June 1991 [SC21 N 6261]
SC21 N 2525	IST/21 Project File: January 1991, January 1991
SC21 N 3122	Informal Guide for ISO/IEC JTC1 and CCITT Cooperation, January 1989
SC21 N 3205	Proposed Modus Operandi and Programme of Work of SC21/WG6 ULA Rapporteur Group, December 1988 [SC21/WG6]
SC21 N 4758	Request to ISO/IEC SC21 from OSF for Establishment of Liaison Relationship, May 1990
SC21 N 4801	Liaison Statement to SC21 on Joint Efforts Between SG VII(Q20) and SG I(Q16), CCITT SG I(Q.16), May 1990
SC21 N 4903	Methodology and Guidelines for the Development of Application Layer Standards, SC21/WG6, June 1990
SC21 N 5071	Recommendations Approved by SC21/WG1 at its Seoul Meeting, 23-31 May 1990, SC21/WG1, May 1990
SC21 N 5072	List of Output Documents of SC21/WG1 Meeting, Seoul, 23-31 May 1990, SC21/WG1, July 1990
SC21 N 5131	Recommendations of the SC21/WG6 Meeting, 23 May - 1 June 1990, Seoul, SC21/WG6, June 1990
SC21 N 5136	Recommendations of SC21/WG3 Meeting in Seoul, May/June 1990, SC21/WG3, June 1990

[15] SGFS: Special Group on Functional Standardization [develops International Standard Profiles (ISPs)].

SC21 N 5154	Recommendations of the SC21/WG5 Meeting, Seoul, 24 May - 1 June 1990, SC21/WG5, June 1990
SC21 N 5194	Resolutions of the Fourth Plenary Meeting of SC21, 5 June 1990, Seoul, SC21, June 1990
SC21 N 5203	SC21/WG1 Convenor's Report to SC21 Plenary Meeting, Seoul, 5-6 June 1990, SC21/WG1, June 1990
SC21 N 5219	Draft Management Guidelines for SC21, Rapporteur for Strategic Planning, July 1990
SC21 N 5228	Report of the ISO/IEC JTC1/SC21 Plenary Meeting, 5 June 1990, Seoul, Korea, July 1990
SC21 N 5229	Report of the JTC1/SC21 Plenary Meeting, 5 June 1990, Seoul, Republic of Korea
SC21 N 5337	EWOS Organizations and Activities, 9 October 1990, EWOS
SC21 N 5505	Liaison to CCITT Q23/VII and Q19/VII, ISO/IEC JTC WG6 ULA, November 1990
SC21 N 5599	Notice of and Draft Agenda for the ISO/IEC JTC1/SC21 Meeting, 4 & 5 June 1991, Arles, France, SC21 Secretariat, February 1991
SC21 N 5605	Subcommittee Report to the ISO/IEC JTC 1 Advisory Group Meeting, 19 - 21 February 1991, Washington, D.C., USA, January 1991
SC21 N 5714	Resolutions of the ISO/IEC JTC1 Advisory Group Meeting, Washington, D.C., 19-21 February 1991, 8 March 1991
SC21 N 5830	SC21 Standards Maintenance, AFNOR, April 1991
SC21 N 5978	Review of SC21 Operation and Structure, May 1991
SC21 N 5984	Report of the Interim Q25/VII and Q26/VII Rapporteur Group Meetings, 11-15 March 1991, 9 May 1991
SC21 N 6060	Proposed Draft Answer to Question Q6/1--Versions and Extensibility, SG6, May 1991
SC21 N 6018	Resolutions of the Eighth SC21/WG4 Meeting, Arles, 20-27 May 1991, 20 June 1991
SC21 N 6019	Minutes of the Eighth SC21/WG4 Meeting, Arles, 20-27 May 1991, May 1991
SC21 N 6020	SC21/WG4 Convenor's Report to the ISO/IEC JTC1/SC21 Plenary Meeting, Arles, June 1991, 20 June 1991
SC21 N 6023	Work Plan for SC21/WG4 Systems Management, 20 June 1991
SC21 N 6061	Progression of Methodology and Guidelines for the Development of Application Layer Standards, WG6, June 1991
SC21 N 6076	Resolutions of the ISO/IEC JTC1/SC21/WG7 Meeting in Arles, France, 22-31 May 1991, 5 September 1991
SC21 N 6078	WG7 Convenor's Report to the SC21 Plenary Meeting in Arles in June 1991, 25 July 1991
SC21 N 6162	ISO/IEC JTC1/SC21/WG1 Programme of Work, 29 July 1991
SC21 N 6204	List of Late Contributions and Output Documents of SC21/WG1 Arles Meeting, 22-30 May 1991, May 1991
SC21 N 6205	Report of the ISO/IEC JTC1/SC21/WG1 Meeting, Arles, France, 29 July 1991
SC21 N 6210	Recommendations Approved by the ISO/IEC JTC1/SC21/WG1 at its Arles Meeting, 22-30 May 1991, May 1991
SC21 N 6217	Recommendations of the ISO/IEC JTC1/SC21/WG5 Meeting, Arles, 23-31 May 1991, June 1991
SC21 N 6248	Resolutions of the ISO/IEC JTC1/SC21/WG6 Meeting, 22-31 May 1991, Arles, France, 10 June 1991
SC21 N 6249	Resolutions of the SC21/WG3 Meeting, Arles (May 1991), 23 July 1991
SC21 N 6260	Report of WG1 Convenor, May 1991

SC21 N 6261	Standing Document 8: SC21 Schedule of Meetings, 20 June 1991
SC21 N 6262	Notes of Ad Hoc Meeting on SC21 Organization, Arles, June 1991
SC21 N 6263	SC21 Contribution to JTC1 SWG Meeting on Organization, 17-19 June 1991, ANSI, 10 June 1991
SC21 N 6264	WG6 Convenor's Report to the SC21 Plenary Meeting in Arles in June 1991, 25 July 1991
SC21 N 6265	ISO/IEC JTC1/SC21/WG5 Convenor's Report to the ISO/IEC JTC1/SC21 Plenary Meeting in Arles, 26 August 1991
SC21 N 6273	Resolutions of the Seventh Plenary Meeting of ISO/IEC JTC1/SC21, 4-5 June 1991, Arles, France, 20 June 1991
SC21 N 6275	Plan to Mechanize the ISO/IEC JTC1 Secretariat (SC21 Pilot Project), June 1991
SC21 N 6277	JTC1 Advisory Group Resolution 8:1991 Regarding Long Range Planning Group (LRPG) Items of High Importance (JTC1 N 1192) and A Vision for the Future (extract contained in JTC1 N 1351), 26 June 1991
SC21 N 6348	Liaison Statement to JTC1/SC21 Regarding a NP on "Framework for CIM Systems Integration", 16 August 1991
SC21 N 6399	The Way Ahead, 10 September 1991
SC21 N 6478	Target Dates for Completion of SC22 Projects, 7 November 1991
SC21 N 6482	Progress Report on ISO/IEC JTC1 and CCITT Cooperation, 23 October 1991
SC21 N 6484	Guide for CCITT and ISO/IEC JTC1 Cooperation, Collaborative Group on Procedures for CCITT and JTC1 Cooperation, 23 October 1991
SC21 N 6493	Revised SC21 Management Guidelines SC21 Strategic Planning Rapporteur, 24 October 1991
SC21 N 6527	Resolutions of the ISO/IEC JTC1 Plenary Meeting, October 2-4, 1991, Madrid, JTC1 Secretariat, 31 October 1991
SC21 N 6528	Request for Review and Action on Resolution 18 (Advisory Group Report - Application Environment Profiles) of the JTC1 Plenary Meeting, October 2-4, 1991, Madrid, JTC1 Secretariat, 31 October 1991
SC21 N 6530	Report of the JTC1 Plenary Ad Hoc Group on EDI, 31 October 1991
SC21 N 6538	Proposed New SC21 Working Group Structure, 4 November 1991
SC21 N 6553	Japanese Position on the SC21 Restructuring, 7 November 1991
IST21 N 2393	Proposals for Corrigenda to OSI Standards - Reprint from BSI News, November 1990
IST21 N 2670	Prospective vs Traditional Standardization, March 1991
IST21 N 2754	Extension of M-IT-01 and M-IT-02 for the Open System Environment, European Workshop for Open Systems, EWOSTA9181, April 1991
IST21 N 2766	March 1991 Resolutions RWS-CC, May 1991
IST21 N 2769	Summary of EWOS Contribution to JTC1 SGFS, June 1991, May 1991
IST21 N 2770	AD HOC Meeting on an Open Systems Framework, May 1991
IST21 N 2793	Status of Project Teams, 29 May 1991
IST21 N 2835	Report on SC21/WG6 Meeting, Arles, May 1991, 4 June 1991
IST21 N 2836	Report on SC21/WG6 ULA Rapporteur Meeting, Arles, May 1991, 5 June 1991
IST21 N 2837	Report on the Arles IRDS Meetings, 4 June 1991
IST21 N 2840	Resolutions of the Seventh Plenary Meeting of ISO/IEC JTC1/SC21, Arles, France, 4-5 June 1991
IST21 N 2842	ISO/IEC JTC1/SC21 Subcommittee Report Part IV: Programme of Work, 3 June 1991

IST21 N 2967	UK Report on ISO/IEC JTC1/SC21/WG1 meeting held in Arles, France (22-30 May 1991), June 1991
IST21 N 2968	ISO/IEC JTC1/SC21 WG3 Data Base, UK Delegate's Report, August 1991
IST21 N 2981	Report of the SC21 Upper Layers Conformance Testing (ULCT) Meeting, May 1991
IST21 N 3038	Informal Notes of the ISO/IEC JTC1 & CCITT Cooperation Meeting, 17-18 September, 1991
IST21 N 3045	Resolutions 7th ISO/IEC JTC1/SGFS meeting, June 18-21, 1991, Berlin, 15 August 1991
IST21 N 3046	JTC1 Directives Annex C, 20 September 1991

C. FORMAL DESCRIPTION TECHNIQUES (FDTs):

ISO 8807♦	LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behavior
DAM[16] 1	Graphical Representation of LOTOS (G-LOTOS) (new work item proposal of December 1989 not accepted; status uncertain work is proceeding) [SC21 N 4871]
ISO 9074♦	Estelle - A Formal Description Technique Based on an Extended State Transition Model
DAM 1♦	Estelle Tutorial [SC21 N 5710] May 1991 (IS text expected June 1992)
TR 10167	Guidelines for the Application of Estelle, LOTOS, and SDL [SC21 N 4259]
WDTR xxxx♦	Architectural Semantics for FDTs, Revised Draft, July 1990, SC21/WG1 [SC21 N 5116]
SC21 N 3132	TTCN Operational Semantics, November 1988
SC21 N 6088	Proposal for a WG7 Question on the Suitability of the Formal Description Technique Z for Use in ODP, 31 May 1991
CCITT X.250	Formal Description Techniques for Data Communications Protocols and Services
CCITT Z.100	Specification and Description Language (SDL)
CCITT Z.110	Criteria for the Use and Applicability of Formal Description Techniques

D. SECURITY:

ISO 8372	Modes of Operation for a 64-bit Block Cipher Algorithm, 1987
ISO 9160	Physical Layer Interoperability Requirements, 1988
ISO 9796	Digital Signature Scheme Giving Message Recovery, 1989
ISO 9797	Data Integrity Mechanisms Using a Cryptographic Check Function Employing a Block Cypher Algorithm, 1989
ISO 9798-1	Entity Authentication Mechanisms - Part 1: General Model
DP[17] 9798-2	Entity Authentication Mechanisms - Part 2: Entity Authentication Mechanisms Using Symmetric Algorithms
ISO 9979	Procedures for the Registration of Cryptographic Algorithms, July 1990 [SC27 N 88]
ISO 10116	Modes of Operation for an N-bit Block Cipher Algorithm, 1989 [SC27 N 86], 1991

16 DAM: Draft Amendment for an ISO standard (has the status of a DIS).

17 DP: Draft Proposal for an ISO standard [to be issued as Committee Drafts (CDs) beginning in 1990].

WD[18] 10181-1♦	Security Frameworks in Open Systems - Part 1: Overview, July 1991 [SC21 N 6166] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
DIS 10181-2	Security Frameworks in Open Systems - Part 2: Authentication Framework, May 1991 [SC21 N 5727] (IS status expected in March 1992)
	WDAM[19] 1 Authentication Elements, July 1991 [SC21 N 6172]
CD 10181-3♦	Security Frameworks in Open Systems - Part 3: Access Control Framework, July 1991 [SC21 N 6168] (DIS text expected in March 1992; IS status in December 1992)
WD 10181-4♦	Security Frameworks in Open Systems - Part 4: Non-Repudiation Framework, July 1991 [SC21 N 6165] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
WD 10181-5♦	Security Frameworks in Open Systems - Part 5: Confidentiality Framework, July 1991 [SC21 N 6164] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
WD 10181-6	Security Frameworks in Open Systems - Part 6: Integrity Framework, July 1991 [SC21 N 6163] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
CD 10181-7	Security Frameworks in Open Systems - Part 7: Security Audit Framework, July 1991 [SC21 N 6169] (DIS text expected in March 1992; IS status in December 1992)
WD 10181-8	Security Frameworks in Open Systems - Part 8: Key Management
DIS 10736	Transport Layer Security Protocol, JTC1/SC6, July 1991 (balloting ends June 1992)
	PDAM 1 Security Association Establishment Protocol, JTC1/SC6, July 1991 (balloting ends April 1992)
CD 10745	Upper Layer Security Model, June 1991 [SC21 N 6095] (CD ballot closes 22 October 1991)
CD 11577	Network Layer Security Protocol, JTC1/SC6, July 1991 (balloting ends April 1992)
WD xxxx-1	Cryptographic Mechanisms for Key Management, Part 1: Key Management Overview [SC27/WG2]
WD xxxx-2	Cryptographic Mechanisms for Key Management, Part 2: Key Management Using Secret Key Techniques [SC27/WG2]
WD xxxx-3	Cryptographic Mechanisms for Key Management, Part 3: Key Management Using Public Key Techniques [SC27/WG2]
WD xxxx-4	Cryptographic Mechanisms for Key Management, Part 4: Key Management Using Public Key Register [SC27/WG2]
WD xxxxx-1	Security Exchange Application Service Element (ASE) Part 1: Model and Specification Framework, WG6, 3 June 1991 [SC21 N 6096]
WD xxxxx-2	Security Exchange Application Service Element (ASE) Part 2: Service Definition, WG6, 3 June 1991 [SC21 N 6096]
WD xxxxx-3	Security Exchange Application Service Element (ASE) Part 3: Protocol Specification, WG6, 3 June 1991 [SC21 N 6096]
WD xxxxx-4	Security Exchange Application Service Element (ASE) Part 4: PICS Proforma, WG6, 3 June 1991 [SC21 N 6096]
JTC1 N 474	Proposal for a New Work Item: OSI Upper Layers Security Model, 21 July 1989 [SC21 N 5447, 30 October 1990]

[18] WD: Working Draft for ISO (status of text prior to being submitted as a Committee Draft).

[19] WDAM: Working Draft Amendment to an ISO Standard (has the status of a WD).

JTC1 N 996	IST/21 N 2478, Catalogue of Security Related Projects for consideration at the JTC 1 Workshop on Security 5-7 November 1990, May 1990
JTC1 N 1011	Results of National Body Survey for Consideration at the JTC1 Workshop on Security, 5-7 November 1990, London, 10 October 1990
JTC1 N 1015	ISO/IEC JTC1/SC21 Presentation Materials for the Workshop on Security (Topic: Security for OSI Management), 10 October 1990
JTC1 N 1016	ISO/IEC JTC1/SC21 Presentation Materials for the Workshop on Security (Topic: OSI Security Architecture and Security Frameworks), 10 October 1990
SC6 N 6219	Liaison to SC21 on Lower Layer Security, ISO/IEC/JTC1/SC6, October 1990
SC6 N 6221	Draft Network Layer Security Protocol, SC6/WG2, September 1990 (incomplete editor's Draft B)
SC6 N 6227	Lower Layer Security Guidelines, SC6/WG2/WG4, September 1990
SC6 N 6285	Working Draft OSI Transport Layer Security Protocol, SC6/WG4, September 1990
SC21 N 2555	Work in Security Within SC21, Gray Girling, February 1991
SC21 N 2652	Security Features in International Standards Profiles (ISPs), E.J. Humphreys, Chair of IST33, March 1991
SC21 N 3141	Response to SC21 N 2864, Issues Concerning the Requirements for Security Services in the Presentation Layer, November 1988 [SC21/WG1]
SC21 N 3167	Response to SC18 Liaison on Encryption, January 1989 [SC21/WG3]
SC21 N 3266	Guide for Open Systems Security, December 1988 [SC21/WG1]
SC21 N 3267	Plan for Work on Security in SC21, December 1988 [SC21/WG1]
SC21 N 3283	Working Draft for Lower-Layer Security Model, December 1988 [SC21/WG1]
SC21 N 3337	Security Management Domain and Security Policies
SC21 N 3991	Security Exchange Service Element, CCITT Q19/VII(DAF), November 1989 (CD text in SC21/WG6 expected in 1992)
SC21 N 4526	Application Layer Security Considerations, Workshop of Distributed Applications, April 1990
SC21 N 4648	Security and Security Exchange Information, February 1990, Canadian contribution to SC21/WG6
SC21 N 4833	Report to JTC1 from SC27 on Security Techniques, SC27 Secretariat, 21 May 1990 [SC27 N 94]
SC21 N 4834	Liaison Statement from SC27 to JTC1 Advisory Group, SC27 Secretariat, 21 May 1990 [SC27 N 93]
SC21 N 4835	Report of the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, SC27 Secretariat, 21 May 1990 [SC27 N 92]
SC21 N 4836	Resolutions Taken at the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, 21 May 1990 [SC27 N 94]
SC21 N 4980	Security Audit Framework Working Document, SC21/WG4, July 1990
SC21 N 5001	Upper Layers Security Model, Third Working Draft, SC21/WG6, June 1990
SC21 N 5002	Commencement of Work on Security ASEs, SC21/WG6, May 1990
SC21 N 5003	Distributed Applications Security Modelling and Infrastructure, SC21/WG6, July 1991
SC21 N 5054	Working Document on Presentation Service to Give Confidentiality and Integrity Protection, SC21/WG6, July 1990
SC21 N 5130	Security Management Plan, 4 June 1990
SC21 N 5346	U.S. Contribution on the Upper Layer Security Model (ULSM), October 1990 [SC21 N 5001]
SC21 N 5347	U.S. Contribution on the Security Frameworks Overview, November 1990 [SC21 N 5044]

SC21 N 5348	U.S. Contribution on the Access Control Framework, November 1990 [SC21 N 5045]
SC21 N 5349	U.S. Contribution on the Non-Repudiation Framework, November 1990 [SC21 N 5046]
SC21 N 5394	Collections of Definitions of OSI Vocabulary, June 1991
SC21 N 5447	The Upper Layers Security Model, fourth working draft, 30 October 1990 (CD text expected in 1991)
SC21 N 5448	Outline Working Draft for Part 1 of Generic Security Exchange ASE Definition, ISO/IEC, October 1990
SC21 N 5503	Response to Liaison Statement SC21 N 5453 on ULA Issues Arising in Security Work, ISO/IEC WG6 ULA, January 1991
SC21 N 5504	Response to Liaison Statement to WG 6 ULA and Upper Layers Security Groups [SC21/WG6 N 906], ISO/IEC WG6 ULA, January 1991
SC21 N 5529	Working Draft Access Control Framework, ISO SC21/WG1, February 1991
SC21 N 5530	Working Draft Confidentiality Framework, SC21/WG 1/CCITT, January 1991
SC21 N 5531	Working Draft Integrity Framework, SC21/WG 1/CCITT, January 1991
SC21 N 5532	Working Draft Security Frameworks Overview, SC21/WG 1/CCITT, January 1991
SC21 N 5533	Guide to Open Systems Security, SC21/WG1, 3 January 1991
SC21 N 5555	Liaison Statement to ISO/IEC JTC 1/SC 21 on Lower Layer Security, SC6, January 1991
SC21 N 5575	Request for National Body Comment, SC21/WG1/CCITT, January 1991
SC21 N 5576	Rapporteur's Report of the SC21/WG1/CCITT Collaborative Meeting on Security Frameworks, January 1991
SC21 N 5580	New Area of Work for SC27/WG1 on IT Security Information Objects, 7 January 1991
SC21 N 5581	New Area of Work for SC27/WG1 on IT Security Terminology, 7 January 1991
SC21 N 5582	Corrections to the Joint Text of the Second Editions for CMIS and CMIP, 7 January 1991
SC21 N 5731	Progression of the Upper Layers Security Standards, Canada, April 1991
SC21 N 5732	Use of Presentation Layer in Providing Confidentiality/Integrity, Canada, April 1991
SC21 N 5733	Proposed ASN.1 Useful Type to Support Presentation Layer Confidentiality/Integrity, Canada, April 1991
SC21 N 5734	Proposed Working Draft for Part 2 of Generic Security Exchange ASE Definition, Canada, April 1991
SC21 N 5737	Recommendation on Progression for CD 9075.2 Information Technology - Database Languages - SQL2, 10 April 1991
SC21 N 5738	Minutes of Editing Meeting for CD 9075.2, April 1991
SC21 N 5756	The Proliferation of Managed Objects, UK, March 1991
SC21 N 5757	Work on Security Within SC21, UK, March 1991
SC21 N 5853	Call for Contributions on SC21 N 5077 Clause 3.1, Formalization of User Defined Operation Definition, April 1991
SC21 N 5856	Discussion Paper on Multi-Protocol Testing, SC21/WG 1 and CCITT SG VII Collaborative Meeting on Conformance, Phoenix, 7-14 February 1991, 5 April 1991
SC21 N 5857	Proposed liaison to SGFS on Proforma Conformance Issues, April 1991
SC21 N 5858	Call for Contributions on Multi-User Test Methods, April 1991

SC21 N 5904	Liaison Statement to JTC 1/SC 18, SC21 and SC 27 - Tracking of Existing and New Security Related Work Items, ISO/TC 68/SC 2, April 1991
SC21 N 5928	Disposition of Comments on DIS 10729-1, April 1991
SC21 N 6037	Need for Security Services with OSI Management, SG4, July 1991
SC21 N 6058	Minutes of the Conceptual Schema Topic Meeting, October 1991
SC21 N 6096	Working Draft of Security Exchange ASE - Part 1: Security Exchange Model and Specification Framework, WG6, June 1991 [Part 2: Security Exchange ASE Service Definition; Part 3: Security Exchange ASE Protocol Specification; and Part 4: Security Exchange ASE PICS Proforma]
SC21 N 6097	Working Draft of Security Exchange ASE - Part 2: Security Exchange ASE Service Definition, WG6, June 1991
SC21 N 6098	Working Draft of Security Exchange ASE - Part 3: Security Exchange ASE Protocol Specification, WG6, June 1991
SC21 N 6099	Authentication Services for Distributed Applications, WG6, 1 July 1991 [WD in May 91, CD May 92, DIS May 93, IS May 94], JTC1 N 1437, July 1991 (new work item)
SC21 N 6130	Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression, WG6, June 1991
SC21 N 6167	Revised Draft Guide to Open Systems Security, WG1, July 1991
SC21 N 6172	Security Enhancement to Directory (Extension to ISO/IEC 9594-8), WG1, July 1991 (new work item)
SC21 N 6219	Liaison statement to ISO/IEC/JTC1/SC21 Lower Layer Security, 10 November 1990
SC21 N 6455	Proposed ASN.1 Specification Framework for Part 1 of Generic Security Exchange ASE Definition (SC21 N 6096), 11 October 1991
SC21 N 6456	Contribution to Part 3 of Generic Security Exchange ASE Definition (SC21 N 6098), 11 October 1991
SC21 N 6457	Frameworks Overview, 15 October 1991
SC21 N 6458	Integrity Framework, 15 October 1991
SC21 N 6459	Confidentiality Framework, 15 October 1991
SC21 N 6460	Contribution on the Security Exchange ASE-Part 3, 15 October 1991
SC21 N 6461	Contribution on the Definition of ENCRYPTED and SIGNED in CD 8824-3 and CD 8824-4,15 October 1991
SC21 N 6475	USA Contribution on the Security Exchange ASE - Part 1, 22 October 1991
SC21/WG6 N 1123	UK Position on Alignment of Upper and Lower Layer Security Protocols, 4 November 1991
SC21/WG6 N 1124	UK Comment on SC21 N 6130, Generic Transfer Syntax Providing Upper Layers Security, 4 November 1991
IST21 N 2478	Catalogue of Security Related Projects for Consideration at the JTC 1 Workshop on Security 5-7 November 1990, May 1990
IST21 N 2555	Work on security within SC21, 15 February 1991
IST21 N 2652	Security Features in International Standardized Profiles (ISPs), 31 January 1991
IST21 N 2852	POSIX Security Call for New Work Items, SC22/WG15, June 1991
IST21 N 3050	UK Comments Accompanying Vote of Disapproval on CD 10745, Upper Layers Securities Model, 2 October 1991

E. OSI MANAGEMENT:

ISO 9595:1991(E)♦	Common Management Information Service (CMIS) Definition, April 1991 CCITT X.710 [SC21 N 5302] (April 1991 edition incorporates AD 1 and AD 2)

	PDAM[20] 3	Support of Allomorphism, November 1990 [SC21 N 4966] (PDAM expected June 1993, IS in March 1994, IS in March 1995)
	DAM 4	Access Control, July 1991 [SC21 N 6286] (IS status expected in June 1992)
	WDAM 5	Enhanced Functionality, July 1991 [SC21 N 6039] (PDAM expected in 1993)
ISO 9596–1	Common Management Information Protocol (CMIP) Specification, April 1991 (CCITT X.711) [SC21 N 5303] (April 1991 edition incorporates AD 1 and AD2)	
	PDAM 3	Support of Allomorphism, July 1990 [SC21 N 4967] (CD text expected November 1990)
	PDAM 4	State Table, January 1990 [SC21 N 4058] [21]
	WDAM 5	Enhanced Functionality, July 1991 [SC21 N 6039] (PDAM expected in 1993)
DIS 9596–2	Common Management Information Protocol (CMIP) Specification, Part 2: PICS Proforma, July 1991 [SC21 N 6287] (CCITT X.712) (IS status expected June 1992)	
ISO 10040♦	Systems Management Overview, August 1991 [SC21 N 6353, September 1991] (CCITT X.701)	
ISO 10164-1♦	Systems Management - Part 1: Object Management Function, October 1991 [SC21 N 6355] (CCITT X.730)	
ISO 10164-2♦	Systems Management - Part 2: State Management Function, October 1991 [SC21 N 6356] (CCITT X.731)	
ISO 10164-3♦	Systems Management - Part 3: Relationship Management Function, October 1991 [SC21 N 6357] (CCITT X.732)	
ISO 10164-4♦	Systems Management - Part 4: Alarm Reporting Function, October 1991 [SC21 N 4858, September 1990] (CCITT X.733)	
ISO 10164-5♦	Systems Management - Part 5: Event Report Management Function, October 1991 [SC21 N 4860, September 1990] (CCITT X.734)	
ISO 10164-6♦	Systems Management - Part 6: Log Control Function, October 1991 [SC21 N 4862, September 1990] (Name changed from Management Service Control Function)	
ISO 10164-7♦	Systems Management - Part 7: Security Alarm Reporting Function, October 1991 [SC21 N 6367] (CCITT X.736)	
DIS 10164-8	Systems Management - Part 8: Security Audit Trail Function, July 1991 [SC21 N 6283] (CCITT X.740) (IS status expected in June 1992)	
CD 10164-9.2	Systems Management - Part 9: Objects and Attributes for Access Control, October 1991 [SC21 N 5764] (CCITT X.741) (second CD ballot failed October 1991; IS status expected December 1992)	
CD 10164-10.2	Systems Management - Part 10: Accounting Meter Function, July 1991 [SC21 N 5648] (CCITT X.742) (second CD ballot expected in 1991; DIS text expected in March 1992, IS in March 1993)	
CD 10164-11.2	Systems Management - Part 11: Workload Monitoring Function, October 1991 [SC21 N 6452] (CCITT X.739) (failed second CD ballot)	
DIS 10164-12	Systems Management - Part 12: Test Management Function, November 1991 [SC21 N 6558] (CCITT X.745) (IS text expected in December 1992)	

[20] PDAM: Proposed Draft Amendment to an ISO Standard (has the status of a CD).

[21] Work on a PDAM for State Table to ISO 9596-1 was cancelled in June 1991.

CD 10164-13.2	Systems Management - Part 13: Summarization Function, 12 November 1991 [SC21 N 6485] (CCITT X.738) (IS text expected December 1992)
CD 10164-14	Systems Management - Part cdt: Confidence and Diagnostic Test Classes, December 1990 [SC21 N 6485] (DIS expected in August 1992, IS in August 1993) (CCITT X.737)
WD 10164-X	Systems Management - Part X: Software Management Function, July 1991 [SC21 N 6040] (CD text expected June 1993, DIS in March 1994, IS in March 1995) (CCITT X.744) second WD in production Jaunary 1952
WD 10164-A	Systems Management - Part A: Time Management Function, July 1990 [SC21 N 4953] (CD text expected June 1993, DIS in March 1994, IS in March 1995) (CCITT X.743)
WD 10164-sm	Systems Management - Part sm: Software Management, June 1991 [SC21 N 6040] (CD expected in December 1992, DIS in August 1993, IS in August 1994)
WD 10164-rtm	Systems Management - Part rtm: Response Time Monitoring, August 1990 [SC21 N 4949; JTC1 N 963] (CD text expected December 1993, DIS in August 1994, IS in August 1995)
WD 10164-s	Systems Management - Part s: Scheduling Function, June 1991 [SC21 N 6021] (CD text expected June 1992, DIS in March 1993, IS in March 1994)
WD 10164-pm	Information Technology - Open Systems Interconnection - Systems Management - Part pm: Performance Management, July 1991 [SC21 N 6306]
ISO 10165-1♦	Structure of Management Information - Part 1: Management Information Model, November 1991 [SC21 N 6351] (CCITT X.720)
ISO 10165-2♦	Structure of Management Information - Part 2: Definition of Management Information, September 1991 [SC21 N 6363] (Incorporated Part 3) (CCITT X.721)
ISO 10165-4♦	Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects, November 1991 [SC21 N 6359] (CCITT X.710)
CD 10165-5♦	Structure of Management Information - Part 5: Generic Management Information, August 1991 [SC21 N 6360] (previously entitled Generic Managed Objects) Failed November 1991 ballot
CD 10165-6♦	Structure of Management Information - Part 6: Requirements and Guidelines for Management Information Conformance Statement (MICS) Proformas, July 1991 [SC21 N 6027] (DIS text expected in March 1992, IS in March 1993) Failed November 1991 ballot
WD 10165-7♦	Structure of Management Information - Part 7: Management Information Register and Registration Procedures (SC21 N 4945, July 1990) (CD expected in June 1992, DIS in December 1992, IS in December 1993)
WD 10165-x	Information Technology - Open Systems Interconnection - Managed Object Conformance Statement (MOCS) Proforma, 14 February 1991 [SC21 N 5686]
DIS 10733	Telecommunications and Information Exchange Between Systems - Elements of Management Information Related to OSI Network Layer Standards [SC21 N 5560, 3 January 1991; SC6 N 6413, 11 December 1990] (IS status expected June 1992)
WD xxxx(E)	Managed Object Conformance Statement (MOCS) Proforma [SC21 N 5686, February 1991]
WDTR xxxx	Systems Management Tutorial, July 1990, SC21/WG4 [SC21 N 4942] (new work item) (CCITT X.702)
WDTR xxxx, Annex A	Systems Management Tutorial - Annex A: Access Control, May 1990 [SC21 N 4970]
JTC1 N 1440	Use of Systems Management for Administration of the Directory, 23 August 1991
SC6 N 5447	Liaison Statement to SC21/WG4 on Lower Layer Management, October 1990

SC6 N 5784	General Principles for the Definition of Lower Layer Management, Second Draft, JTC1 SC6/WG2/WG4, April 1990
SC6 N 6413	Elements of Management Information Related to OSI Network Layer Standards, December 1990 (see CD 10733]
SC21 N 3307	WG4 Architecture Issues List
SC21 N 3311♦	Configuration Management Overview
SC21 N 3316	Access Control for OSI Management and The Directory
SC21 N 3390	NWI Proposal for an Addendum to CMIS/CMIP on Suppress Relay, July 1989
SC21 N 4058	State Tables for CMIP, January 1990
SC21 N 4077♦	Fault Management Working Document, SC21/WG4, December 1989
SC21 N 4085♦	Accounting Management Working Document, Third Version, SC21/WG4, November 1989
SC21 N 4091♦	OSI Security Management Working Document, November 1989
SC21 N 4906	Upper Layer Management - Call for Contributions, SC21/WG6, June 1990
SC21 N 4943	Extended Systems Management Architecture, July 1990 (planned to be an amendment to ISO 10040)
SC21 N 4944	Generic Managed Objects, July 1990
SC21 N 4945	Definition of a Management Information Register and Registration Procedures, July 1990 (see WD 10165-7)
SC21 N 4946	Requirements and Guidelines for Managed Object Conformance Statement (MOCS) Proformas, July 1990
SC21 N 4947	Formal Descriptions of CMIP, July 1990
SC21 N 4953	Time Management: Representation of Time, SC21/WG4, July 1990
SC21 N 4960	Generic Managed Objects, Working Draft, SC21/WG4, July 1990
SC21 N 4961	Request for Contributions to Progress Work on the Definition of State Tables for CMIP, May 1990
SC21 N 4968	Synchronization Across Multiple Managed Objects, SC21/WG4, July 1990
SC21 N 4969	Call for National Body Contributions on Time Management, SC21/WG4, May 1990
SC21 N 4973	The Use of System Title by OSI Management, SC21/WG4, July 1990
SC21 N 4974	Use of Global Naming for Identification of Managed Objects, SC21/WG4, July 1990
SC21 N 4975	A General Model for Relationship Management, SC21/WG4, May 1990
SC21 N 4977	Use of Action to Invoke State Changes, SC21/WG4, July 1990
SC21 N 4979	Request for National Body Comment on the Need for an Access Control Information Management Function, SC21/WG4, May 1990
SC21 N 4981♦	Performance Management Working Document, Sixth Working Draft, July 1990
SC21 N 4982	WG4 Systems Management Issues, SC21/WG4, July 1990
SC21 N 5079	Draft Answer to Q1/63.1 on Conformance to Objects in the Context of OSI Management, SC21/WG1, May 1990
SC21 N 5080	Call for Contributions on OSI Management Conformance Issues, SC21/WG1, July 1990
SC21 N 5228	Proposed Technical Corrigenda to ISO 9595 and ISO 9596
SC21 N 5351	Time Stamps, 24 September 1991
SC21 N 5543	Planning and Organization of SC21/WG4 Systems Management Activities, November 1990
SC21 N 5544	Call for Input on the Work Plan for SC21/WG4, November 1990
SC21 N 5545	Working Draft Input on Scheduling for Management Functions, OSI, 12-23 November 1990

SC21 N 5546	Agreement on Planning Future Releases of CMIS/P, OSI, November 1990
SC21 N 5557	Liaison Statement to ISO/IEC JTC1/SC21/WG1 on SC6 PICS Proforma Guidelines, SC6, January 1991
SC21 N 5548	Issues Concerning the Management Information Model and GDMO, OSI, 12-23 November 1990
SC21 N 5549	Preliminary Consideration of New Work Items Relating to SMI, OSI, 12-23 November 1990
SC21 N 5551	Work Plan for Managed Objects Standardization, OSI, November 1990
SC21 N 5560	Liaison Statement to WG4 Concerning SMI-related Issues, SC6, January 1991
SC21 N 5582	Corrections to the Joint Text of the Second Editions for CMIS and CMIP, 7 January 1991
SC21 N 5606	Working Draft for [Information Technology - Open Systems Interconnection - Structure of Management Information - Part X:] Generic Managed Objects [for CCITT Applications], March 1991
SC21 N 5686	Managed Object Conformance Statement (MOCS) Proforma, 14 February 1991
SC21 N 5687	Management Information Registration Procedure, ISO CCITT, February 1991
SC21 N 5756	The Proliferation of Managed Objects, UK, March 1991
SC21 N 5803	Extended Relationship Management, USA, March 1991
SC21 N 5815	A General Model for Managed Object Relationships, Canada, March 1991
SC21 N 5891	Contribution to the New Work Item: Management Information Register and Registration Procedures, Germany, 16 April 1991
SC21 N 6021	[Information Technology - Open Systems Interconnection - Systems Management - Part s:] Scheduling Function, 29 July 1991
SC21 N 6029	Proposal for the Establishment of a Managed Object Advisory Group, WG4, June 1991
SC21 N 6035	Enhanced Event Management and Log Control, WG4, July 1991 (new work item)
SC21 N 6036	Planning and Organization of SC21/WG4 Systems Management Activities, 20 June 1991
SC21 N 6037	Need for Security Services with OSI Management, SG4, July 1991
SC21 N 6039	Development of Enhanced Functionality for CMIS/P, WG4, July 1991 [CD expected in 1993, DIS in 1994, IS in 1995], JTC1 N 1438 (voting ends October 1991) (new work item)
SC21 N 6040	OSI Software Management - Working Draft, WG4, June 1991
SC21 N 6041	General Relationship Model--Working Draft, WG4, June 1991
SC21 N 6046	Response to Systems Management Tutorial NWI Proposal Ballot (contains initial May 1991 draft of the Systems Management Tutorial), WG4, June 1991
SC21 N 6047	First Working Draft on Management Domains, WG4, June 1991 (part of the Extended Systems Management Architecture)
SC21 N 6048	Working Document on Management Knowledge Management, WG4, June 1991 (part of the Extended Systems Management Architecture)
SC21 N 6049	Working Document on Synchronization, WG4, June 1991 (part of the Extended Systems Management Architecture)
SC21 N 6066	Liaison to SC6/WG4, SC21/WG6, SC21/WG4, and SC21/WG1 on Managed Object Structures, 24 July 1991
SC21 N 6194	Final Answer to Q1/63.1--Meaning of Conformance to Objects in the Context of OSI Management, WG1, May 1991
SC21 N 6196	PICS Issues (Part 7 to ISO/IEC 9646), WG1, July 1991

SC21 N 6306	[Information Technology - Open Systems Interconnection - Systems Management -] Performance Management Working Document - Seventh Draft, 29 July 1991
SC21 N 6307	[Information Technology - Open Systems Interconnection - Systems Management -] Confidence and Diagnostic Test Categories [for CCITT Applications], 29 July 1991
SC21 N 6469	Liaison Statement to SC21/WG4 - Generic Management Information, 22 October 1991
SC21 N 6470	Liaison Statement to CCITT SG XI/Q20 - Protocol Discriminator, 22 October 1991
SC21 N 6471	Liaison Statement to SC21/WG1 - PICS Proforma Guidelines for 22 October 1991
SC21 N 6485	CD 10164-13.2, Information Technology - OSI - Systems Management - Part 13: Summarization Function CD 10164-13 Editing Meeting, 23 October 1991
IST21 N 2734	Part 1: Specification of ACSE, Presentation and Session Protocols for the use by ROSE and CMISE; Part 2: Enhanced Management Communications; 15 April 1991
IST21 N 3037	EWOS/EG/NM/91/115: Management Information Catalogue (Sixth Draft), 11 September 1991
IST21 N 3058	Report of Joint IST/21 - UK SGVII Panel on OSI Management, October 1991

F. OSI REGISTRATION AUTHORITIES:

ISO 9834-1♦	Procedures for Specific OSI Registration Authorities - Part 1: General Procedures, March 1990 [SC21 N 4352]
ISO 9834-2♦	Procedures for Specific OSI Registration Authorities - Part 2: Registration Procedures for Document Types, November 1990 [SC21 N 5275] (approved June 1991; IS text expected in late 1991)
ISO 9834-3♦	Procedures for Specific OSI Registration Authorities - Part 3: Procedures for Specific Registration of Joint Object Identifier Component Values for Joint ISO-CCITT Use, September 1990 [SC21 N 4718]
ISO 9834-4♦	Procedures for Specific OSI Registration Authorities - Part 4: Register of VTE Profiles, 1 November 1991 [SC21 N 6541]
ISO 9834-5♦	Procedures for Specific OSI Registration Authorities - Part 5: Register of VT Control Objects, 1 November 1991 [SC21 N 6543]
DIS 9834-6	Procedures for Specific OSI Registration Authorities - Part 6: Registration Authority Procedures for Application Process Titles and Application Entity Titles, September 1990 [SC21 N 5?18] ((DIS ballot failed 25 April 1991))
WD 9834-B	Procedures for Specific OSI Registration Authorities - Part B: Registration of Abstract Syntaxes, 1990
WD 9834-C	Procedures for Specific OSI Registration Authorities - Part C: Registration of Transfer Syntaxes, 1990
WD 9834-D	Procedures for Specific OSI Registration Authorities - Part D: Registration of Application Contexts (work suspended by SC21, November 1989)
WD 9834-E	Procedures for Specific OSI Registration Authorities - Part E: Registration of System Titles, 1990 (will probably be incorporated in OSI management standards)
WD 9834-F	Procedures for Specific OSI Registration Authorities - Part F: Registration of Authentication Mechanisms (WITHDRAWN; cancelled by SC21, November 1989)
TR 9973	Registration of Graphical Items
WD xxxx	Registration of System Titles (DP expected November 1990)
SC21 N 5014	Liaison Statement to CCITT SG VII (Q.23) on Collaborative Work on OSI Registration, June 1990

SC21 N 5687 — Management Information Registration Procedure, Working Draft, February 1991

SC21 N 5758 — Discussion Paper on Conformance and Registration, BSI, March 1991

SC21 N 5888 — Liaison Statement to the Registration Authority for the Register of Object Identifier Components Allocated to Areas of Joint ISO-CCITT Work - Request for Updates to the Register, 16 April 1991

SC21 N 5891 — Contribution to the New Work Item: Management Information Register and Registration Procedures, Germany, 16 April 1991

SC21 N 6370 — Register of Object Identifier Components Allocated to Areas of Joint ISO/CCITT Work, 20 August 1991

G. OSI CONFORMANCE TESTING:

ISO 9646-1.2♦ — OSI Conformance Testing Methodology and Framework - Part 1: General Model, May 1991 [SC21 N 5865] (CCITT X.290)

- PDAM 1 — Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6173] (DIS text expected March 1992; IS in December 1992)
- PDAM 2 — Multi-Party Testing Methodology, June 1991 [SC21 N 6178] (DIS text expected March 1992; IS in December 1992)

ISO 9646-2.2♦ — OSI Conformance Testing Methodology and Framework - Part 2: Abstract Test Suite Specification, May 1991 [SC21 N 5867]

- Annex — Guidelines for PICS Proformas [SC6 N 6243]
- PDAM 1 — Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6174] (DIS text expected March 1992; IS in December 1992)
- PDAM 2 — Multi-Party Testing Methodology, June 1991 [SC21 N 6179] (DIS text expected March 1992; IS in December 1992)

ISO 9646-3♦ — OSI Conformance Testing Methodology and Framework - Part 3: Executable Test Derivation, July 1991

- PDAM 1 — TTCN Extensions, November 1991 [SC21 N 6666] (DAM expected June 1992; (AM June 1993)
- WDAM 2 — Addendum 2: Further TTCN Extensions, 26 November 1991 [SC21 N 6641]

ISO 9646-4♦ — OSI Conformance Testing Methodology and Framework - Part 4: Test Realization (Requirements for Implementors), May 1991 [SC21 N 5869]

- PDAM 1 — Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6175] (DIS text expected March 1992; IS in December 1992)
- PDAM 2 — Multi-Party Testing Methodology, June 1991 [SC21 N 6181] (DIS text expected March 1992; IS in December 1992)

ISO 9646-5♦ — OSI Conformance Testing Methodology and Framework - Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process (Test Execution), May 1991 [SC21 N 5871]

- PDAM 1 — Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6176] (DIS text expected March 1992; IS in December 1992)
- PDAM 2 — Multi-Party Testing Methodology, June 1991 [SC21 N 6182] (DIS text expected March 1992; IS in December 1992)

CD 9646-6 — OSI Conformance Testing Methodology and Framework - Part 6: Protocol Profile Test Specification, June 1991 [SC21 N 6177] (DIS text expected March 1992; IS in December 1992)

WD 9646-7	OSI Conformance Testing Methodology and Framework - Part 7: Requirements and Guidelines on Implementation Conformance Statement (ICS) and ICS Proformas, June 1991 (new work item)
CD 10641	Conformance Testing of Implementations of Graphics Standards, 1991
WD xxxx	Multi-Party Testing Methodology, July 1990, SC21/WG1 [SC21 N 5076] (CD text expected October 1990)
WDTR xxxx	Catalogue of PICS Proforma Notations, July 1990 (joint work of WG1 and CCITT SG VII)
SGFS N 214	Catalogue of PICS Proforma Notations, SC21, January 1991
SC21 N 3665	Specific Partial Abstract Test Suite (ATS) for Response Tests (CD text expected in October 1992; DIS in October 1993; IS in October 1994)
SC21 N 3666	Abstract Test Suite (ATS) for CS Test Method (WD text expected in June 1992; CD in October 1992; DIS in October 1993; IS in October 1994)
SC21 N 4215	Formal Methods in Conformance Testing (new work item, January 1990), CD expected June 1994
SC21 N 5075	Protocol Profile Testing Methodology, Second Working Draft, SC21/WG1, July 1990
SC21 N 5078	Catalogue of PICS Proforma Notations, SC21/WG1, July 1990
SC21 N 5108 ADD	Report of the Conformance Testing Meeting, held in Seoul, 22-20 May 1990, December 1990
SC21 N 5112	Discussion Paper on Formal Methods in Conformance Testing, SC21/WG1, July 1990
SC21 N 5117	Multiparty Testing for MHS, SC21/WG1, July 1990
SC21 N 5158	Conformance Test Suite for the VT Protocol, July 1990 [JTC1 N 770] (new work item; CD text expected November 1990)
SC21 N 5557	Liaison Statement to WG1 on SC6 PICS Proforma Guidelines, January 1991
SC21 N 5657	Liaison Statements from CCITT SG VII to SC21/WG1 on Various Topics (conformance testing, OSI Reference Model regarding ISDN, OSI naming and addressing), February 1991
SC21 N 5707	Position Statement on PICS Notations, SGFS, March 1991
SC21 N 5758	Discussion Paper on Conformance and Registration, UK, March 1991
SC21 N 5853	Call for Contributions on SC21 N 5077 Clause 3.1, Formalization of User Defined Operation Definition, April 1991
SC21 N 5856	Discussion Paper on Multi-Protocol Testing, SC21/WG 1 and CCITT SG VII Collaborative Meeting on Conformance, Phoenix, 7-14 February 1991, 5 April 1991
SC21 N 5857	Proposed liaison to SGFS on Proforma Conformance Issues, April 1991
SC21 N 5858	Call for Contributions on Multi-User Test Methods, April 1991
SC21 N 5864	Disposition of Comments on DIS 9646-1, April 1991
SC21 N 5866	Disposition of Comments on DIS 9646-2, April 1991
SC21 N 5868	Disposition of Comments on DIS 9646-4, April 1991
SC21 N 5870	Disposition of Comments on DIS 9646-5, April 1991
SC21 N 5903	Presentation Connection-Oriented Abstract Test Suite (ATS), Common Partial ATS (CD expected in June 1992; DIS in June 1993; IS in June 1994)
SC21 N 5928	Disposition of Comments on DIS 10729-1, April 1991
SC21 N 6160	Catalogue of PICS Proforma Notations, WG1, July 1991
SC21 N 6201	Working Draft on Formal Methods in Conformance Testing, WG1, July 1991
SC21 N 6398	Request for SGFS Member Comment on Standardization of Profile Test Specifications, 10 September 1991

SC21 N 6470	Liaison Contribution to CCITT SG XI/Q20 - Protocol Discriminator, 22 October 1991
SC21 N 6471	Liaison Statement to SC21/WG1 - PICS Proforma Guidelines for SC6, 22 October 1991
SC21 N 7016	Presentation Connection-Oriented Abstract Test Suite (ATS), Specific Partial ATS
SC21 N 7018	Common Partial Embedded ATS (CD text expected June 1992)
CCITT X.290	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications (see ISO 9646-1 and ISO 9646-2)
IST21 N 2531	Discussion Paper on the Nature of Protocol Profiles, UK, February 1991
IST21 N 2589	Minutes of the 20th Meeting of EWOS EGLL from October 8 to October 11, 1990, in Brussels, February 1991
IST21 N 2758	Liaison Statement to ISO/IEC JTC1 SGFS on the Relationship of ISPs to Registration Authorities, 12 April 1991
IST21 N 2772	Project Team Proposal on Production of Standardized Conformance Test Specifications for FTAM, 30 April 1991
IST21 N 2981	Report of the SC21 Upper Layers Conformance Testing (ULCT) Meeting, May 1991

H. TAXONOMY AND PROFILES:

STANAG 4406♦	NATO Standard Profile on Military Message Handling System (MMHS), Draft, October 1991
STANAG xxxx♦	NATO Standard Profile on R.131(M), Draft, October 1991
STANAG xxxx♦	NATO Standard Profile on TC 111(M), Draft, Version 1.3, October 1991
STANAG xxxx♦	NATO Standard Profile on TA 51(M), Draft, Version 2.0, October 1991
TR 10000-1♦	International Standardized Profiles (ISPs) - Part 1: Taxonomy Framework, July 1990 [JTC1 SGFS, SGFS N 184]
TR 10000-2♦	International Standardized Profiles (ISPs) - Part 2: Taxonomy of Profiles, July 1990 [JTC1 SGFS,SGFS N 185]
DTR 10000-2.2(E)	Framework of International Standardized Profiles (ISPs) - Part 2: Taxonomy of Profiles, June 1991 [SGFS N 384]
ISP 10607-1	ISPs - AFT nn - File Transfer, Access, and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM, April 1990 [SGFS N 131] (submitted by SPAG)
ISP 10607-2	ISPs - AFT nn - File Transfer, Access, and Management - Part 2: Definition of Document Types, Constraint Sets and Syntaxes, 17 January 1991 [SGFS N 285] (submitted by SPAG)
	AD 1 Additional Definitions, 27 May 1991 (SGFS N 363)
ISP 10607-3	ISPs - AFT nn - File Transfer, Access, and Management - Part 3: AFT 11 - Simple File Transfer Service (Unstructured), 17 January 1991 [SGFS N 286] (submitted by SPAG)
ISP 10607-4	ISPs - AFT nn - File Transfer, Access, and Management - Part 4: AFT 12 - Positional File Transfer Service, July 1990
	AD 1 Additional Definitions, 17 July 1990 (SGFS N 245)
ISP 10607-5	ISPs - AFT nn - File Transfer, Access, and Management - Part 5: AFT 22 - Positional File Access Service, July 1990
ISP 10607-6	ISPs - AFT nn - File Transfer, Access, and Management - Part 6: AFT 12 - File Management Service, July 1990

pDISP[22] 10608-1	ISP TA - Connection-Mode Transport Service over Connectionless Network Service, Part 1: General Overview and Subnetwork-Independent Requirements
pDISP 10608-2	Part 2:TA51 Profile Including Subnetwork-Dependent Requirements for CSMA/CD LANs
pDISP 10608-5	Part 5:TA1111/TA1121 Profiles Including Subnetwork-Dependent Requirements for X.25 Packet Switched Data Networks Using Switched Virtual Circuits
DISP 10609-1	ISP Profiles TB, TC, TD, and TE - Connection-Mode Transport Service over Connection-Mode Network Service, Part 1: Subnetwork-type Independent Requirements for Group TB
DISP 10609-2	Part 2: Subnetwork-type Independent Requirements for Group TC
DISP 10609-3	Part 3: Subnetwork-type Independent Requirements for Group TD
DISP 10609-4	Part 4: Subnetwork-type Independent Requirements for Group TE
DISP 10609-5	Part 5: Definition of Profile TB 1111/TB 1121
DISP 10609-6	Part 6: Definition of Profile TC 1111/TC 1121
DISP 10609-7	Part 7: Definition of Profile TD 1111/TD 1121
DISP 10609-8	Part 8: Definition of Profile TE 1111/TE 1121
DISP 10609-9	Part 9: Subnetwork-type Dependent Requirements for Network Layer, Data Link Layer, and Physical Layer Concerning Permanent Access to a Packet Switched Data Network Using Virtual Call
pDISP 11183-1	Information Technology - International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by ROSE and CMISE, Second Version, 27 April 1991 [SGFS N 357 and 358, 24 May 1991]
pDISP 11183-2	Information Technology - International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 2: Enhanced Management Communications, Fourth Version, 27 April 1991 [SGFS N 359, 24 May 1991]
pDISP 11183-3	Information Technology - International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 3: AOM11 - Basic Management Communications, Draft pDISP text, First Version, 23 May 1991 [IST/21:2808]
SGFS N 100	Information Technology - Framework and Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein, Revision 3, 10 September 1991
SGFS N 201	ISPs - Taxonomy Update, ISP Approval, and Maintenance Process, May 1990 (standing SGFS document)
SGFS N 219	An Example of T-Profiles Multi-Part ISP Structure, June 1990
SGFS N 224	Documents Relating to Applications Portability Profile Work from JTC1/TSG-1, 11 June 1990
SGFS N 226	Liaison Statement to JTC1 on Multi-Part ISDN ISP Structures, June 1990
SGFS N 228	Liaison Statement to JTC1 SGFS on the Inclusion of a Profile for MMS in the Taxonomy of Profiles TR 100000-2, June 1990
SGFS N 282	Resolutions of the 4th RWS-CC Meeting, 18-19 October 1990, January 1991
SGFS N 373	Output from the 5th Regional Workshop Coordinating Committee (RWS-CC), March 18-19, 1991, 13 June 1991
SGFS N 401	Information Processing Systems, International Standardized Profiles, Taxonomy Update, ISP Approval and Maintenance Process, 23 September 1991
SC21 N 3674	ISPs - Directory of ISPs and Profiles Contained Therein, June 1989
SC21 N 3675	ISPs - ISP Approval and Maintenance Process, June 1989

[22] pDISP: Proposed Draft International Standardization Profile.

SC21 N 3678	ISPs - Proposed New AMH Taxonomy, June 1989
SC21 N 4716	Initial List of Planned pDISPs, April 1990
SC21 N 6398	Request for SGFS Member Comment on Standardization of Profile Test Specifications, 10 September 1991
EWOS/EGTP/91/12	Draft Taxonomy for Distributed Transaction Processing, EWOS, February 1991
IST21 N 2604	Relaying the MAC Service using Transparent Bridging (CSMA/CD-CSMA/CD), 26 February 1991
IST21 N 2605	Connection-mode Transport Service over Connectionless-mode Network Service, 26 February 1991
IST21 N 2659	EWOS Releases More IT Functional Standard Proposals for Open Systems, 12 March 1991
IST21 N 2754	Extension of M-IT-01 and M-IT-02 for the Open System Environment, European Workshop for Open Systems, EWOSTA9181, April 1991
IST21 N 2755	Extension of TR 10000 for the Open System Environment, EWOS Contribution to ISO/IEC JTC1 SGFS, April 1991
IST21 N 2756	Extension of TR 10000-2 Taxonomy for the Directory (ADI and FDI), EWOS Contribution to ISO/IEC JTC1 SGFS, 17 April 1991
IST21 N 2758	Liaison Statement to ISO/IEC JTC1 SGFS on the Relationship of ISPs to Registration Authorities, 12 April 1991
IST21 N 2759	EWOS/TLG Report to TA 13, May 14/15, 1991
IST21 N 2760	Liaison Statement to ISO/IEC JTC1 SGFS on the Virtual Terminal Taxonomy in TR 10000-2, 12 April 1991
IST21 N 2765	EWOS Proposed Taxonomy for OSI-TP, May 1991
IST21 N 2766	Resolutions RWS-CC, March 1991
IST21 N 2767	Report to EWOS/TA (14/15 May, 1991) From EGTP Chair, May 1991
IST21 N 2773	The Future of European Standardization, 10 May 1991
IST21 N 2794	1st Workshop on Open Information Interchange, May 1991
IST21 N 2795	EWOS Work Programme, May 1991
IST21 N 2796	EWOS ISP Activities, 21 May 1991
IST21 N 2799	The COSINE Concise Information Service Project, May 1991
IST21 N 2880	Interim Report on the Feasibility of Profiling Database Enquiry, EWOSPT N 014, June 1991
IST21 N 2854	Memorandum M-IT-02 on Taxonomy of Profiles and Directory of Functional Standards, May 1991
IST21 N 2889	Documents Relating to Functional Standards, 17 July 1991
IST21 N 2938	Identification of ENV/ENs with Equivalent ISO/IEC ISPs, 13 August 1991
IST21 N 2948	EWOS/EGTP #4 Main Results, Brussels, 25-28 June 1991
IST21 N 2949	EWOS Active Work Items - Status, 6 August 1991
IST21 N 2950	EWOS Internal Schedule of Deliverables, 6 August 1991
IST21 N 2951	EWOS Active Work Items - Information, 6 August 1991
IST21 N 2952	EWOS Completed Work Items, 6 August 1991
IST21 N 2956	EWOS Documents: Their Status and Processing in European and International Contexts, 7 August 1991
IST21 N 3045	Resolutions 7th ISO/IEC JTC1/SGFS meeting, June 18-21, 1991, Berlin, 15 August 1991
IST21 N 3044	An Informal Quality Service for Functional Standards, 30 August 1991
IST21 N 3045	Resolutions 7th ISO/IEC JTC1/SGFS meeting, June 18-21, 1991, Berlin, 15 August 1991
IST21 N 2531	Discussion Paper on the Nature of Protocol Profiles, BSI, February 1991

ENV[23] 41 101♦	LANs: Provision of the OSI Connection-Mode Transport Service (COTS) Service Using the Connectionless-Mode Network Service (CLNS) on a CSMA/CD Single LAN, June 1986
ENV 41 102♦	LANs: Provision of the OSI COTS and the CLNS on a CSMA/CD Single or Multiple LAN Configuration, June 1986 (ISO Profile TA51)
ENV 41 103♦	LANs: Provision of the OSI COTS and the Connection-Mode Network Service (CONS) in an End System on a CSMA/CD LAN, December 1987
ENV 41 104	Packet Switched Data Networks: Permanent Access, August 1987 (ISO Profile Tx11y)
ENV 41 105♦	Packet Switched Data Networks: Switched Access, June 1988
ENV 41 106♦	Digital Data Circuit (CSDN) - Provision of the OSI COTS in the T.70 Case for Telematic End Systems, June 1988
ENV 41 107♦	Digital Data Circuit (CSDN) - Provision of the OSI COTS and the OSI CONS, June 1988
ENV 41 108♦	LANs: Provision of the OSI COTS and CONS in an End System on a Token Ring LAN, May 1988
ENV 41 109♦	LANs: Provision of the OSI COTS Using CLNS on a Token Ring Single LAN, February 1988
ENV 41 110♦	LANs: Provision of the OSI COTS Using CLNS in an End System on a Token Ring LAN in a Single or Multiple LAN Configuration, February 1988 (ISO Profile TA53)
ENV 41 201	Private Message Handling System - User Agent and Message Transfer Agent; Private Management Domain to Private Management Domain, June 1986
ENV 41 202	Message Handling Systems; User Agent and Message Transfer Agent: Access to an Administration Management Domain (ADMD), August 1987
ENV 41 203	Exchange of Telex Documents Between Two End Systems, Which May Be Teletex Terminals, June 1988
ENV 41 204♦	FTAM: Simple File Transfer, June 1988 (ISO Profile AFT11)
ENV 41 205♦	FTAM: File Management, June 1987 (ISO Profile AFT3)
ENV 41 206♦	FTAM: Positional File Transfer (ISO Profile AFT12)
ENV 41 207♦	FTAM: Positional File Access (ISO Profile AFT22)
ENV 41 208♦	VT: Basic Class - S Mode - Forms (ISO Profile AVT22)
ENV 41 209♦	VT: Control Objects
ENV 41 509♦	ODA: Basic Character Content (ISO Profile FOD11)
ENV 41 510♦	ODA: Enhanced Mixed Mode (ISO Profile FOD26)
ENV 41 511♦	ODA: Simple Messaging Profile
ENV 41 901	X.29-Mode Procedures Between a Packet Mode DTE or a PAD and a PAD via a Public or Private X.25 Packet Switched Network or ISO 8208 Packet Level Entity and ISO 7776 Link Level Entity, June 1987
M-IT-02	Directory of Functional Standards (For Interworking in an OSI Environment) Adopted by the CEN/CENELEC/CEPT/ITSTC, March 1987

[23] ENV indicates an interim standard approved by the Join European Standards Institution (CEN/CENELEC) and the European Workshop for Open Systems (EWOS).

II. LAYER 1: PHYSICAL LAYER[24]

A. General
B. Mechanical
C. Functional
D. Procedural
E. Local Area Networks

A. GENERAL:

STANAG 4251♦	NATO Reference Model for OSI - Layer 1 (Physical Layer) Service Definition, Draft, October 1991
STANAG 4261♦	NATO Reference Model for OSI - Layer 1 (Physical Layer) Protocol Specification, Draft, October 1991
ISO 9160	Physical Layer Interoperability Requirements
DIS 9316	Small Computer System Interface (SCSI)
DIS 9318-1	Intelligent Peripheral Interface - Part 1: Physical Level, August 1987
ISO 9318-2	Intelligent Peripheral Interface - Part 2: Device Specific Command Set for Magnetic Disk Drives, 1990
ISO 9318-3	Intelligent Peripheral Interface - Part 3: Device Generic Command Set for Magnetic and Optical Disk Drives, 1990
ISO 9318-4	Intelligent Peripheral Interface - Part 4: Device Generic Command Set for Magnetic Tape Drives, 1990
DIS 9324	Information Processing - Storage Module Interfaces, September 1988
ISO 10022♦	Physical Service Definition, August 1990 (CCITT X.211)
DIS 10222	Enhanced Small Device Interface, 1991
CCITT X.211	Physical Service Definition for OSI for CCITT Applications (see DIS 10022), 1988 Blue Books

B. MECHANICAL:

ISO 2110.3♦	25-Pin DTE/DCE Interface Connector and Pin Assignments (Revision of ISO 2110)
	DAM 1 Interface Connector and Contact Number Assignments for a DTE/DCE for Data Signalling Rates Above 20 kbit/s
ISO 2593.3♦	34-Pin DTE/DCE Interface Connector and Pin Assignments (third edition awaiting publication)
ISO 4902.3♦	37-Pin DTE/DCE Interface Connector & Pin Assignments, Third Edition, 1989
ISO 4903.3♦	15-Pin DTE/DCE Interface Connector and Pin Assignments, Third Edition, 1989
TR 7477♦	Arrangements for DTE/DTE Physical Connection Using V.24 and X.24 Interchange Circuits, 15 September 1985
ISO 8481♦	DTE/DTE Physical Connection Using X.24 Interchange Circuits with DTE-Provided Timing

[24] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy.*

ISO 8877♦	Interface Connector and Contact Assignments for ISDN Basic Access Interface Located at Reference Points S and T
	DAM 1♦ Standard ISDN Basic Access TE Connecting Cord
ISO 10173	ISDN Primary Access Connector at Reference Points S and T, 1991
CCITT I.340	ISDN Connection Types

C. ELECTRICAL:

ISO 8482♦	Twisted Pair Multipoint Interconnections
ISO 9549♦	Galvanic Isolation of Balanced Interchange Circuits, October 1990
CCITT V.5	Data Signalling Rates for Synchronous Data Transmission in the General Switched Telephone Network
CCITT V.6	Data Signalling Rates for Synchronous Data Transmission on Leased Telephone-Type Circuits
CCITT V.28♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits
CCITT V.31♦	Electrical Characteristics for Single-Current Interchange Circuits Controlled by Contact Closure
CCITT V.31 bis♦	Electrical Characteristics for Single-Current Interchange Circuits Using Opto Couplers
CCITT V.35♦	Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits
CCITT V.36♦	Modems for Synchronous Data Transmission Using 60-108 kHz Group Band Circuits

D. FUNCTIONAL:

DIS 7480.2♦	Start-Stop Transmission Signal Quality at DTE/DCE Interfaces, Draft Second Edition
ISO 9543♦	Synchronous Transmission Signal Quality at DTE/DCE Interfaces
CCITT I.411	ISDN User-Network Interfaces - Reference Configuration
CCITT I.412	ISDN User-Network Interfaces - Interface Structures and Access Capabilities
CCITT X.1	International User Classes of Service in Public Data Networks and Integrated Services Digital Networks (ISDNs)
CCITT X.4	General Structure of Signals of International Alphabet No. 5 Code for Data Transmission Over Public Data Networks
CCITT X.10	Categories of Access for DTE to Public Data Transmission Services Provided by PDNs and/or ISDNs through Terminal Adaptors
CCITT X.24♦	List of Definitions for Interchange Circuits Between DTE and DCE on Public Data Networks

E. PROCEDURAL:

ISO 8480♦	DTE/DCE Back-Up Control Operation Using the 25-Pole Connector
ISO 9067♦	Automatic Fault Isolation Procedures Using Test Loops
CCITT I.420	Basic User-Network Interface (ISDN)
CCITT I.421	Primary Rate User-Network Interface (ISDN)
CCITT I.430♦	Basic User-Network Interface - Layer 1 Specification (ISDN)
CCITT I.431♦	Primary Rate User-Network Interface - Layer 1 Specification (ISDN)
CCITT I.460♦	Multiplexing, Rate Adaptation and Support of Existing Interfaces (ISDN)
CCITT I.461♦	Support of X.21 and X.21 bis Based DTEs by an ISDN (X.30)
CCITT I.462♦	Support of Packet Mode Terminal Equipment by an ISDN (X.31)
CCITT I.463♦	Support of DTEs with V-Series Type Interfaces by an ISDN

CCITT I.464♦	Multiplexing Rate Adaptation and Support of Existing Interfaces for Restricted 64 kbit/s Transfer Capability
CCITT V.10/X.26♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communication
CCITT V.11/X.27♦	Electrical Characteristics for Balanced Double-Current Interchange Circuits for General Use With Integrated Circuit Equipment in the Field of Data Communications
CCITT V.20♦	Telex and Gentex Signalling on Radio Channels (Synchronous 7-Unit Systems Affording Error Correction by Automatic Repetition)
CCITT V.24♦	List of Definitions for Interchange Circuits Between DTE and DCE
CCITT V.25	Automatic Answering Equipment and/or Parallel Automatic Calling Equipment on the General Switched Telephone Network Including Procedures for Disabling of Echo Control Devices for Both Manually and Automatically Established Calls
CCITT V.28♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits
CCITT V.31♦	Electrical Characteristics for Single-Current Interchange Circuits Controlled by Contact Closure
CCITT V.31 bis♦	Electrical Characteristics for Single-Current Interchange Circuits Using Opto Couplers
CCITT V.35♦	Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits, 1988
CCITT V.36♦	Modems for Synchronous Data Transmission Using 60-108 kHz Group Band Circuits, 1988
CCITT V.37♦	Synchronous Data Transmission at a Data Signalling Rate Higher than 72 kbit/s Using 60-108 kHz Group Band Circuits
CCITT V.54	Loop Test Devices for Modems
CCITT X.20♦	Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks
CCITT X.20 bis	Use on Public Data Networks of DTE Which Is Designed for Interfacing to Asynchronous Duplex V-Series Modems
CCITT X.21♦	Interface Between DTE and DCE for Synchronous Operation on Public Data Networks
CCITT X.21 bis♦	Use on Public Data Networks of DTE Which Is Designed for Interfacing to Synchronous V-Series Modems
CCITT X.22♦	Multiplex DTE/DCE Interface for User Classes 3-6
CCITT X.31♦	Support of Packet Mode Terminal Equipment by an ISDN
CCITT X.32♦	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Accessing a Packet Switched PDN Through a Public Switched Telephone Network or a Circuit Switched PDN
CCITT X.150	Principles of Maintenance Testing for Public Data Networks Using DTR and DCE Test Loops

F. LOCAL AREA NETWORKS (LANs):

ISO 8802-1♦	LANs - Part 1: General Introduction
DIS 8802-1.2♦	LANs - Part 1: General Introduction with System Load Protocol
ISO 8802-2.2♦	LANs - Part 2: Logical Link Control, July 1990
DAM 1♦	Flow Control Techniques for Bridged LANs
DAM 2♦	Type 3 Operation - Acknowledge Connectionless Service
PDAM 3	PICS Proforma
DAM 4	Editorial Changes and Technical Corrections, June 1989

ISO 8802-3♦	LANs - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Access Method and Physical Layer Specifications
DAM 1♦	Physical Signalling, Medium Attachment, and Baseband Medium Specifications for Type 1BASE5
DAM 2♦	Repeater Set and Repeater Unit Specification for Use with 10BASE5 and 10 BASE2 Networks
DAM 3♦	Broadband Medium Attachment Unit and Broadband Medium Specifications, Type 10BROAD36
DAM 4♦	CSMA/CD, STARLAN, 1BASE5
DAM 5♦	Medium Attachment Baseband Medium Specification for a Vendor-Independent Fibre Optic Inter Repeater Link (FOIRL)
DAM 6	Summary of IEEE 802.3 First Maintenance Ballot
PDAM 7	LAN Layer Management
PDAM 9	Physical Medium, Medium Attachment, and Baseband Medium Specifications, Type 10baseT (new work item)
ISO 8802-4.2♦	LANs - Part 4: Token-Passing Bus Access Method and Physical Layer Specifications
ISO 8802-5♦	LANs - Part 5: Token Ring Access Method and Physical Layer Specifications, February 1987 (second DIS ballot on consolidated document--Revised Edition--containing Part 5 and its first 3 addenda closed 1 September 1990)
PDAM 1	4 and 16 Mbit/s Specification
PDAM 2	MAC Sublayer Enhancement
PDAM 3	Management Entity Specification
DAM 4	Source Routing MAC Bridge
DAM 5	PICS Proforma
DIS 8802-5.2♦	LANs - Part 5: Token Ring Access Method and Physical Layer Specification, Revised Edition (second DIS ballot on consolidated document containing Part 5 and its first 3 addenda closed 1 September 1990)
DIS 8802-6♦	LANs - Part 6: Distributed Queue Dual Bus (DQDB) Media Access Control (MAC)
ISO 8802-7♦	LANs - Part 7: Slotted Ring Access Method and Physical Layer Specification
DIS 8802-9♦	LANs - Part 9: Integrated Voice and Data (IVD) LAN
ISO 9314-1♦	Fibre Distributed Data Interface (FDDI) - Part 1: Physical Layer Protocol (PHY)
ISO 9314-2♦	FDDI - Part 2: Media Access Control (MAC)
ISO 9314-3♦	FDDI - Part 3: Physical Layer Medium Dependent (PMD), August 1990
CD 9314-4♦	FDDI-Part 4: Single-Mode Fiber/Physical Layer Medium Dependent
CD 9314-5♦	FDDI-Part 5: Hybrid Ring Control (FDDI-II), May 1990
DP 9314-6♦	FDDI-Part 6: Station Management (SMT) Standard
TR 9578	Communication Interface Connectors Used in LANs
DIS 10038♦	MAC Sublayer Interconnection (MAC Bridging)
PDAM 1	Specification of Management Information for CMIP
PDAM 2	Source Routing Supplement
ISO 10039♦	MAC Service Definition, October 1990
PDTR 10178	Structure and Coding of Link Service Access Point Addresses in LANs

III. LAYER 2: DATA LINK LAYER[25]

A. General
B. Character-Oriented Service (Basic Mode)
C. Bit-Oriented Service (HDLC Procedures)
D. Integrated Services Digital Network (ISDN)
E. Error Correction and Conformance Test Suite

A. GENERAL:

STANAG 4252♦	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Service Definition, Draft, 5 December 1991
STANAG 4262♦	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Protocol Specification, Draft, 5 December 1991
ISO 8886.3[26]♦	Data Link Service Definition for OSI
TR 10171♦	List of Standard Data Link Layer Protocols that Utilize HDLC Classes of Procedures (awaiting publication)
	PDAM 1 Registration of XID Format Identifiers and Private Parameter Set Identifiers
SC21 N 6346	Liaison Statement to JTC1/SC21 on Data Link Layer Security, 16 August 1991
CCITT X.212	Data Link Service Definition for OSI for CCITT Applications (see ISO 8886), 1988 Blue Books

B. CHARACTER-ORIENTED SERVICE (BASIC MODE):

ISO 1155	Use of Longitudinal Parity to Detect Errors in Information Messages
ISO 1177	Character Structure for Start/Stop and Synchronous Character Oriented Transmission
ISO 1745	Basic Mode Control Procedures for Data Communication Systems
ISO 2111	Basic Mode Control Procedures - Code Independent Information Transfer
ISO 2628	Basic Mode Control Procedures - Complements
ISO 2629	Basic Mode Control Procedures - Conversational Information Message Transfer

C. BIT-ORIENTED SERVICE (HIGH-LEVEL DATA LINK CONTROL PROCEDURES [HDLC]):

ISO 3309♦	HDLC - Frame Structure, Third Edition (second DIS ballot for a draft fourth edition closed 26 October 1990)
	AD 1♦ Start/Stop Transmission, March 1990
	DAM 2 Extended Transparency Options for Start/Stop Transmission
	PDAM 3 Seven-bit Transparency Options for Start/Stop Transmission
ISO 4335♦	HDLC - Elements of Procedures, Third Edition (second DIS ballot for a draft fourth edition closed 26 October 1990)
	AD 1♦ Asynchronous (Start/Stop) Transmission Operation

---

25 The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

26 For ISO standards, the decimal indicates the version number; thus, DIS 8886.3 is Version 3 (no decimal indicates Version 1).

	AD 2♦	Enhancement of the XID Function Utility
	AD 3♦	Start/Stop Transmission, March 1990
	DAM 4♦	Flow Control Unnumbered Information (FUI)
	PDAD 5	Multi-Selective Reject
ISO 7478♦	Multilink Procedures	
	Cor 1	Technical Corrigendum 1, 1 March 1989
ISO 7776♦	HDLC - Description of the X.25 LAPB-Compatible DTE Data Link Procedures	
	Cor 1	Technical Corrigendum 1, 1 April 1989
	Cor 2	Technical Corrigendum 2, 1 September 1989
	DAM 1	PICS Proforma
ISO 7809♦	HDLC - Consolidation of Classes of Procedures, February 1984 (second DIS ballot for a Revised Edition closed 26 October 1990)	
	AD 1♦	UI Command/Response
	AD 2♦	Descriptions of Optional Functions
	AD 3♦	Stop/Start Transmission, March 1990
	PDAD 4♦	List of Standard Data Link Layer Protocols that Utilize HDLC Classes of Procedures [see DTR 10171]
	DAM 5	Connectionless Class of Procedure
	DAM 6	Extended Transparency Option
	AM 7	Multi-Selective Reject, 1991
	PDAM 9	Seven-bit Transparency Option for Start/Stop Transmission
ISO 8471♦	HDLC Balanced Classes of Procedures - Data Link Layer Address Resolution/ Negotiation in Switched Environments	
ISO 8885♦	HDLC - General Purpose XID Frame Information Field Content and Format	
	AD 1♦	Additional Operational Parameters for the Parameter Negotiation Data Link Layer Subfield and Definition of a Multilink Parameter Negotiation Data Link Layer Subfield
	AD 2♦	Stop/Start Transmission, March 1990
	DAM 3♦	Definition of a Private Parameter Negotiation Data Link Layer Subfield
	DAM 4	Extended Transparency Option
	DAM 5	Multi-Selective Reject
	PDAM 6	Seven-bit Transparency Option for Start/Stop Transmission
	PDAM 7	Frame Check Sequence Negotiation Using the Parameter Negotiation Subfield
DIS 9234	Industrial Asynchronous Data Link for Two-Way Simultaneous or Two-Way Alternate Mode, 1989	
CCITT T.71♦	LAPB Extended for Half-Duplex Physical Level Facility	

D. INTEGRATED SERVICES DIGITAL NETWORK (ISDN):

CCITT I.440♦	ISDN User-Network Interface Data Link Layer - General Aspects
CCITT I.441♦	ISDN User-Network Interface Data Link Layer - Specification

E. ERROR CORRECTION AND CONFORMANCE TEST SUITE:

CCITT X.141	General Principles for the Detection and Correction of Errors in Public Data Networks
DIS 8882-2♦	Data Link Layer Conformance Test Suite
DTR 10174	Logical Link Control (Type 2 Operation) Test Purposes

IV. LAYER 3: NETWORK LAYER[27]

A. General
B. Packet-Switched Service
C. Connectionless Service
D. Integrated Services Digital Network (ISDN)
E. Routing and Relay
F. Automatic Calling/Answering Equipment
G. Circuit Switched Service
H. Local Area Networks (LANs)

A. GENERAL:

STANAG 4253♦	NATO Reference Model for OSI - Layer 3 (Network Layer) Service Definition, Draft, November 1991
STANAG 4263♦	NATO Reference Model for OSI - Layer 3 (Network Layer) Protocol Specification, Draft, November 1991
ISO 8348♦	Network Service Definition
	AD 1♦ Connectionless-Mode Transmission
	AD 2♦ Network Layer Addressing
	AD 3♦ Additional Features of the Network Service
	PDAM 4 Removal of the Preferred Decimal Encoding of the NSAP Address
ISO 8648♦	Internal Organization of the Network Layer
	Cor.1 Technical Corrigendum 1 (awaiting publication)
ISO 8880-1♦	Protocol Combination to Provide and Support the OSI Network Service - Part 1: General Principles, 1990
ISO 8880-2♦	Protocol Combination to Provide and Support the OSI Network Service - Part 2: Provision and Support of the Connection-Mode Network Service, 1990
	DAM 1 Addition of the ISDN Environment
	PDAM 2 Addition of the PSTN and CSDN Environments
ISO 8880-3♦	Protocol Combination to Provide and Support the OSI Network Service - Part 3: Provision and Support of the Connectionless-Mode Network Service, 1990
WD 8880-4♦	Protocol Combination to Provide and Support the OSI Network Service - Part 4: Interconnection of OSI Environments
TR 9577♦	Protocol Identification in the OSI Network Layer, October 1990
TR 10172	Network/Transport Protocol Interworking Specification, October 1990
DIS 10177	Intermediate-System Support of the OSI Connection-Mode Network Service Using ISO 8208 in Accordance with ISO 10028, October 1989 (ballot closed 23 February 1991)
CD 10733	Specification of the Elements of Management Information Related to OSI Network Layer Standards [SC 21 N 5560, SC 6 6413] January 1991
CD 11577	Network Layer Security Protocol, JTC1/SC6, July 1991 (balloting ends April 1992)

[27] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

CCITT T.70♦	Network-Independent Basic Transport Service for the Telematic Services
CCITT X.213	Network Service Definition for OSI for CCITT Applications

B. PACKET-SWITCHED SERVICE:

ISO 8208♦	X.25 Packet Level Protocol (PLP) for DTE (second edition published March 1990)	
	AM[28] 1.2♦	Alternative Logical Channel Number Allocation, September 1990
	PDAD 2♦	Extensions for Private Switched Use (WITHDRAWN, 1989)
	AM 3♦	Static Conformance Requirements, October 1990
ISO 8878♦	Use of X.25 to Provide the OSI Connection-Mode Network Service	
	Cor 1	Technical Corrigendum 1, published 1 March 1990
	Cor 2	Technical Corrigendum 2, published 15 June 1990
	Cor 3	Technical Corrigendum 3, awaiting publication
	AD 1	Protection and Priority, June 1990
	AD 2	Use of an X.25 PVC to Provide the OSI CONS, June 1990
	DAM 3	Conformance
	PDAM 4	PICS Proforma
ISO 8881.3♦	Use of the X.25 PLP in LANs	
ISO 8882-1♦	X.25-DTE Conformance Testing - Part 1: General Principles	
DIS 8882-1.2	X.25-DTE Conformance Testing - Part 1: General Principles, Revised Edition (awaiting second DIS ballot)	
DIS 8882-2♦	X.25-DTE Conformance Testing - Part 2: Data Link Conformance Test Suite	
ISO 8882-3♦	X.25-DTE Conformance Testing - Part 3: Packet Level Conformance Test Suite	
DIS 10588	Use of the X.25 PLP in Conjunction with X.21/X.21bis to Provide OSI CONS	
CD 10732	Use of the X.25 PLP to Provide OSI CONS Over Telephone Network	
CCITT X.25(84)♦	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit	
CCITT X.75(84)♦	Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits Between PSDNs	
CCITT X.223	Use of X.25 to Provide the OSI Connection-Mode Network Service for CCITT Applications (see ISO 8878)	
CCITT X.244	Procedure for the Exchange of Protocol Identification During Virtual Call Establishment on Packet Switched Public Data Networks	

C. CONNECTIONLESS SERVICE:

ISO 8473♦	Protocol for Providing the Connectionless-Mode Network Service	
	PDAD 1♦	Provision of the Underlying Service Assumed by ISO 8473 Over Point-to-Point Subnetworks Which Provide the OSI Data Link Service
	PDAD 2♦	Estelle Formal Description of ISO 8473 (to be reballoted as a DTR)
	AD 3♦	Provision of the Underlying Service Assumed by ISO 8473 over Subnetworks Which Provide the OSI Data Link Service
	PDAM x	PICS Proforma (new work item)
	PDAM y	Provision of the Underlying Service Assumed by ISO 8473 over ISDN Circuit-Switched B-channels (new work item)

[28] AM: Amendment to ISO standard.

DIS 9068♦	Provision of the Connectionless Network Service Using ISO 8208
PDTR xxxx♦	Formal Description of ISO 8473

D. ISDN:

ISO 9574♦	Provision of the OSI Connection-Mode Network Service (CONS) by Packet Mode Terminal Equipment Connected to an Integrated Services Digital Network (ISDN)
	DAM 1 Provision of the CONS on an ISDN Circuit-Switch Channel Connecting Directly to the Remote Terminal
SC21 N 5572	Report of the Ad Hoc CCIR/CCITT Experts Group Meeting on ISDN Satellite Matters 5-9 November 1990, Geneva, 7 January 1991
CCITT I.450♦	ISDN User-Network Interface - Layer 3 - General Aspects
CCITT I.451♦	ISDN User-Network Interface - Layer 3 - Specification
CCITT I.461♦	Support of X.21 and X.21 bis Based DTEs by an ISDN (X.30)
CCITT I.462♦	Support of Packet Mode Terminal Equipment by an ISDN (X.31)
CCITT I.463♦	Support of DTEs with V-Series Type Interfaces by an ISDN

Note: Additional ISDN standards are listed in the last section of this Appendix

E. ROUTING AND RELAY:

ISO 9542♦	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service
	Cor.[29]1 Technical Corrigendum 1 (awaiting publication)
	PDAM 1 Dynamic Discovery of OSI Addresses by End Systems (new work item)
TR 9575♦	OSI Routing Framework, 1 June 1990
DIS 10028-1♦	Definition of the Relaying Functions of a Network Layer Intermediate System - Part 1: Connection-mode Network Service
DIS 10028-2♦	Definition of the Relaying Functions of a Network Layer Intermediate System - Part 2: Connectionless Network Service
TR 10029♦	Operation of an X.25 Interworking Unit, March 1989
ISO 10030-1	End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP) [SC6 N 5006], October 1990
	PDAM 1 Dynamic Discovery of OSI NSAP Addresses by End Systems (new work item)
	PDAM 3 Specification of IS-SNARE Interactions
CD 10030-2	End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP) - Part 2· PICS Proforma [SC6 N 4053] (awaiting CD ballot)
DIS 10589	Intermediate System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8473
IST21 N 2860	EWOS Technical Guide Routeing (sic) in the Context of OSI, EWOS-EGLL9172, Final Draft, 27 May 1991
SC6 N 4053	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with ISO 8473
SC6 N 5006	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with ISO 8208 (X.25/PLP), May 1988

[29] Cor.. Technical Corrigendum to ISO standard.

SC21 N 5074	Final Answer to Q1/330.6 on Relay, Routing, and Network Management, SC21/WG1, May 1990
IST21 N 2604	Relaying the MAC Service using Transparent Bridging (CSMA/CD-CSMA/CD), 26 February 1991
IST21 N 2605	Connection-mode Transport Service over Connectionless-mode Network Service, 26 February 1991
CCITT X.110	International Routing Principles and Routing Plan for Public Data Networks
CCITT X.353	Routing Principles for Interconnecting the Maritime Satellite Data Transmission System With Public Data Networks

F. AUTOMATIC CALLING/ANSWERING EQUIPMENT:

CCITT V.25♦	Automatic Answering Equipment and/or Parallel Automatic Calling Equipment on the General Switched Telephone Network Including Procedures for Disabling of Echo Control Devices for Both Manually and Automatically Established Calls
CCITT V.25 bis♦	Automatic Calling and/or Answering Equipment on the General Switched Telephone Network (GSTN) Using the 100-Series Interchange Circuits

G. CIRCUIT SWITCHED SERVICE:

Covered by CCITT	X.21, X.24, X.26, X.27, ISO 4903, listed under Physical Layer Standards

H. LOCAL AREA NETWORKS (LANs):

DIS 10038♦	MAC Sublayer Interconnection (MAC Bridging)
ISO 10039♦	MAC Service Definition

Other standards are covered in the discussion of LAN standards for Layer 1 (Section II)

V. LAYER 4: TRANSPORT LAYER[30]

A. General
B. Connection-Oriented Service
C. Connectionless Service
D. Conformance Testing

A. GENERAL:

STANAG 4254♦	NATO Reference Model for OSI - Layer 4 (Transport Layer) Service Definition, Draft, July 1990
STANAG 4264♦	NATO Reference Model for OSI - Layer 4 (Transport Layer) Protocol Specification, Draft, July 1990
ISO 8072♦	Transport Service Definition
	AD 1♦ Connectionless-Mode Transmission
PDTR 10023♦	A Formal Description of ISC 8072 in LOTOS (awaiting decision concerning further progression)
PDTR 10172	Network/Transport Protocol Interworking Specification
PDTR 10734	Guidelines for Bridged LAN Source Routing Operation by End Systems
PDTR 10735	Standard Group MAC Addresses
DIS 10736	Transport Layer Security Protocol, JTC1/SC6, July 1991 (balloting ends June 1992)
	PDAM 1 Amendment 1, Security Association Establishment Protocol, JTC1/SC6, July 1991 (balloting ends April 1992)
DIS 10737	Specification of Elements of Management Information Related to OSI Transport Layer Standards (IS status expected June 1992)
CD xxxx♦	A Formal Description of the Transport Service Definition in Estelle
CD xxxx♦	A Formal Description of the Transport Protocol Specification in Estelle
CD xxxx♦	Transport Layer Security Protocol (awaiting CD ballot)
CCITT T.70♦	Network-Independent Basic Transport Service for the Telematic Services
CCITT X.214	Transport Service Definition for OSI for CCITT Applications

B. CONNECTION-ORIENTED SERVICE:

ISO 8073♦	Connection Oriented Transport Protocol Specification
	Cor 1♦ Technical Corrigendum 1, 15 January 1990
	Cor 2♦ Technical Corrigendum 2, 1 May 1990
	Cor 3♦ Technical Corrigendum 3, 1 June 1990
	AD 1♦ Network Connection Management Subprotocol
	AD 2♦ Operation of Class 4 Over Connectionless Network Service
	DAM 3♦ Protocol Implementation Conformance Statement Proforma
	DAM 4 Transport Protocol Enhancements
CD 10024♦	A Formal Description of ISO 8073 in LOTOS, 1988
CCITT X.224	Transport Protocol Specification for OSI for CCITT Applications

[30] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

C. CONNECTIONLESS SERVICE:

ISO 8073 DAD[31] 2♦	Connection Oriented Transport Protocol Specification - Addendum 2: Operation of Class 4 Over Connectionless Network Service
ISO 8602♦	Protocol for Providing the Connectionless-Mode Transport Service
	DAM 1 PICS Proforma

D. CONFORMANCE TESTING:

DIS 10025-1♦	Transport Conformance Testing for Connection Oriented Transport Protocol Operating Over the Connection Oriented Network Service (CONS) - Part 1: General Principles, 1989
CD 10025-2♦	Transport Conformance Testing for Connection Oriented Transport Protocol Operating Over the Connection Oriented Network Service (CONS) - Part 2: Test Suite Structure and Test Principles, 1989
DP 10025-3♦	Transport Conformance Testing for Connection Oriented Transport Protocol Operating Over the Connection Oriented Network Service (CONS) - Part 3: Abstract Test Suite Specification, 1989
DIS 10739-1	Conformance Test Suite for 9041 - Virtual Terminal Basic Class Protocol - Part 1: Test Suite Structure and Test Purposes, 31 October 1991 [SC21 N 6499] (IS expected July 1992)
CD xxxxx	Transport Test Management Protocol

[31] DAD: Draft Addendum for an ISO Standard (has the status of a DIS).

VI. LAYER 5: SESSION LAYER[32]

A. General
B. Connection-Oriented Service
C. Connectionless Service
D. Telematic Services

A. GENERAL:

STANAG 4255♦	NATO Reference Model for OSI - Layer 5 (Session Layer) Service Definition, Draft, April 1990
STANAG 4265♦	NATO Reference Model for OSI - Layer 5 (Session Layer) Protocol Specification, Draft, April 1990
ISO 8326♦	Basic Connection-Oriented Session Service Definition (equivalent to CCITT X.215), August 1987 (draft revised text of April 1990 incorporates AD 1, AD 2, and AD 3); Technical Corrigendum, April 1990
AD 1♦	Session Symmetric Synchronization for the Session Service (not part of CCITT Recommendation), October 1989 [SC21 N 3507]
AD 2♦	Incorporation of Unlimited User Data, June 1988 [SC21 N 2495]
AD 3♦	Connectionless-Mode Session Service, August 1989 [SC21 N 3462]
DAM 4.2	Additional Resynchronization Functionality, May 1991 [SC21 N 5921]
TR 9571♦	LOTOS Description of the Session Service, September 1989 [SC21 N 3148, January 1989]
TR 9572♦	LOTOS Description of the Session Protocol, September 1989 [SC21 N 3149, January 1989]
ISO 10168-1♦	Conformance Test Suite for the Session Protocol - Part 1: Test Suite Structure and Test Purposes, 19 April 1990 [SC21 N 4159, December 1989], January 1991)
WD 10168-2♦	Conformance Test Suite for the Session Protocol - Part 2: Generic Test Suite, 1989 (CD text expected October 1993, DIS in October 1994, IS in October 1995)
WD 10168-3♦	Conformance Test Suite for the Session Protocol - Part 3: Session Generic Test Suite, July 1989 [SC21 N 3667] (CD text expected in October 1993)
DIS 10168-4♦	Conformance Test Suite for the Session Protocol - Part 4: Session Test Management Protocol Specification, December 1990 [SC21 N 5026]
SC21 N 6110	Session Layer Extension to Support Re-Use of Transport Connections, WG6, JTC1 N 1436, 3 July 1991 (voting ends 21 October 1991) (new work item)
CCITT X.215	Session Service Definition for OSI for CCITT Applications

[32] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

B. CONNECTION-ORIENTED SERVICE:

ISO 8327♦	Basic Connection-Oriented Session Protocol Specification, August 1987 (draft revised text of April 1990 incorporates AD 1 and AD 2); Technical Corrigendum, April 1990
AD 1♦	Session Symmetric Synchronization for the Session Protocol, October 1989 [SC21 N 3508]
AD 2♦	Incorporation of Unlimited User Data, June 1988 [SC21 N 2494]
DAM 3.2	Additional Synchronization Functionality, July 1991 [SC21 N 5922 revised]
WDAM 4	Session Layer Extension to support Re-use of Transport Connection when Transport Expedited is available, July 1991, [SC21 N 6110] (PDAM expected May 1994)
CD 8327-2.2♦	Basic Connection-Oriented Session Protocol Specification - Part 2: PICS Proforma, 9 September 1991 [SC21 N 6374] (second CD went out for ballot September 1991)
CCITT X.225	Session Protocol Specification for OSI for CCITT Application

C. CONNECTIONLESS SERVICE:

ISO 8326 AD 3♦	Basic Connection-Oriented Session Service Definition, Connectionless-Mode Session Service, August 1989 [SC21 N 3462]
ISO 9548♦	Session Connectionless Protocol to Provide Connectionless-Mode Session Service [SC21 N 3460], August 1989
DIS 9548-2	Session Connectionless Protocol to Provide Connectionless-Mode Session Service - Part 2: PICS Proforma, 7 October 1991 (IS expected December 1992)

D. TELEMATIC SERVICES:

CCITT T.5♦	General Aspects of Group 4 Facsimile Apparatus
CCITT T.62♦	Control Procedures for Teletex and Group 4 Facsimile Services
CCITT X.3♦	Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN), 1988
CCITT X.20♦	Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks, 1988
CCITT X.28♦	DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Directory (Country), 1988
CCITT X.29♦	Procedures for the Exchange of Control Information and User Data Between a PAD and a Packet Mode DTE or Another PAD, 1988

VII. LAYER 6: PRESENTATION LAYER[33]

A. General
B. Connectionless Service
C. Abstract Syntax Notation One (ANS.1)
D. Telematic Services

A. GENERAL:

STANAG 4256♦	Presentation Layer Service Definition, Draft, January 1990	
STANAG 4266♦	Presentation Layer Protocol Specification, Draft, January 1990	
ISO 8822♦	Connection-Oriented Presentation Service Definition, August 1988	
	AM 1♦	Connectionless-Mode Presentation Service, 1991 [SC21 N 4933, June 1990]
	PDAM 2	Unlimited User Data, July 1991 [SC21 N 5065, July 1990] (DIS text expected June 1992, IS text in June 1993)
	PDAM 3	Abstract Syntax Registration, July 1990 [SC21 N 5067] (DIS text expected in August 1991, IS text in March 1992)
	PDAM 4♦	Support of Session Symmetric Synchronization Service, February 1990 (DIS text expected in June 1992, IS text in October 1993)
	DAM 5	Delivery of additional session synchronizaton functionality to the presentation service user, July 1991 [SC21 N 5923] (IS text expected in March 1992)
	WDAM 6	Confidentiality and Integrity, July 1990 [SC21 N 5054] (CD text expected June 1992, but may be merged with or replaced by Amendment 3)
ISO 8823♦	Connection-Oriented Presentation Protocol Specification	
	DAD 1	Renumbered as DIS 8823-2 (see below)
	WDAM 2♦	Unlimited User Data, July 1990 [SC21 N 5066]
	PDAM 3	Transfer Syntax Registration, July 1990 [SC21 N 5068] (DIS text expected August 1991, IS text in June 1992)
	PDAM 4	Support of Session Symmetric Synchronization Service, February 1990 (PDAM expected August 1991)
	DAM 5	Additional Resynchronization Functionality, July 1991 [SC21 N 5924] (IS text expected in March 1992)
	WDAM 6	Confidentiality and Integrity, July 1990 [SC21 N 3164, July 1989] (PDAM expected June 1992, but may be merged with or replaced by Amendment 3)
DIS 8823-2.2♦	Connection-Oriented Presentation Protocol Specification - Part 2: PICS Proforma, July 1990 [SC21 N 5258] (IS text expected November 1992)	
DIS 10729-1♦	Conformance Test Suite for the Presentation Protocol, Part 1: Test Suite Structure and Test Purposes, SC21/WG6, April 1991 [SC21 N 5927] (IS expected June 1992)	
CD 10729-2♦	Conformance Test Suite for the Presentation Protocol, Part 2: Test Suite Structure and Test Purposes for ASN.1 Encodings, SC21/WG6, 20 December 1991 [SC21 N 6634] (DIS text expected in June 1992, IS in June 1993)	

[33] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

[SC21 N 4151] (CD text expected in October 1991, DIS in June 1992, IS in June 1993)

WD 10729-3 — Conformance Test Suite for the Presentation Layer, Part 3: Common Presentation Abstract Test Suite, October 1991, (CD text expected June 1992)

SC21 N 5054 — Working Document on Basic Connection-Oriented Presentation Service Definition - Presentation Service to Give Confidentiality and Integrity Protection, SC21/WG6, July 1990

SC21 N 5064 — Working Document on Basic Connection-Oriented Presentation Protocol Specification - Amendment to the Presentation Protocol to Give Confidentiality and Integrity Protection, SC21/WG6, 11 July 1990

SC21 N 6132 — Call for National Body and Liaison Organization Comment on Symmetric Synchronization, 25 July 1991

CCITT X.216 — Presentation Service Definition for OSI for CCITT Applications (see ISO 8822, 1988)

CCITT X.226 — Presentation Protocol Specification for OSI for CCITT Application (see ISO 8823, 1988)

B. CONNECTIONLESS SERVICE:

ISO 8822 AD 1♦ — Connection-Oriented Presentation Service Definition - Connectionless-Mode Presentation Service, July 1990 [SC21 N 4933]

ISO 9576-1♦ — Presentation Connectionless Protocol to Provide Connectionless-Mode Presentation Service, July 1990 [SC21 N 4934]

DIS 9576-2♦ — Presentation Connectionless Protocol to Provide Connectionless-Mode Presentation Service - Part 2: PICS Proforma, July 1990 [SC21 N 5020] (balloting ended 4 January 1991; IS expected February 1992)

C. ABSTRACT SYNTAX NOTATION ONE (ASN.1):

STANAG 4258♦ — Specification of ASN.1, Draft, January 1990

STANAG 4259♦ — Specification of Basic Encoding Rules for ASN.1, Draft, January 1990

ISO 8824♦ — Specification of ASN.1, December 1987; Revised text of April 1990 incorporates AM 1 on ASN.1 Extensions [SC21 N 4720]

- AD 1♦ — ASN.1 Extensions, June 1988 (incorporated in Revised Edition of ISO 8824)
- PDAM 2 — Amendments to ISO 8824 to Give ISO 8824 Part 1: Basic ASN.1, July 1991 [SC21 N 6294] (balloting ends 29 October 1991; DIS text expected December 1991, IS in October 1992)

WD 8824-1 — Specification of Abstract Syntax Notation One (ASN.1) - Part 1: Basic ASN.1, July 1991 [SC21 N 6294]

CD 8824-2 — Specification of Abstract Syntax Notation One (ASN.1) - Part 2: Information Object Specification, July 1991 [SC21 N 6289]

CD 8824-3 — Specification of Abstract Syntax Notation One (ASN.1) - Part 3: Constraint Specification, July 1991 [SC21 N 6290]

CD 8824-4 — Specification of Abstract Syntax Notation One (ASN.1) - Part 3: Parameterisation of ASN.1 Specifications, July 1991 [SC21 N 6291]

ISO 8825♦ — Specification of Basic Encoding Rules for ASN.1, November 1987 [SC21 N 4721] (revised text of April 1990 incorporates AM 1 on ASN.1 Extensions)

- AD 1♦ — ASN.1 Extensions, June 1988 (incorporated in Revised Edition of ISO 8825)
- WDAM 2 — Amendments to ISO 8825 to Give ISO 8825 Part 1: Basic Encoding Rules, July 1991 [SC21 N 6295] (balloting ends

	29 October 1991; DIS text expected December 1991, IS in October 1992)
WD 8825-1	Specification of Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 1: Basic Encoding Rules, July 1991 [SC21 N 6295]
CD 8825-2	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 2: Packed Encoding Rules, July 1991 [SC21 N 6292]
CD 8825-3	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 3: Distinguished Encoding Rules, July 1991 [SC21 N 6293]
WD 8825-4	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 4: Light Weight Encoding Rules for ASN.1, June 1991 [SC21 N 6131]
SC21 N 3174	Working Document on ASN.1, Including Timetable, March 1989 [SC21/WG6]
SC21 N 5051	Working Document on ASN.1 Extensions, Character Sets, Version 3, SC21/WG6, July 1990
SC21 N 5052	Working Document on ASN.1 Extensions, Table Types and Functions, Version 4, SC21/WG6, July 1990
SC21 N 5053	Working Document on ASN.1 Extensions, Machine Processibility, Version 3, SC21/WG6, May 1990
SC21 N 5055	Working Document on ASN.1 Extensions, Miscellaneous Enhancements, Version 3, SC21/WG6, May 1990
SC21 N 5061	Handling of Exception Cases in ASN.1, SC21/WG6, July 1990
SC21 N 5063	Liaison on Handling of Character Sets in ASN.1, JTC1/SC2, June 1990
SC21 N 5069	Call for Comments on Technical Approval for Development of ASN.1 Work Plan, SC21/WG6, July 1990
SC21 N 5893	Liaison Statement to SC21/WG6 on Notation for Conditional ASN.1, 16 April 1991
SC21 N 6130	Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression, WG6, June 1991
SC21 N 6131	Working Draft on Light-Weight Encoding Rules for ASN.1, WG6, July 1991
SC21 N 6133	Abstract Syntax Model, WG6, June 1991
SC21 N 6136	Light Weight Encoding Rules (LWER) for ASN.1, WG6, JTC1 N 1434, July 1991 (voting ends 21 October 1991) (draft is SC21 N 6131) (new work item)
SC21/WG6 N 1125	UK Contribution on Lightweight Encoding Rules for ASN.1, 4 November 1991
CCITT X.208	Specification of Abstract Syntax Notation One (ASN.1) (see ISO 8824, Revised Edition)
CCITT X.209	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (see ISO 8825, Revised Edition)

D. TELEMATIC SERVICES:

CCITT T.6♦	Facsimile (FAX) coding schemes and coding control functions for Group 4 Facsimile Apparatus
CCITT T.51♦	Coded Character Sets for Telematic Services
CCITT T.61♦	Character Repertoire and Coded Character Sets for the International Teletex Service
CCITT T.73♦	Document Interchange Protocol for the Telematic Services

(This page intentionally left blank.)

VIII. LAYER 7: APPLICATION LAYER[34]

A. General
B. OSI Directory
C. Operating System Interface (POSIX)
D. Association Control Service Element (ACSE)
E. Commitment, Concurrency, and Recovery (CCR) Service Element
F. Reliable Transfer (RT), Remote Operations (RO), and Remote Procedure Call (RPC)
G. Message Handling System (MHS)
H. Message Oriented Text Interchange System (MOTIS)
I. Manufacturing Message Specification (MMS)
J. File Transfer, Access and Management (FTAM)
K. Virtual Terminal (VT)
L. Terminal Management (TM), Visual Display Terminal (VDT), and X-Windows
M. Job Transfer and Manipulation (JTM)
N. Telematic Services
O. Information Resource Dictionary System
P. Remote Database Access (RDA)
Q. Data Management Concepts
R. Database Languages and Concepts (SQL, NDL)
S. Distributed Transaction Processing (TP)
T. Open Distributed Processing
U. Graphical Kernel System
V. Programmer's Hierarchical Interactive Graphics System (PHIGS)
W. Dialogue with Graphical Devices (CGI)
X. Document Exchange (ODA, ODIF, DOAM, DFR, DTAM)
Y. Picture Description Information Exchange (CGM, Data Compression)
Z. Standard Generalized Markup Language (SGML)
AA. Other Application Layer Standards

A. GENERAL:

STANAGs♦	[Separate Application Layer STANAGs will be developed for each application; each will contain the service definition, the protocol specification, and an interoperability profile.][35]
ISO 9545♦	Application Layer Structure (ALS), December 1989 [SC21 N 3825, August 1989]
	DAM 1 Extended Application Layer Structure (XALS), July 1991 [SC21 N 6301] (AM expected in June 1994)
	WDAM 2 Connectionless Mode Transmission, June 1988 [SC21 N 2470] (PDAM expected late 1991)
CD 10745	Upper Layer Security Model, June 1991 [SC21 N 6095] (CD ballot closes 22 October 1991)
WD xxxx	Service and Protocol for Authentication Exchange Application Service Element (ASE), January 1990 [SC21 N 4110]

[34] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

[35] *NTIS Transition Strategy*, p.3.

PDTR xxxx	Methodology and Guidelines for the Development of Application Layer Protocols, June 1990 [SC21 N 4903] (new work item of June 1988 failed but program of work with CDTR is still active; status uncertain)
WDTR xxxx	Application Layer Guidelines, November 1989 [SC21 N 3206, December 1988]
IST21 N 2836	Report on SC21/WG6 ULA Rapporteur Meeting, Arles, May 1991, 5 June 1991
SC21 N 3109	Architectural and Descriptive Issues Identified During the Workshop on Application Layer Standardization, December 1988 [SC21/WG1]
SC21 N 3208	Requirements for More Efficient Use of Application Associations, December 1988 [SC21/WG6]
SC21 N 3733	Access Control for OSI Applications, July 1989
SC21 N 4002	Extended Application Layer Structure, ANSI Contribution to SC21/WG6, October 1989
SC21 N 4106	Application Layer Recovery, January 1990 (new work item)
SC21 N 4107	Modelling for Communications Aspects of Distributed Applications, January 1990 (new work item)
SC21 N 4108	Management Information in the Upper Layers, January 1990
SC21 N 4110	Service and Protocol for Security Application Service Element, Proposal for NWI, January 1990 [name changed from Authentication Exchange ASE to Security ASE; CD expected June 1992]
SC21 N 4354	Topics Proposed for Discussion at the JTC1 Workshop on Distributed Applications, Phoenix, March 1990, U.K. Contribution, January 1990
SC21 N 4519	Clarification of ALS Modelling Concepts, Workshop on Distributed Applications, April 1990
SC21 N 4520	Issues for Consideration by Joint ULA/ODP Meeting, Seoul, May/June 1990, Workshop on Distributed Applications, April 1990
SC21 N 4674	Liaison Statement Regarding Common Application Interfaces for the Telematic Services, CCITT SG I, May 1990
SC21 N 4764	Progression of Association Pools, ANSI, May 1990
SC21 N 4766	U.S. Response to SC21/WG6 N 770 on Requirements for Extended ALS, ANSI, May 1990
SC21 N 4903	Methodology and Guidelines for the Development of Application Layer Standards, SC21/WG6, June 1990
SC21 N 4904	Request for Comment on Characteristics of an Application Service Element and Application Service Object, SC21/WG6, May 1990
SC21 N 4905	Request for Comment on Introduction of a New Relationship in ALS, SC21/WG6, June 1990
SC21 N 4908	Liaison to CCITT SG VII(Q19,Q25) on ULA Topics, SC21/WG6, June 1990
SC21 N 4926	Liaison to CCITT SG VII(Q19) on DAF, SC21/WG6, June 1990
SC21 N 5003	Distributed Applications Security Modelling and Infrastructure, SC21/WG6, July 1991
SC21 N 5011	Modelling Recovery in the Application Layer, SC21/WG6, 1 June 1990 (new work item)
SC21 N 5012	Mock-up of ISO/IEC 9545 ALS with Proposed Changes for Extended ALS, November 1990
SC21 N 5012	Proposed Draft Amendment 1 to ALS on Extended Application Layer Structure, ISO/IEC JTC WG6 ULA, November 1990
SC21 N 5016	Meeting Report for SC21/WG1/WG4/WG6/WG7 Joint Meeting on Service Conventions, ODP, and ULA on 29 May 1990, SC21, June 1990
SC21 N 5502	Liaison Concerning Application Context Negotiation During Association Establishment, November 1990

SC21 N 5503	Response to Liaison Statement SC21 N 5453 on ULA Issues Arising on Security Work, November 1990
SC21 N 5504	Response to Liaison Statement to WG6 ULA and Upper Layer Security Groups (SC21/WG6 N 906), November 1990
SC21 N 5848	Request for Documenting Requirements for More Performant Association Establishment, 4 April 1991
SC21 N 5889	Liaison Statement to SC21/WG6 CASE and ULCT Groups Regarding ACSE PICS Proforma, 16 April 1991
SC21 N 5890	Liaison Statement to SC21/WG6 CASE and ULA Groups Regarding ACSE Application Context Negotiation, 16 April 1991
SC21 N 6017	Comments on Standardization of Application Programmatic (sic) Interfaces, WG4, May 1991
SC21 N 6061	Progression of Methodology and Guidelines for the Development of Application Layer Standards, WG6, June 1991
SC21 N 6068	Modelling Recovery in the Application Layer, WG6, June 1991
SC21 N 6071	Guidelines for Application Context Definition, WG6, June 1991
SC21 N 6096	Working Draft of Security Exchange ASE - Part 1: Security Exchange Model and Specification Framework, WG6, June 1991 [Part 2: Security Exchange ASE Service Definition; Part 3: Security Exchange ASE Protocol Specification; and Part 4: Security Exchange ASE PICS Proforma]
SC21 N 6097	Working Draft of Security Exchange ASE - Part 2: Security Exchange ASE Service Definition, WG6, June 1991
SC21 N 6098	Working Draft of Security Exchange ASE - Part 3: Security Exchange ASE Protocol Specification, WG6, June 1991
SC21 N 6099	Authentication Services for Distributed Applications, WG6, 1 July 1991 [WD 5/91, CD 5/92, DIS 5/93, IS 5/94], JTC1 N 1437, July 1991 (new work item)
SC21 N 6404	Proposal for a New Work Item: API (Application Program Interface) for Windows Systems, 10 September 1991
SC21 N 6405	Proposal for a New Work Item: Model and Framework of Interfaces for Application Portability, 10 September 1991

Note: Presentation cryptographic techniques [Project transferred from SC20]

Note: Practical conditions for ACSE authentication [Project transferred from SC20]

B. OSI DIRECTORY:

ISO 9594-1♦ The Directory - Part 1: Overview of Concepts, Models and Services, December 1990 [SC21 N 4701] (CCITT X.500)

- PDAM 1.2 Replication, Schema and Access Control, May 1991 [SC21 N 5942] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-2♦ The Directory - Part 2: Models, December 1990 [SC21 N 4702] (CCITT X.501)

- PDAM 1.3 Access Control, May 1991 [SC21 N 5952] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)
- PDAM 2.2 Schema Extensions, May 1991 [SC21 N 5943] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)
- PDAM 3.2 Replication, May 1991 [SC21 N 5944] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-3♦ The Directory - Part 3: Abstract Service Definition, December 1990 [SC21 N 4703] (CCITT X.511)

PDAM 1.3 Access Control, May 1991 [SC21 N 5953] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

PDAM 2.2 Replication, Schema and Enhanced Search, May 1991 [SC21 N 5945] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-4♦ The Directory - Part 4: Procedures for Distributed Operations, December 1990 [SC21 N 4704] (CCITT X.518)

PDAM 1.3 Access Control, 16 May 1991 [SC21 N 5954] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

PDAM 2.2 Replication, Schema and Enhanced Search, May 1991 [SC21 N 5946] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-5♦ The Directory - Part 5: Protocol Specifications, December 1990 [SC21 N 4705] (CCITT X.519)

PDAM 1.2 Replication, May 1991 [SC21 N 5947] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-6♦ The Directory - Part 6: Selected Attribute Types, December 1990 [SC21 N 4706] (CCITT X.520)

PDAM 1.2 Schema Extensions, May 1991 [SC21 N 5946] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-7♦ The Directory - Part 7: Selected Object Classes, December 1990 [SC21 N 4707] (CCITT X.521)

PDAM 1.2 Schema Extensions, May 1991 [SC21 N 5946] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-8♦ The Directory - Part 8: Authentication Framework, December 1990 [SC21 N 4708] (CCITT X.509)

PDAM 1.2 Access Control, May 1991 [SC21 N 5955] (balloting ends September 1991; DIS text expected in November 1991, IS in October 1992)

CD 9594-9.2 The Directory - Part 9: Replication, May 1991 [SC21 N 5951]

WD 9594-10♦ The Directory - Part 10: Directory PICS Proforma, July 1990 [SC21 N 4913] (CD text expected in June 1992, DIS text in June 1993, and IS text in June 1994)

WD 9594-X♦ The Directory - Part X: Text Suite Structure and Test Purposes and Abstract Test Suite for the OSI Directory, August 1990 [SC21 N 4951] (NWI not accepted]

WD 9594-Y♦ The Directory - Part Y: Replication and Knowledge Management, July 1990 [SC21 N 4913] (CD text expected November 1991]

JTC1 N 1440 Use of Systems Management for Administration of the Directory, 23 August 1991

SC21 N 3316 Access Control for OSI Management and The Directory

SC21 N 3317 Working Document on Extended Information Models

SC21 N 3318 Working Document on the Directory Schema

SC21 N 3319 Working Document on Replication and Knowledge Distribution

SC21 N 3320 Working Document on Access Control

SC21 N 3321 Working Document on Enhanced Search

SC21 N 3322 Working Document on Attribute Classes

SC21 N 3323	Request for National Body and CCITT Member Contributions on Directory PICS Proforma
SC21 N 4709	Directory Implementor's Guide, CCITT WG VII(Q.20), June 1990
SC21 N 4744	Development of the DSA Information Model: Extended Distribution Knowledge Model, SC21/WG4, May 1990
SC21 N 4769	Discussion of Initial Schema Information Acquisition for Directory, SC21/WG4, May 1990
SC21 N 4770	Short-Form Names for Directory, SC21/WG4, May 1990
SC21 N 4771	US Positions on SC21 N 433, Working Draft on the Schema, SC21/WG4, May 1990
SC21 N 4773	Development of the DSA Information Model: Basic Distribution Knowledge, SC21/WG4, May 1990
SC21 N 4799	Letter for Information on Disposition of EDIMS Use of Directory, May 1990
SC21 N 4802	Liaison Statement to SC21 on Comments on Short Form Names and Other Name Forms, CCITT SG I(Q.16), May 1990
SC21 N 4803	Publication of Directory Schema and Other Registered Object Definitions, Canada, May 1990
SC21 N 4804	Proposed DIT Structure Rule Definition, May 1990
SC21 N 4806	Use of External Data Transfer Systems for Shadow Updates, May 1990
SC21 N 4918	Question on Standardization of Directory API, July 1990
SC21 N 4922	Information on Distributed Entries, SC21/WG4, July 1990
SC21 N 4924	Extensions to Directory Abstract Service, Working Draft, SC21/WG4, July 1990
SC21 N 4951	Test Suites for OSI Directory, SC21/WG4, July 1990 (new work item)
SC21 N 5351	USA, Time Stamps, September 1990
SC21 N 5426	Directory Implementor's Guide - Editor, Version 3, ISO/IEC JTC1, November 1990
SC21 N 5826	EWOS Working Document on Behaviour of DSAs for Distributed Operations, EWOS/EGDIR/91/A/713, April 1991
SC21 N 5887	Liaison Statement to CCITT Q20/VII and SC21/WG4 Directories Regarding Use of caseExactStringSyntax in Transaction Processing, 16 April 1991
SC21 N 6002	Liaison to SC21 on Directory's Use of ISO 9066 (ROSE), WG4, June 1991
SC21 N 6006	Use of Systems Management for Administration of the Directory, WG4, JTC1 N 1440, July 1991 (new work item)
SC21 N 6007	FTAM Document Type for Directory, WG4, May 1991
SC21 N 6008	Proposed New Question Q4/4 on Directory Schema Migration, 29 July 1991
SC21 N 6063	Use of Object Identifiers to Access Directory Information, WG6, June 1991
SC21 N 6172	Security Enhancement to Directory (Extension to ISO/IEC 9594-8), WG1, July 1991 (new work item)
SC21 N 6314	Directory Implementor's Guide , Version 5, CCITT, July 1991
CCITT X.500	The Directory - Overview of Concepts, Models, and Services
CCITT X.501	The Directory - Models
CCITT X.509	The Directory - Authentication Framework
CCITT X.511	The Directory - Abstract Service Definition
CCITT X.518	The Directory - Procedures for Distributed Operation
CCITT X.519	The Directory - Protocol Specifications
CCITT X.520	The Directory - Selected Attribute Types
CCITT X.521	The Directory - Selected Object Classes

C. CPERATING SYSTEM INTERFACE:

ISO 2375	Data Processing - Procedures for the Registration of Escape Sequences, November 1985
ISO 9945-1	Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Interface, 1990
DP 9945-1.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.1: Language Independent Base (WG 15 work item based on IEEE P1003.1c)
DP 9945-1.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.2: Real-time and Extensions (WG 15 work item based on IEEE P1003.4 and .1b)
DP 9945-1.3	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3: Distribution Services (WG 15 work item based on IEEE P1003.8)
DP 9945-1.3.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.1: Transparent File Access (WG 15 work item based on IEEE P1003.8)
DP 9945-1.3.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.2: Remote Procedure Call (WG 15 work item based on IEEE P1237)
DP 9945-1.3.3	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.3: Transport Interface (WG 15 work item based on IEEE P1003.11)
DP 9945-1.3.4,	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.4: Name Space/Directory Services (WG 15 work item based on IEEE P1003.12)
DP 9945-2	Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities, 1990 [failed registration ballot; new draft requested for registration (on hold)]
DP 9945-2.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 2.1: Shell and Utilities (WG 15 work item based on IEEE P1003.2)
DP 9945-2.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 2.2: User Portability Extensions (WG 15 work item based on IEEE P1003.2a)
DP 9945-3	Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Management
DP 9945-3.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 3.1: General Services (WG 15 work item based on IEEE P1003.7)
DP 9934-3.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 3.2: Batch Services (WG 15 work item based on IEEE P1003.10)
DP xxxx♦	Operating System Command and Response Language (OSCRL)
DP xxxx♦	System Software Interface for Application Programmes (SSI)
IST21 N 2852	POSIX Security Call for New Work Items, SC22/WG15, June 1991
SC21 N 6403	Proposal for a New Work Item: Generic Operating System Interface, 10 September 1991

D. ASSOCIATION CONTROL SERVICE ELEMENT (ACSE):

ISO 8649♦	Service Definition for the ACSE (equivalent to CCITT X.217)	
	AM 1	Peer-Entity Authentication During Association Establishment, September 1989 [SC21 N 5462, November 1990]
	AM 2♦	Connectionless-Mode ACSE Service, April 1991 [SC21 N 3458, 1 June 1990]

	WDAM 3♦ Application Context Management (CD text expected in June 1993)
ISO 8650♦	Protocol Specification for the ACSE (equivalent to CCITT X.227); Technical Corrigendum, 1 June 1990
	AM 1 Peer-Entity Authentication During Association Establishment, September 1989 [SC21 N 5463, November 1990]
	WDAM 2♦ Application Context Management (PDAM expected in June 1993)
DIS 8650-2	ACSE PICS Proforma, July 1990 [SC21 N 5024] (IS text expected in 1991)
ISO 10035♦	Connectionless ACSE Protocol Specification, July 1990 [SC21 N 3456]
WD 10035-2	Connectionless ACSE Protocol Specification - Part 2: PICS Proforma for Connectionless ACSE Protocol, July 1989 [SC21 N 3218]
ISO 10169-1♦	Conformance Test Suite for the ACSE Protocol - Part 1: Test Suite Structure and Test Purposes, 24 September 1991 [SC21 N 6421]
WD 10169-2	Conformance Test Suite for the ACSE Protocol - Part 2: Abstract Test Suite, (CD expected October 1992)
SC21 N 5835	Discussion Paper on Association Pools as an Extension of ACSE, WG5, April 1991
SC21 N 5848	Request for Documenting Requirements for More Performant Association Establishment, 4 April 1991
SC21 N 5889	Liaison Statement to SC21/WG6 CASE and ULCT Groups Regarding ACSE PICS Proforma, 16 April 1991
SC21 N 5890	Liaison Statement to SC21/WG6 CASE and ULA Groups Regarding ACSE Application Context Negotiation, 16 April 1991
CCITT X.217	Association Control Service Definition for OSI for CCITT Applications (see ISO 8649)
CCITT X.227	Association Control Protocol Specification for OSI for CCITT Applications (see ISO 8650)

E. COMMITMENT, CONCURRENCY, AND RECOVERY (CCR) SERVICE ELEMENT:

ISO 9804♦	Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element Service, July 1990 [SC21 N 4611] (CCITT X.237)
	WDAM 1 Enhancements, 4th working draft, 1 October 1991 [SC21 N 6433] (DIS text expected March 1993, IS in March 1994)
	PDAM 2 Session Mapping Changes (Additional Resynchronization Functionality), 10 July 1991 [SC21 N 5925] (IS text expected in March 1992)
	WDAM 3♦ Restart (CD text expected May 1992)
ISO 9805♦	Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element Protocol, April 1990 [SC21 N 4612] (CCITT X.247)
	WDAM 1♦ Enhancements, 4th working draft, 24 September 1991 [SC21 N 6429] (DIS text expected March 1993, IS text March 1994)
	PDAM 2 Session Mapping Changes (Additional Resynchronization Functionality), 10 July 1991 [SC21 N 5926] (IS text expected in March 1992)
	WDAM 3♦ Restart (CD text expected May 1992, DIS in May 1993, IS in May 1994)
CD 9805-2.2♦	Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element Protocol - Part 2: PICS Proforma, August 1991 [SC21 N 6332] (DIS text expected November 1991, IS text November 1992)

SC21 N 3180	Possible CCR Extensions - Base Text, January 1989 [SC21/WG6]
SC21 N 4279	CCR Conformance Test Suite, January 1990 (CD text expected June 1993)
SC21 N 5833	TP/CCR Extensions - Proposed Restructure for Future Work, USA, April 1991
SC21 N 6126	LOTOS Description of CCR Service and Protocol, WG6, JTC1 N 1435, 3 July 1991 (voting ends 21 October 1991) [PDTR 5/92, DTR 6/93, TR 6/94] (new work item)

F. RELIABLE TRANSFER (RT), REMOTE OPERATIONS (RO), AND REMOTE PROCEDURE CALL (RPC):

ISO 9066-1.2♦	Reliable Transfer - Part 1: Model, Notation and Service Definition
ISO 9066-2.2♦	Reliable Transfer - Part 2: Protocol Specification
ISO 9072-1.2♦	Remote Operations - Part 1: Concepts and Model
	PDAM 1 Enhancements [SC21 N 6151] (Subject to Transfer of ROSE from SC18)
ISO 9072-2.2♦	Remote Operations - Part 1: Protocol Specification
DIS 10148	Basic Remote Procedure Call (RPC) Using OSI Remote Operations, [SC21 N 3463; fast-track ballot failed; DIS 10148 WITHDRAWN; proposal for new work item, SC21 N 4153, January 1990] (WG6 has requested authorization to progress to CD status) [SC21 N 6111, third working draft, 25 June 1991]
CD 11578-1	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 1: Model, Target date not available
CD 11578-2	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 2: Interface Definition Notation, Target date not available
CD 11578-3	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 3: Service Definition, Target date not available
CD 11578-4	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 4: Protocol Specification, Target date not available
CD 11578-5	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 5: PICS Proforma, Target date not available
IST21 N 2734	Part 1: Specification of ACSE, Presentation and Session Protocols for the use by ROSE and CMISE; Part 2: Enhanced Management Communications; 15 April 1991
SC21 N 4523	Modelling of Application Program Interfaces and Remote Procedure Calls, Distributed Applications Workshop, 2 April 1990
SC21 N 4767	US Response to SC21/WG6 N 7889 on Requirements for RPC Interface Definition Notation, May 1990
SC21 N 4925	Liaison to SC22/WG11 Concerning Remote Procedure Call Interface Definition Notation (IDN), June 1990
SC21 N 4927	Remote Procedure Call, Working Draft, SC21/WG6, June 1990
SC21 N 4928	Remote Procedure Call Definitions and Requirements, SC21/WG6, June 1990
SC21 N 5583	RPC Rapporteur Group Meeting, Valbonne, 5-9 November 1990
SC21 N 5584	Remote Procedure Call, Second Working Draft, SC21/WG6, January 1991
SC21 N 5585	Call for Comment on RPC Bindings in the Computational Model, SC21/WG6, January 1991
SC21 N 5586	Call for Comment on the Nature of the OSI RPC Service Boundary and Service Provider, SC21/WG6, January 1991
SC21 N 5587	Call for Comment on RPC Exception Model, SC21/WG6, January 1991
SC21 N 5588	Call for Comment on OSI RPC Interface Definition Notation (IDN), SC21/WG6, January 1991

SC21 N 5590	Temporary Working Definitions for (RPC) Client and Server, SC21/WG6, January 1991
SC21 N 5593	The Role of the Extended Application Layer Structure in the Standardization of RPC, ECMA, January 1991
SC21 N 5596	Multiple Outstanding RPC Calls, ECMA, January 1991
SC21 N 5597	RPC Context Handles, ECMA, January 1991
SC21 N 5816	Position on RPC Modelling, ECMA, March 1991
SC21 N 5817	Binding Concepts Within RPC, ECMA, March 1991
SC21 N 5818	Proposal for RPC Service Definition and Protocol Specification Parts, ECMA, March 1991
SC21 N 5819	Modelling Rationale for OSI RPC, ECMA, 28 March 1991
SC21 N 5821	Contribution on the [RPC] Computation Model, ECMA, 28 March 1991
SC21 N 5822	Proposal for the Use of the XALS in the Standardization of RPC, ECMA, March 1991
SC21 N 5823	Position on RPC Context Handles, 28 March 1991
SC21 N 5997	USA Position on Use of RTSE by SC21 Standards, June 1991
SC21 N 6002	Liaison to SC21 on Directory's Use of ISO 9066 (ROSE), WG4, June 1991
SC21 N 6111	Information Technology - Open Systems Interconnection - Remote Procedure Call, Third Working Draft, WG6, June 1991
SC21 N 6119	RO Extensions--Concepts, Model, and Notation, WG6, June 1991
SC21 N 6120	RO Extensions--Service Definition, WG6, June 1991
SC21 N 6121	RO Extensions--Protocol Specification, WG6, June 1991
SC21 N 6151	Enhancements to ROSE Service Definition, Protocol Specification, and Concepts, Model and Notation, WG6, July 1991; JTC1 N 1433 (new work item)
SC21/WG6 N 965	An OSI RPC Example Based on Other USA Positions, 22 January 1991
CCITT X.218	Reliable Transfer: Model and Service Definition (see ISO 9066-1)
CCITT X.219	Remote Operations: Model, Notation and Service Definition (see ISO 9072-1)

G. MESSAGE HANDLING SYSTEM (MHS):

STANAG 4257♦	Military Message Handling System (MMHS), Draft, May 1990
IST21 N 2685	Access to Public and Private MHS (1988) Common Facilities MTS End-User to MTS End-User and MTA, March 1991
CCITT X.218	Reliable Transfer: Model and Service Definition (see ISO 9066-1)
CCITT X.219	Remote Operations: Model and Service Definition (see ISO 9072-1)
CCITT X.228	Reliable Transfer: Protocol Specification (see ISO 9066-2)
CCITT X.229	Remote Operations: Protocol Specification (see ISO 9072-2)
CCITT X.400♦	Message Handling Systems (MHSs): System Model - Service Elements (see ISO 10021-1 for MOTIS)
CCITT X.401♦	MHSs - Basic Service Elements and Optional User Facilities
CCITT X.402♦	MHSs: Overall Architecture (ISO 10021-2, MOTIS)
CCITT X.403♦	MHSs: Conformance Testing
CCITT X.407♦	MHSs - Abstract Service Definition Conventions (ISO 10021-3, MOTIS)
CCITT X.408♦	MHSs - Encoded Information-Type Conversion Rules
CCITT X.409♦	MHSs - Presentation Transfer Syntax and Notation [replaced by X.208 (ISO 8824 with DAD 1) and X.208 (ISO 8825 with DAD 1)]

CCITT X.410♦	MHSs - Remote Operations and Reliable Transfer Server [replaced by X.218 (ISO 9066-1), X.219 (ISO 9072-1), X.228 (ISO 9066-2), and X.229 (ISO 9072-2)]
CCITT X.411♦	MHSs - Message Transfer Layer (see ISO 10021-4)
CCITT X.413♦	MHSs - Message Store: Abstract Service Definition (ISO 10021-5, MOTIS)
CCITT X.419♦	MHSs: Protocol Specifications (ISO 10021-6, MOTIS)
CCITT X.420♦	MHSs - Interpersonal Messaging User Agent Layer (ISO 10021-7, MOTIS)
CCITT X.430♦	MHSs - Access Protocol for Teletex Terminals
CCITT F.400	Message Handling System and Service Overview
CCITT F.401	Naming and Addressing for Public Message Handling Services
CCITT F.410	The Public Messaging Transfer Service
CCITT F.415	Intercommunication with Public Physical Delivery Services
CCITT F.420	The Public Interpersonal Messaging (IPM) Service
CCITT F.421	Intercommunication Between the IPM Service and the Telex Service
CCITT F.422	Intercommunication Between the IPM Service and the Teletex Service
CCITT F.500	International Public Directory Services

H. MESSAGE ORIENTED TEXT INTERCHANGE SYSTEM (MOTIS):[36]

DIS 8505	Functional Description and Service Specification for Message Oriented Text Interchange Systems (MOTIS), February 1986 (WITHDRAWN, superceded by ISO 10021)
DIS 8883	Message Oriented Text Interchange System, Message Transfer Sublayer, Message Interchange Service and Message Transfer Protocol, February 1986 [WITHDRAWN, superceded by ISO 10021-6]
DIS 9065	Message Oriented Text Interchange System (MOTIS) User Agent Sublayer - Interpersonal Messaging User Agent - Message Interchange Formats and Protocols, February 1986 [WITHDRAWN, superceded by ISO 10021]
ISO 10021-1♦	MOTIS - Part 1: System and Service (CCITT X.400), 1990
ISO 10021-2♦	MOTIS - Part 2: Overall Architecture (CCITT X.402), 1990
ISO 10021-3♦	MOTIS - Part 3: Abstract Service Definition Conventions (CCITT X.407), 1990
ISO 10021-4♦	MOTIS - Part 4: Message Transfer System - Abstract Service Definition and Procedures (CCITT X.411), 1990
ISO 10021-5♦	MOTIS - Part 5: Message Store - Abstract Service Definition (CCITT X.413), 1990
ISO 10021-6♦	MOTIS - Part 6: Protocol Specifications (CCITT X.419), 1990
ISO 10021-7♦	MOTIS - Part 7: Interpersonal Message System (CCITT X.420), 1990
DP xxxx	Mailbox Access Service and Protocol

I. MANUFACTURING MESSAGE SPECIFICATION:

ISO 9506-1♦	Manufacturing Message Specification - Part 1: Service Definition, 1990
ISO 9506-2♦	Manufacturing Message Specification - Part 2: Protocol Specification, 1990

J. FILE TRANSFER, ACCESS AND MANAGEMENT (FTAM):

ISO 8571-1♦	FTAM - Part 1: General Introduction
AM 1♦	Filestore Management, July 1991

[36] DIS 8505♦, DIS 8883♦, and DIS 9065♦ have been superceded by the other standards.

	DAM 2♦	Overlapped Access, June 1991 [SC21 N 5872]
	PDAM 3	Service Enhancement, July 1991 [SC21 N 6218)
	WDAM 4	Enhancement to FTAM Security Services [SC21 N 5155, July 1990] (CD text expected October 1992)
ISO 8571-2♦	FTAM - Part 2: Virtual Filestore Definition	
	AM 1♦	Filestore Management, July 1991
	DAM 2♦	Overlapped Access, June 1991 [SC21 N 5873]
	PDAM 3	Service Enhancement, July 1991 [SC21 N 6219)
	WDAM 4	Enhancement to FTAM Security Services [SC21 N 5155, July 1990] (CD text expected October 1992)
ISO 8571-3♦	FTAM - Part 3: File Service Definition	
	AM 1♦	Filestore Management, July 1991
	DAM 2♦	Overlapped Access, June 1991 [SC21 N 5874]
	PDAM 3	Service Enhancement, July 1991 [SC21 N 6220)
	WDAM 4	Enhancement to FTAM Security Services [SC21 N 5155, July 1990] (CD text expected October 1992)
ISO 8571-4♦	FTAM - Part 4: File Protocol Specification	
	AM 1♦	Filestore Management, July 1991
	DAM 2♦	Overlapped Access, June 1991 [SC21 N 5875]
	PDAM 3	Service Enhancement, July 1991 [SC21 N 6221)
	WDAM 4	Enhancement to FTAM Security Services [SC21 N 5155, July 1990] (CD text expected October 1992)
ISO 8571-5:1990(E)♦	FTAM - Part 5: Protocol Implementation Conformance Statement Proforma [SC21 N 5493, November 1990]	
	WDAM 1♦	Filestore Management, November 1991, [SC21 N 6665] [PDAM expected June 1992]
	WDAM 2♦	Overlapped Access, July 1990 [PDAM expected June 1992]
	WDAM 3	Service Enhancement [SC21 N 5614, January 1990] (PDAM text expected October 1992, DAM in June 1993, AM in June 1994)
	WDAM 4	Enhancement to FTAM Security Services [SC21 N 5155, July 1990] (CD text expected October 1992)
ISO 10170-1♦	Conformance Test Suite for the FTAM Protocol - Part 1: Test Suite Structure and Test Purposes, June 1991 [SC21 N 6269]	
WD 10170-2♦	Conformance Test Suite for the FTAM Protocol - Part 2: FTAM Abstract Test Suite [SC21 N 3665, June 1989] (CD text expected in 1991)	
WD 10170-3♦	Conformance Test Suite for the FTAM Protocol - Part 3: ACSE Abstract Test Suite Embedded Under FTAM (CD text expected June 1992)	
WD 10170-4♦	Conformance Test Suite for the FTAM Protocol - Part 4: Presentation Abstract Test Suite Embedded Under FTAM (CD text expected June 1992)	
WD 10170-5♦	Conformance Test Suite for the FTAM Protocol - Part 5: Session Abstract Test Suite Embedded Under FTAM (CD text expected June 1992)	
ISP 10607-1	ISPs - AFT nn - File Transfer, Access, and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM, 17 January 1991 [SGFS N 284] (ISP accepted December 1990)	
ISP 10607-2	ISPs - AFT nn - File Transfer, Access, and Management - Part 2: Definition of Document Types, Constraint Sets and Syntaxes, April 1990 [SGFS N 131] (submitted by SPAG; ISP accepted December 1990), (reprinted April 1991 to correct error in Foreword)	
	AD 1	Additional Definitions, December 1990 [balloted March 1991]

ISP 10607-3	ISPs - AFT nn - File Transfer, Access, and Management - Part 3: AFT 11 - Simple File Transfer Service (Unstructured), 17 January 1991 [SGFS N 286] (submitted by SPAG), reprinted April 1991 to correct error in Foreword
ISP 10607-4	ISPs - AFT nn - File Transfer, Access, and Management - Part 4: AFT 12 - Positional File Transfer Service, July 1991
	AD 1 Additional Definitions, July 1990 [SGFS N 245]
ISP 10607-5	ISPs - AFT nn - File Transfer, Access, and Management - Part 5: AFT 22 - Positional File Access Service, July 1991
ISP 10607-6	ISPs - AFT nn - File Transfer, Access, and Management - Part 6: AFT 12 - File Management Service, July 1991
IST21 N 2731	Proposed EN 41204, Simple File Transfer Service, April 1991
SC21 N 3372	Sharing an Association Between FTAM and Other ASE, February 1989 [SC21/WG5]
SC21 N 4162	Proposal for a NWI for Enhancement of FTAM Services to Satisfy Additional User Requirements, December 1989
SC21 N 4184	Request for National Body Comment on Security Enhancements to FTAM, SC21/WG5, November 1989
SC21 N 4192	Proposed FTAM Document Type to Support CGM, SC21/WG5, December 1989
SC21 N 5155	Enhancement of FTAM Security Services, New Work Item Proposal, SC21/WG5, July 1990
SC21 N 5164	Planned Work Schedule for FTAM, SC21/WG5, June 1990
SC21 N 5165	FTAM Constraint Set and Document Types for CGM, SC21/WG5, June 1990
SC21 N 5189	Liaison Statement to JTC1/SWG-EDI on EDIFACT Document Types for FTAM, SC21/WG5, June 1990
SC21 N 6224	Proposed EDIFACT/FTAM Document Type, WG5, July 1991
SC21 N 6225	Response to Liaison from JTC1/SC24/WG3 about CGM Document Types, 3 July 1991
IST/21 N 2514	International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM, Project Editor, January 1991
IST/21 N 2742	International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 2: Definition of Document Types, Constraint Sets and Syntaxes, Project Editor, January 1991
IST/21 N 2743	International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 3: AFT 11 - Simple File Transfer Service (Unstructured), Project Editor, January 1991
JTC1 N 955	Amendment to ISO 8671 to Deal with Authentication and Access Control in FTAM (new work item)

K. VIRTUAL TERMINAL (VT):

ISO 9040♦	Virtual Terminal Service - Base Class (April 1990 Revised Edition incorporates AD 1)
	AD 1♦ Extended Facility Set
	AM 2♦ Additional Functional Units, July 1991
ISO 9041♦	Virtual Terminal Protocol - Basic Class (April 1990 Revised Edition incorporates AD 1)
	AD 1♦ Extended Facility Set
	AM 2♦ Additional Functional Units, July 1991
ISO 9041-2♦	Virtual Terminal Protocol - Part 2: PICS Proforma, February 1992)

SC21 N 3365	Guide to ISO Virtual Terminal Standards, February 1989 [SC21/WG5]
SC21 N 5162	Conformance Test Suite for the VT Protocol, July 1990
SC21 N 6227	Virtual Terminal Support of ODA, WG5, July 1991
IST21 N 2838	Report on Work Item 21.11/Virtual Terminals, June 1991
ED xxx	Application Function A/4113, Basic Class VT, A-mode X3 Functional Standard, European Workshop for Open Systems [EWOS EG VT/90/112], Final Draft, November 1990
ENV 41 208	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 1: Virtual Terminal Service, European Prestandard, December 1990
ENV 41 208	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 2: Check List, European Prestandard, December 1990
ENV 41 208	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 3: Underlying Layers Checklist, European Prestandard, December 1990
ENV 41 209	Information System Interconnection - Basic Class Virtual Terminal - Common Control Objects, European Prestandard, December 1990

L. TERMINAL MANAGEMENT (TM), VISUAL DISPLAY TERMINAL (VDT), AND X-WINDOWS:

ISO 9241-1	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 1: Introduction
ISO 9241-2	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 2: Task Requirements
DIS 9241-3	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 3: Visual Display Requirements
DIS 9241-4	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 4: Keyboard Requirements
CD 9241-5	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 5: Workstation Layout and Postural Requirements
CD 9241-6	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 6: Environmental Requirements
CD 9241-7	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 7: Display Requirements with Reflections
CD 9241-8	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 8: Requirements for Displayed Colors
CD 9241-9	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 9: Requirements for Non-Keyboard Input Devices
WD 9241-10	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 10: Dialogue Principles
CD 9241-11	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 11: Usability Statements
CD 9241-12	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 12: Presentation of Information
WD 9241-13	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 13: User Guidance
CD 9241-14	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 14: Menu Dialogues
WD 9241-15	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 15: Command Dialogues
WD 9241-16	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 16: Direct Manipulation Dialogues

WD 9241-17	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 17: Form-Filling Dialogues
XX 9241-18	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 18: Question and Answer Dialogues (not yet started)
XX 9241-19	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 19: Natural Language Dialogues (not yet started)
CD 10184-1.2	Terminal Management - Model, July 1991 [SC21 N 4176, June 1990] (DIS text expected in July 1992, IS in July 1993)
WD 10184-2	Terminal Management - Service, July 1991 [SC21 N 4176, June 1990] (CD text expected July 1992, DIS in December 1992, IS in December 1993)
WD 10184-3	Terminal Management - Protocol, July 1991 [SC21 N 4176, June 1990] (CD text expected July 1992, DIS in December 1992, IS in December 1993)
IST21 N 2744	A Mapping of the X Window System over and OSI Stack, EWOSEG VT, April 1991
IST21 N 2982	A Mapping of the X Window System Over an OSI Stack, August 1991
SC21 N 3369	Terminal Management (TM) Issues List, February 1989 [SC21/WG5]
SC21 N 3381	Statement on TM Strategic Direction, February 1989 [SC21/WG5]
SC21 N 3383	Relationship Between TM and User Interfaces, February 1989 [SC21/WG5]
SC21 N 3390	NWI Proposal for an Addendum to CMIS/CMIP on Suppress Relay, July 1989
SC21 N 3930	Liaison Statement from JTC1/SC18 to JTC1/SC21/WG5 on Comments on Terminal Management, SC18/WG4, October 1989
SC21 N 4188	Response to SC18/WG4 N 1183, Comments on Terminal Management, and SC18/WG3 and CCITT SG VII(Q27) Liaison Statement on Terminal Management, SC21/WG5, December 1989
SC21 N 4189	Comments on the Integration of X-Windows into the OSI Environment, December 1989

M. JOB TRANSFER AND MANIPULATION (JTM):

ISO 8831♦	Job Transfer and Manipulation Concepts and Services, June 1989
DIS 8831.2	Job Transfer and Manipulation (JTM) Concepts and Service, June 1991 (IS second edition text expected November 1991)
ISO 8832♦	Specification of the Basic Class Protocol for Job Transfer and Manipulation
AM 1♦	JTM Full Protocol Specification, May 1990 [SC21 N 5225, text with amendment incorporated; and SC21 N 5224, amendment alone] (IS text expected November 1991)
SC21 N 4603	Position on Reassessment of JTM Full Class Protocol, AFNOR, March 1990
SC21 N 4641	U.S. Position on JTM Reassessment, March 1990
SC21 N 4679	Reassessment of Project 1.21.13.03 (JTM Full Class), SC21, June 1990

N. TELEMATIC SERVICES:

CCITT F.200♦	Teletex Service
CCITT F.200/C♦	Teletex Service, Annex C: Mixed Mode of Operation
CCITT F.201♦	Internetworking Between the Teletex Service and the Telex Service
CCITT T.60♦	Terminal Equipment for Use in the Teletex Service
CCITT T.63♦	Provision for Verification of Teletex Compliance
CCITT T.72♦	Terminal Capabilities for Mixed Mode of Operation
CCITT T.90♦	Teletex Requirements for Internetworking with the Telex Service
CCITT T.91♦	Teletex Requirements for Real-Time Internetworking with the Telex Service in a Packet-Switched Network Environment

CCITT T.330♦	Telematic Access to Interpersonal Messaging System
CCITT X.430♦	MHS, Access Protocol for Teletex Terminals

O. INFORMATION RESOURCE DICTIONARY SYSTEM (IRDS):

DP 8800-1	Information Resource Dictionary System (IRDS) - Part 1: Command Language and Panel Interface, April 1987 [SC21 N 1789] (projected suspended until the IRDS services interface reaches DIS status; the command language and panel interface are expected to be split into separate standards)
ISO 10027♦	IRDS Framework, June 1990 [SC21 N 4727, May 1990]
DIS 10728	IRDS - Services Interface, July 1991 [SC21 N 6315, 1 August 1991]
WD xxxx	IRDS - Design Support for SQL Applications (CD text expected January 1991)
WD xxxx	IRDS - Export/Import (CD text expected November 1990)
WD xxxx	IRDS - Extensions, July 1990 [SC21 N 5139] (CD text expected June 1992)
IST21 N 2499	Report on the Anaheim IRDS Services Interface Meetings, David JL Gradwell, 18 January 1991
IST21 N 2361	UK Comment Accompanying Vote of Disapproval on CD 10728, Information Resource Dictionary System Services Interface, UK, October 1990
IST21 N 2837	Report on the Arles IRDS Meetings, 4 June 1991
IST21 N 3055	Report on the ANSI "Harmonizing Around IRDS" Meeting, 19 August 1991
JTC1 N 1021	Proposal for a New Work Item: Data Management Export/Import for SQL and IRDS, October 1990
JTC1 N 1023	Proposal for a New Work Item: Information Resource Dictionary Systems (IRDS), October 1990
JTC1 N 1252	Summary of Voting on Document JTC1 N 1021, Proposal for a New Work Item on Data Management Export/Import for SQL and IRDS, JTC1 Secretariat, February 1991
JTC1 N 1254	Summary of Voting on Document JTC1 N 1023, Proposal for a New Work Item on Information Resource Dictionary Systems (IRDS), JTC1 Secretariat, February 1991
JTC1 N 1484	Final Disposition of Proposal for a New Work Item on Data Export/Import for SQL and IRDS, 16 August 1991
JTC1 N 1486	Final Disposition of Proposal for a New Work Item on Information Resource Dictionary Systems, 16 August 1991
SC21 N 3344	IRDS Rapporteur Group Position on Need for IRDS Specialization for RDA, April 1989 [SC21/WG3]
SC21 N 4806	Use of External Data Transfer Systems for Shadow Updates, May 1990
SC21 N 5137	Data Management Export/Import for SQL and IRDS, SC21/WG3, October 1990 (new work item)
SC21 N 5139	IRDS Extensions, SC21/WG3, July 1990 (new work item)
SC21 N 5437	Proposed Amendment to CD 10728 to Cover Error States, UK, November 1990
SC21 N 5438	CD 10728 Clause 6, Proposed Revision 1, UK, November 1990
SC21 N 5439	Proposal to Merge Working Set and Definition Working Set, UK, November 1990
SC21 N 5574,	Interim Minutes of the CD 10728 Editing Meeting, Secretary, February 1991
SC21 N 6257	Recommendation on NWI for Stored DBL Procedures, 23 July 1991
SC21 N 6251	Proposed New Question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM),, 23 July 1991.
SC21 N 6252	Revision of the IRDS Framework, WG3, July 1991 (new work item)

SC21 N 6253	Proposed New Question on the Approach to Remote IRDS Access, , 23 July 1991.
SC21 N 6317	Recommendations on IRDS Services Interface Progression (CD 10728), 1 August 1991
SC21 N 6387	Minutes of the CD 10728 (IRDS Services Interface) Continuation Meeting, 20-24 May 1991, Arles, France, 5 September 1991

P. REMOTE DATABASE ACCESS (RDA):

DIS 9579-1♦	Remote Database Access (RDA) - Part 1: Generic Model, Service, and Protocol, July 1991 [SC21 N 6375, 30 August 1991] (IS text expected in 1992)
	WDAM 1 Amendment 1. PDAM expected June 1992
DIS 9579-2♦	Remote Database Access (RDA) - Part 2: SQL Specialization, July 1991 [SC21 N 6376, 30 August 1991] (IS text expected in 1992)
	WDAM 1 Support for SQL2, March 1990 (CD text expected June 1993)
WDTR xxxx♦	Remote Database Access Tutorial, January 1989 [SC21 N 3343]
IST21 N 3059	RDA Issues and Recommended Positions, September 1991
JTC1 N 1485	Final Disposition of Proposal for a New Work Item on RDA Support for Stored DBL Statements, 16 August 1991
SC21 N 3344	IRDS Rapporteur Group Position on Need for IRDS Specialization for RDA, April 1989 [SC21/WG3]
SC21 N 3346	RDA Use of Remote Operation Notation of ROSE, December 1988 [SC21/WG3]
SC21 N 3351	RDA Requirements for CCR, December 1988 [SC21/WG3]
SC21 N 3352	Harmonization of RDA and TP, December 1988 [SC21/WG3]
SC21 N 5138	RDA Support for Shared DBL Statements, October 1990 (new work item)

Q. DATA MANAGEMENT CONCEPTS:

TR 9007	Concepts and Terminology for the Conceptual Schema and the Information Base
DIS 10032♦	Reference Model of Data Management, Revised Draft, May 1991 [SC21 N 5991] (balloting ends 4 January 1992)
WDTR xxxx	Tutorial on the Reference Model for Data Management (CDTR expected June 1992)
IST21 N 2880	Interim Report on the Feasibility of Profiling Database Enquiry, EWOSPT N 014, June 1991
NIST	Database Management Standards: Status and Applicability, 11 July 1991
SC21 N 197	Concepts and Terminology for the Conceptual Schema and the Information Base, TC97/SC5, March 1982
SC21 N 236	Assessment Guidelines for Conceptual Schema Language Proposals, TC97/SC21/WG5-3, 31 August 1985
SC21 N 3358	Generic Data Management Export/Import
SC21 N 3806	Request for New Question on Conceptual Schema Standardization, September 1989
SC21 N 3903	Modelling, Specification, Use, and Role of Conceptual Schemas, October 1989
SC21 N 4195	Draft WG3 Position on Conceptual Schema Question, February 1990
SC21 N 4199	Liaison Statement to JTC1/SC1 on SC21/WG3 Terminology, contains the Reference Model on Data Management (dated 8 August 1989), February 1990
SC21 N 4280	Proposed New Work Item: Conceptual Data Modelling Facility, SC21/WG3, February 1990
SC21 N 4383	Development of the Extended Information Model, January 1990

SC21 N 4511	U.S. Comments on Conceptual Schema, ANSI, March 1990
SC21 N 4524	Consideration of the Data Management Component of Application Standards, Workshop of Distributed Applications, April 1990
SC21 N 4593	Metadata Use and Standards for Managing Metadata, ANSI, April 1990
SC21 N 5137	Data Management Export/Import for SQL and IRDS, SC21/WG3, July 1990 (new work item)
SC21 N 5193	Conceptual Schema HOD/C Meeting report Held on 31 May 1990 in Seoul, July 1990
SC21 N 5764	Information Retrieval, Transfer and Management for USA (ANSI), April 1991
SC21 N 5851	USA Contribution to SC21 on the Conceptual Schema Topic, USA, April 1991
SC21 N 6057	Report of the Conceptual Schema Topic Meeting, Arles, 9 October 1991
SC21 N 6058	Minutes of the Conceptual Schema Topic Meeting, October 1991
SC21 N 6059	Initiative on Conceptual Schema and Common Data Modelling Facility, Conceptual Schema Topic Meeting, Arles, 25 May 1991, 28 May 1991
SC21 N 6213	Motive for the Establishment of a SC21 Special Group on Conceptual Schema and Common Data Modelling Facilities Issues, 9 October 1991
SC21 N 6449	Calling Notice for SC21 Special Meeting on Conceptual Schema Facilities and Common Data Modelling Facilities, 9-13 March 1992, Renesse, The Netherlands, 9 October 1991

R. DATABASE LANGUAGES AND CONCEPTS:

ISO 8907♦	Database Language NDL, June 1987
ISO 9075.2♦	Database Language SQL, April 1989 (incorporates AD 1) [SC21 N 3158]
	AD 1♦ Integrity Enhancements
DIS 9075.3♦	Database Language SQL2, July 1991 [SC21 N 5739] (IS status expected June 1992)
WD 9075.4♦	Database Language SQL3 (CD expected June 1993)
IST21 N 2880	Interim Report on the Feasibility of Profiling Database Enquiry, EWOSPT N 014, June 1991
JTC1 N 1484	Final Disposition of Proposal for a New Work Item on Data Export/Import for SQL and IRDS, 16 August 1991
NISTIR 4494	SQL3 Support for CALS Applications, NIST, December 1990
SC21 N 4672	Liaison Statement on Character Internationalization, SC21/WG3 on Database Language Extended SQL, 26 May 1990
SC21 N 4875	Recommendation on SQL2 Progress ISO 9075 Revised, 31 May 1990
SC21 N 5137	Data Management Export/Import for SQL and IRDS, SC21/WG3, July 1990 (new work item)
SC21 N 5737	Recommendation on Progression for CD 9075.2 Information Technology - Database Languages - SQL2, 10 April 1991
SC21 N 5738	Minutes of Editing Meeting for CD 9075.2, April 1991
SC21 N 6257	Recommendation on NWI for Stored DBL Procedures, 23 July 1991

S. DISTRIBUTED TRANSACTION PROCESSING (TP):

DIS 10026-1.2♦	Distributed Transaction Processing (TP) - Part 1: Model, February 1991 [SC21 N 5671] (IS text expected June 1992)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Security, WDAMs, January 1990 [SC21 N 4163]

DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Association Management, WDAMs, January 1990 [SC21 N 4164] (CD text expected June 1992)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Heuristic Decisions, WDAMs, January 1990 [SC21 N 4167]
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Commitment Optimization, WDAMs, January 1990 [SC21 N 4168]
DIS 10026-1/3	Draft Amendments to Parts 1-3: Distributed Transaction Processing Dialogue Recovery and User Suspension of a Dialogue, WDAMs, January 1990 [SC21 N 4170] (CD text expected June 1992)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Distributed Transaction Processing Savepoints, January 1990 [SC21 N 4171] (new work item; not accepted by JTC1, June 1990)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Sub-Transactions, WDAMs, July 1990 [SC21 N 5156] (CD text expected January 1992)
DIS 10026-1/4	Draft Amendments to Parts 1-3: Transaction Processing Separate Data and Commit Associations, WDAMs, July 1990 [SC21 N 5156] (CD text expected May 1993)
DIS 10026-2.2♦	Distributed Transaction Processing (TP) - Part 2: Service Definition, February 1991 [SC21 N 5673] WDAM 1 Commit Optimizations, February 1991 [SC21 N 5187]
DIS 10026-3♦	Distributed Transaction Processing (TP) - Part 3: Transaction Processing Protocol Specification, 15 November 1991 [SC21 N 6567] WDAM 1 Commit Optimizations, February 1991 [SC21 N 5187]
CD 10026-4.2	Distributed Transaction Processing (TP) - Part 4: PICS Proforma, October 1991 [SC21 N 6476]
CD 10026-5	Distributed Transaction Processing (TP) - Part 5: Application Context Proforma, February 1991 [SC21 N 5160]
CD 10026-6	Distributed Transaction Processing (TP) - Part 6: Unstructured Data Transfer, July 1991 [SC21 N 6222, 23 August 1991; JTC1 N 775] (DIS text expected in October 1991, IS in October 1992
WD 10026-z	Distributed Transaction Processing (TP) - Part 7: Other Data Transfer, January 1990 [SC21 N 4166] (new work item; CD text expected November 1992]
WD xxxx-1	Conformance Test Suite for the TP Protocol, Part 1: Test Suite Structure and Test Purposes, 6th Working Draft, June 1990 [SC21 N 5162] (formal WD text expected February 1991, CD text June 1992)
WD xxxx-2	Conformance Test Suite for the TP Protocol, Part 2: Abstract Test Suites, January 1990 [SC21 N 4172]
IST21 N 2765	EWOS Proposed Taxonomy for OSI-TP, May 1991
IST21 N 2879	Status of ISO Work on OSI TP Standards, EWOS/EGTP/90/19r, June 1991
SC21 N 4167	TP Heuristic Decisions, January 1990 [PDAMs dependent on National Body input]
SC21 N 4168	TP Commitment Optimizations, January 1990 [PDAMs expected June 1991]
SC21 N 4170	TP Dialogue Recovery and User Suspension of a Dialogue, January 1990 [PDAMs expected June 1992]
SC21 N 4171	TP Savepoints, January 1990 [NWI not accepted]
SC21 N 5156	TP Sub-Transactions, New Work Item Proposal, SC21/WG5, July 1990 [PDAMs expected January 1992]
SC21 N 5157	TP Separate Data and Commit Associations, New Work Item Proposal, SC21/WG5, July 1990 [PDAMs expected May 1993]
SC21 N 5170	OSI TP Association Management - Statement of Requirements, SC21/WG5, June 1990 [PDAMs expected June 1992]

SC21 N 5171	OSI TP Security - Statement of Requirements, SC21/WG5, June 1990
SC21 N 5172	Combined Use of RPC and OSI TP, SC21/WG5, June 1990
SC21 N 5173	Working Draft Unstructured Data Transfer (UDT) for TP, SC21/WG5, May 1990
SC21 N 5176	OSI TP Security, New Work Item, June 1990
SC21 N 5177	OSI TP Association Management - Revised New Work Item, SC21/WG5, June 1990
SC21 N 5179	Proposed Replacement Text for the NWI Proposal on Commitment Optimizations in SC21 N 4168 (JTC1 N 631), SC21/WG5, June 1990
SC21 N 5183	Combined Use of CMISE and OSI TP, SC21/WG5, June 1990
SC21 N 5184	Queued Data Transfer for TP, SC21/WG5, May 1990
SC21 N 5833	TP/CCR Extensions - Proposed Restructure for Future Work, USA, April 1991
SC21 N 5836	USA Discussion Paper on Subtransactions, April 1991
SC21 N 5845	Questions and Issues Concerning Combined Use of CMISE and TP, USA, April 1991
SC21 N 5886	Cooperation Between TP and CCR, 16 April 1991
SC21 N 5887	Liaison Statement to CCITT Q20/VII and SC21/WG4 Directories Regarding Use of caseExactStringSyntax in Transaction Processing, 16 April 1991
SC21 N 6222	CD 10026-6, Information Technology - Open Systems Interconnection - Distributed Transaction Processing - Part 6: Unstructured Data Transfer, 23 August 1991
SC21 N 6233	Issues Relating to TP Association Management, 29 July 1991
SC21 N 6226	TP Statement of Results, July 1991
SC21 N 6231	Preliminary Model and Service Definition for Queued Data Transfer, WG5, July 1991
SC21 N 6232	Preliminary TP Security Model, WG5, June 1991
SC21 N 6236	Requirements and Issues for Subtransactions, WG5, June 1991
SC21 N 6239	Working Document for TP Commit Optimization, WG5, June 1991
SC21 N 6240	Requirements and Issues on Separation of Data and Commitment Flows, WG5, June 1991
SC21 N 6243	TP Testing Methodology (Revised), WG5, June 1991
SC21 N 6244	Conformance Test Suite for the TP Protocol - Part 1: Test Suite Structure and Test Purposes, WG5, June 1991
SC21 N 6462	Application Context for Systems Management with TP, 15 October 1991
SC21 N 6463	Response to SC21 N 5845, "Questions and Issues Concerning Combined Use of CMISE and TP", 15 October 1991
SC21 N 6464	Contribution for TP Testing Methodology, 15 October 1991
SC21 N 6465	Contribution on Test Purposes for TP, 15 October 1991
SC21 N 6476	CD 10026-4.2, Information Technology - OSI - Distributed Transaction Processing - Part 4: PICS Proforma CD 10026-4 Editing Meeting, Arles, May 1991, 23 October 1991

T. OPEN DISTRIBUTED PROCESSING (ODP):

WD 10746-1♦	Basic Reference Model for Open Distributed Processing - Part 1: Overview (proposal for new work item, 1987) [SC21 N 6083, 30 May 1991] (CD text expected June 1993)
CD 10746-2♦	Basic Reference Model for Open Distributed Processing - Part 2: Descriptive Model (proposal for new work item, 1987) [SC21 N 6079, 30 May 1991] (proposed CD expected June 1992, but may be held up until Part 3 catches up)

WD 10746-3♦	Basic Reference Model for Open Distributed Processing - Part 3: Descriptive Model (proposal for new work item, 1987) [SC21 N 6080] 30 May 1991 (CD text expected June 1992)
WD 1076-4♦	Basic Reference Model for Open Distributed Processing - Part 4: User Model (proposal for new work item, 1987) [SC21 N 6083] (CD text expected May 1993)
WD 10746-5	Basic Reference Model for Open Distributed Processing - Part 5: Architectural Semantics, Specification Techniques, and Formalisms [SC21 N 6082] 30 May 1991. (CD expected May 1993)
SC21 N 1889	ODP: Proposed Revised Text for the NWI on the Basic Reference Model of Open Distributed Processing, April 1987
SC21 N 2507	ODP: Report on Topic 1 - The Problem of Distributed Processing, March 1988 [SC21/WG7]
SC21 N 2511	ODP: Definitions and Glossary - March 1988 Version, March 1988 [SC21/WG7]
SC21 N 3194	ODP: Working Document on Topic 2.3 - Framework of Abstractions, December 1988 [SC21/WG7]
SC21 N 3202	ODP: Recommendations of SC21/WG7, Sydney, December 1988
SC21 N 3288	ODP: Working Document on Topic 2.2 - Properties and Design Freedoms, December 1988 [SC21/WG7]
SC21 N 3801	Support Environment for Open Distributed Processing, ECMA, September 1989
SC21 N 4019	ODP: Topics List - November 1989 Version - for the Basic Reference Model of Open Distributed Processing, November 1989
SC21 N 4020	ODP: List of Open and Resolved Issues - November 1989 Version, December 1989
SC21 N 4021	ODP: Document Register and Bibliography - November 1989 Version, December 1989
SC21 N 4022	ODP: Working Document on Topic 4.1 - Structures and Functions, December 1989 [superceded by SC21 N 4885]
SC21 N 4023	ODP: Working Document on Topic 6.1 - Modelling Techniques and Their Use in ODP, December 1989
SC21 N 4024	ODP: Working Document on Topic 6.2 - Formalisms and Specifications, December 1989
SC21 N 4025	ODP: Working Document on Topic 8.1 - Draft Basic Reference Model of Open Distributed Processing, December 1989
SC21 N 4026	ODP: Recommendations of SC21/WG7, Florence, December 1989
SC21 N 4027	ODP: Meeting Minutes of the Florence Working Group Meeting of WG7, December 1989
SC21 N 4028	ODP: SC21/WG7 Convener's Report to SC21 Plenary Meeting, December 1989
SC21 N 4029	ODP: Liaison Statement to JTC1/TSG-1 on IAP, December 1989
SC21 N 4030	ODP: Cooperation between SC21/WG7 and CCITT SG VII (Q19/DAF), December 1989
SC21 N 4031	ODP: Session Report on Joint Meeting on FDT, December 1989
SC21 N 4032	ODP: Liaison Statement to JTC1/SWG-EDI on EDI Modelling, December 1989
SC21 N 4033	ODP: Proposal for Future Cooperation Between SC21/WG6 and SC21/WG7 on ULA and ODP, December 1989
SC21 N 4564	ODP: Liaison Statement to SC21/WG7 on Relationship of DAF Architecture/Infrastructure with ODP Topic 4 - Functions and Interfaces, CCITT SG VII, March 1990

SC21 N 4655	Architectural Semantics for ODP - Reassessment Report, SC21/WG7, April 1990
SC21 N 4885	ODP: Working Document in Topic 4.3 - Function and Interface Definitions, 13 July 1990
SC21 N 5564	Proposal for a New Work Item: ODP Trader - A Standard to Define the Role and Function of the Trader in Open Distributed Processing (ODP), November 1990
SC21 N 5840	Comments on the Relationship Between Concepts and Models for OSI and ODP, USA, April 1991
SC21 N 6069	Proposed New WG6 Question Q6/2 on the Relationship Between the OSI Upper Layer Architecture and ODP, 24 July 1991
SC21 N 6070	Working Draft Answer to the Proposed WG6 Question on the Architectural Relationship Between OSI and ODP, 25 June 1991
SC21 N 6073	List of Open and Resolved Issues--June 1991 Version, June 1991
SC21 N 6079	CD 10746-2, Reference Model of ODP - Part 2: Descriptive Model, SC 21/WG 7, 30 May 1991
SC21 N 6080	Working Draft for Part 3 of the Reference Model for ODP, SC 21/WG 7, 30 May 1991
SC21 N 6081	ODP Working Document on Topic 4.3 - Function and Interface Definitions, 31 May 1991
SC21 N 6082	Recommendation X.9zz: Basic Reference Model of Open Distributed Processing - Part 5: Architectural Semantics, Specification Techniques and Formalisms, 21 August 1991
SC21 N 6083	Working Document Partial Text for Part 1 and Part IV of the Reference Model for ODP, SC 21/WG 7, 30 May 1991
SC21 N 6084	ODP Working Document on Topic 9.1 - ODP Trader, 31 May 1991
SC21 N 6085	Revised NP on ODP Trader, SC 21/WG 7, 30 May 1991
SC21 N 6086	Resolution of Ballot Comments on the NP on ODP Trader, SC 21/WG 7, 30 May 1991
SC21 N 6088	Proposal for a WG7 Question on the Suitability of the Formal Description Technique Z for Use in ODP, 31 May 1991
SC21 N 6226 Rev	OSI Distributed Transaction Processing Statement of Results, June 1991

U. GRAPHICAL KERNEL SYSTEM (GKS):

ISO 7942	Graphical Kernel System (GKS) Functional Description DAD 1 Audit Trail Metafile
ISO 8651-1	GKS Language Bindings - Part 1: FORTRAN
ISO 8651-2	GKS Language Bindings - Part 2: Pascal
ISO 8651-3	GKS Language Bindings - Part 3: Ada
DIS 8651-4	GKS Language Bindings - Part 4: C (ballot closed 2 December 1990)
ISO 8805	GKS for Three Dimensions (GKS-3D) Functional Description WDAD 1 Name Set Addendum
DIS 8806-1	GKS-3D Language Bindings - Part 1: FORTRAN
DIS 8806-3	GKS-3D Language Bindings - Part 3: Ada
DIS 8806-4	GKS-3D Language Bindings - Part 4: C (ballot closed 2 December 1990)

V. PROGRAMMER'S HIERARCHICAL INTERACTIVE GRAPHICS SYSTEM (PHIGS):

ISO 9592-1	Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 1: Functional Description

	AM 1 Amendment 1: PHIGS Plus Support
ISO 9592-2	PHIGS Language Bindings - Part 2: Archive File Format
	AM 1 Amendment 1: PHIGS Plus Support
ISO 9592-3	PHIGS Language Bindings - Part 3: Clear-Text Encoding of Archive File
	AM 1 Amendment 1: PHIGS Plus Support
ISO 9592-4	Part 4: PHIGS Plus [SC24 N 224] (ballot closed 1 September 1990)
ISO 9593-1	PHIGS Language Bindings - Part 1: FORTRAN Binding, August 1990
DIS 9593-2	PHIGS Language Bindings - Part 2: Extended Pascal (awaiting DIS ballot)
ISO 9593-3	PHIGS Language Bindings - Part 3: Ada, July 1990
DIS 9593-4	PHIGS Language Bindings - Part 4: C (ballot closed 21 March 1991)

W. DIALOGUES WITH GRAPHICAL DEVICES:

DIS 9636-1	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 1: Overview, Profiles, and Conformance (ballot closed 8 September 1990)
DIS 9636-2	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 2: Control, Negotiation, and Errors (ballot closed 8 September 1990)
DIS 9636-3	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 3: Output and Attributes (ballot closed 8 September 1990)
DIS 9636-4	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 4: Segmentation (ballot closed 8 September 1990)
DIS 9636-5	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 5: Input and Echoing (ballot closed 8 September 1990)
DIS 9636-6	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 6: Raster
WD 9636-8	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 8: FORTRAN Language Binding of CGI
WD 9636-11	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 11: C Language Binding of CGI
DIS 9637-1	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 1: Character Encoding (review period ends 19 November 1991)
DIS 9637-2	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 2: Binary Encoding
DIS 9637-3	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 3: Clear Text Encoding
DIS 9638-1	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 1: FORTRAN
DIS 9638-2	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 2: Pascal
DIS 9638-3	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 3: Ada
DIS 9638-4	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 4: C (review period ends 10 September 1991)
CD 11072	Information Processing Systems - Computer Graphics - Reference Model of Computer Graphics, 1991
CD 10641	Conformance Testing of Implementations of Graphics Standards, 1991

X. DOCUMENT EXCHANGE--ODA, ODIF, DOAM, DFR, AND DTAM:

ISO 8211	Specification for a Data Descriptive File for Information Interchange
WD 8211.2	Specification for a Data Descriptive File for Information Interchange, July 1991 [SC21 N 6128] (CD text expected December 1991, DIS in August 1992, IS in March 1993]
ISO 8613-1♦	Office Document Architecture (ODA) and Interchange Format - Part 1: Introduction and General Principles
	AM 1 Amendment 1: Document Application Profile Proforma and Notation (ballot closed 1 July 1990)
	AM 2 Amendment 2: Confor
ISO 8613-2♦	ODA and Interchange Format - Part 2: Document Structures
	PDAD 1 Formal Specification of ODA Document Structures
WD 8613-3♦	ODA and Interchange Format - Part 3: Document Processing Reference Model (WITHDRAWN)
ISO 8613-4♦	ODA and Interchange Format - Part 4: Document Profile
ISO 8613-5♦	ODA and Interchange Format - Part 5: Office Document Interchange Format (ODIF)
ISO 8613-6♦	ODA and Interchange Format - Part 6: Character Content Architectures
ISO 8613-7♦	ODA and Interchange Format - Part 7: Raster Graphics Content Architectures
ISO 8613-8♦	ODA and Interchange Format - Part 8: Geometric Graphics Content Architectures
	AM 2 Amendment 2: Color
	AD 3 Addendum 3: Alternative Representation
	AD 4 Addendum 4: Security
	AD 5 Addendum 5: Streams
	AD 6 Addendum 6: Styles
WD 8613-9	ODA and Interchange Format - Part 9: Audio Content Architecture, WD 1991; CD 1992 (1Q); DIS 1992 (4Q), IS 1993 (3Q)
ISO 8613-10	ODA and Interchange Format - Part 10: Formal Specifications
	AM 1 Amendment 1: Formal Specification of the Document Profile (ballot closed 1 March 1991)
	AM 2 Amendment 2: Formal Specification of the Raster Graphics Content Architectures (ballot closed 1 March 1991)
ISO 10031-1	Distributed Office Applications Model (DOAM) - Part 1: General Model, 1991
ISO 10031-2	Distributed Office Applications Model (DOAM) - Part 2: Referenced Data, 1991
ISO 10166-1	Document Filing and Retrieval (DFR) - Part 1: Abstract Service Definition and Procedures, 1991 [SC18 N 2069, February 1989]
ISO 10166-2	Document Filing and Retrieval (DFR) - Part 2: Protocol Specification, 1991 [SC18 N 2070, February 1989]
DTR 10183	ODA and Interchange Format - Testing Methodology and Abstract Cases - Implementation Testing, 1991
DP 10303	Standard for Exchange of Product Model Data (STEP)
CD 10744	Information Technology - Hypermedia/Time-based Structuring Language (HyTime), April 1, 1991
SC21 N 4472	Liaison Statement from JTC1/SC18 to JTC1/SC21 on Changes to ASN.1, SC18/WG3 (title is in error--changes are for ODA, ISO 8613) February 1990
SC21 N 5561	Liaison Statement to ISO/IEC JTC1/SC21 from ISO/IEC JTC1/SC18 on Problem with Filters in Distributed Office Applications, 3 January 1991
SC21 N 6227	Virtual Terminal Support of ODA, WG5, July 1991
CCITT T.400	Introduction to Document Architecture, Transfer and Manipulation

CCITT T.411	Open Document Architecture (ODA) and Interchange Format - Introduction and General Principles (see ISO 8613-1)
CCITT T.412	Open Document Architecture (ODA) and Interchange Format - Document Structures (see ISO 8613-2)
CCITT T.414	Open Document Architecture (ODA) and Interchange Format - Document Profile (see ISO 8613-4)
CCITT T.415	Open Document Architecture (ODA) and Interchange Format - Open Document Interchange Format (ODIF) (see ISO 8613-5)
CCITT T.416	Open Document Architecture (ODA) and Interchange Format - Character Content Architectures (see ISO 8613-6)
CCITT T.417	Open Document Architecture (ODA) and Interchange Format - Raster Graphics Content Architectures (see ISO 8613-7)
CCITT T.418	Open Document Architecture (ODA) and Interchange Format - Geometric Graphics Content Architectures (see ISO 8613-8)
CCITT T.431	Document Transfer and Manipulation (DTAM) - Services and Protocols, Introduction and General Principles
CCITT T.432	DTAM - Services and Protocols, Service Definition
CCITT T.433	DTAM - Services and Protocols, Protocol Specification
CCITT T.441	DTAM - Operational Structure
CCITT T.501	Document Application Profile MM for the Interchange of Formatted Mixed Mode Documents (Mixed Mode)
CCITT T.502	Document Application Profile PM1 for the Interchange of Processible Form Documents (Teletex Processible Mode)
CCITT T.503	Document Application Profile for the Interchange of Group 4 Facsimile Documents

Y. PICTURE DESCRIPTION INFORMATION EXCHANGE:

ISO 8632-1	Computer Graphics Metafile (CGM): Metafile for the Storage and Transfer of Picture Description Information - Part 1: Functional Specification
	DAD 1 Audit Trail Metafile
	PDAD 2 3D Static Picture Capture Metafile
ISO 8632-2	CGM: Metafile for the Storage and Transfer of Picture Description Information - Part 2: Character Encoding
ISO 8632-3	CGM: Metafile for the Storage and Transfer of Picture Description Information - Part 3: Binary Encoding
ISO 8632-4	CGM: Metafile for the Storage and Transfer of Picture Description Information - Part 4: Clear Text Encoding
DIS 9281	Identification of Picture Coding Methods
CD 10918-1	Digital Compression and Coding of Continuous-Tone Still Images, Part 1: Requirements and Guidelines, February 1991
CD 10918-2	Digital Compression and Coding of Continuous-Tone Still Images, Part 2: Compliance Testing (expected to be published in 1991)
CD 11172	Coding of Moving Pictures and Associated Audio, December 1990
SC21 N 4192	Proposed FTAM Document Type to Support CGM, SC21/WG5, December 1989
SC21 N 5165	FTAM Constraint Set and Document Types for CGM, SC21/WG5, June 1990

Z. STANDARD GENERALIZED MARKUP LANGUAGE (SGML):

ISO 8879	Standard Generalized Markup Language (SGML), October 1986
	AM 1 Amendment 1, July 1988

ISO 9069	SGML Support Facilities - SGML Document Interchange Format (SDIF)
ISO 9070	SGML Support Facilities - Registration Procedures for Public Text Owner Identifiers, February 1990
TR 9573	SGML Support Facilities - Techniques for Using SGML
TR 10037	SGML and Text-Entry Systems - Guidelines for SGML Syntax-Directed Editing Systems (awaiting publication)
DIS 10179	Document Style Semantics and Specification Language (DSSSL), 28 June 1991
DIS 10180	Standard Page Description Language (SPDL), March 1991
SC21 N 6189	Liaison Statement to SC 18 on [SGML] Conformance, WG 1, 22 July 1991

AA. OTHER APPLICATION LAYER STANDARDS:

CCITT X.3◆	Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN)
CCITT X.28◆	DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Directory
CCITT X.29◆	Procedures for the Exchange of Control Information and User Data Between a PAD and a Packet Mode or Another PAD

(This page intentionally left blank.)

IX. MISCELLANEOUS STANDARDS[37]

A. Integrated Services Digital Network (ISDN): General Standards
B. Electronic Data Interchange (EDI)
C. Telematic Services
D. Vocabulary and Representations
E. Coded character sets
F. Man-Machine Language (MML)
G. Software Development and Documentation
H. Information Processing Equipment

A. INTEGRATED SERVICES DIGITAL NETWORK (ISDN): GENERAL STANDARDS[38]

ISO 9574♦	Provision of the OSI Connection-Mode Network Service by Packet Mode Terminal Equipment Connected to an ISDN
SC21 N 6157	Answer to CCITT SG VII Q 23 on OSI Reference Model Regarding ISDN, May 1991
CCITT I.110	General Structure of the I-Series Recommendations
CCITT I.111	Relationship With Other Recommendations Relevant to ISDNs
CCITT I.120	ISDNs
CCITT I.130	Attributes for the Characterization of Telecommunications Service Supported by an ISDN and Network Capabilities of an ISDN
CCITT I.210	Principles of Telecommunications Services Supported by an ISDN
CCITT I.211	Bearer Services Supported by an ISDN
CCITT I.212	Teleservices Supported by an ISDN
CCITT I.310	ISDN - Network Functional Principles
CCITT I.320	ISDN Protocol Reference Model
CCITT I.330	ISDN Numbering and Addressing Principles
CCITT I.331	Numbering Plan for the ISDN Era
CCITT I.410	General Aspects and Principles Relating to Recommendations on ISDN User-Network Interfaces

B. ELECTRONIC DATA INTERCHANGE (EDI):

ISO 9735	Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application Level Syntax Rules
JTC1 N 1240	Multimedia and Hypermedia, Ms. M.A. Gray, February 1991
JTC1 N 1161	Technical Study Group on Multimedia and Hypermedia, USA, January 1991
JTC1 SWG-EDI N 177	Conceptual Model for Electronic Data Interchange Standards and Services, December 1990
SC21 N 3925	Liaison Statement to JTC1 SC21 from JTC1 SWG-EDI, JTC1 SWG-EDI, October 1989
SC21 N 4799	Letter for Information on Disposition of EDIMS Use of Directory, May 1990

---

[37] The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth (Fifth Edition) *NTIS Transition Strategy*.

[38] A complete list of CCITT 1988 Recommendations on ISDN is provided in Appendix E, Section II.B.

SC21 N 5189	Liaison Statement to JTC1/SWG-EDI on EDIFACT Document Types for FTAM, SC21/WG5, June 1990
SC21 N 5635	Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI), January 1991
SC21 N 6224	Proposed EDIFACT/FTAM Document Type, WG5, July 1991

C. TELEMATIC SERVICES:

DP 9071-1.2	Text and Office Systems - Basic and Optional Requirements - Part 1: Facsimile Equipment
DP 9071-2.2	Text and Office Systems - Basic and Optional Requirements - Part 2: Text Communications Terminals
CCITT T.0	Classification of Facsimile Apparatus for Document Transmission Over the Public Networks

D. VOCABULARY AND REPRESENTATIONS:

ISO 2382-9	Vocabulary - Part 9: Data Communications
CD 2382-17.4	Data Processing - Vocabulary - Part 17: Databases, fourth committee draft [SC21 N 1281], 31 August 1991
ISO 2382-18	Data Processing - Vocabulary - Part 18: Distributed Data Processing, 1987
DP 2382-26.3	Data Processing - Vocabulary - Part 26: OSI Architecture, third CD, August 1991
ISO 3307	Representations of Time of the Day
ISO 3534	Statistics - Vocabulary and Symbols, 1977
ISO 4031	Representation of Local Time Differentials
ISO 6093	Representation of Numeric Values in Character Strings for Information Exchange
ISO 6523	Data Interchange - Structure for the Identification of Organizations
DP 7826	Representation of Data Elements
ISO 8211	Specification for a Data Descriptive File for Information Interchange
DIS 8601	Representation of Dates and Times
ISO 8790	Computer System Configuration Diagram Symbols and Conventions
DIS 9282-1	Coded Representation of Pictures - Part 1: Encoding Principles for Picture Representation in a 7- or 8-Bit Environment
DIS 9282-2	Coded Representation of Pictures - Part 2: Encoding Principles for Photographic Images
DTR 9544	Computer-Assisted Publishing - Vocabulary
SC21 N 4728	Collections of Definitions of OSI Vocabulary, SC21, April 1990
SC21 N 5394	Collections of Definitions of OSI Vocabulary, June 1991

E. CODED CHARACTER SETS:

ISO 646	ISO 7-Bit Coded Character Set for Information Exchange
ISO 2022	ISO 7-Bit and 8-Bit Coded Character Sets - Code Extension Techniques
ISO 4873	8-Bit Code for Information Interchange - Structure and Rules for Implementation
DIS 6429	ISO 7-Bit and 8-Bit Coded Character Sets - Control Functions for Coded Character Sets
ISO 6936	Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2)

DIS 6936.2	Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2), Draft Second Edition
ISO 6937-1	Coded Character Sets for Text Communication - Part 1: General Introduction
ISO 6937-2	Coded Character Sets for Text Communication - Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters
	DAD 1 Addendum 1
DIS 6937-3	Coded Character Sets for Text Communication - Part 3: Control Functions for Page-Image Format
DIS 6937-7	Coded Character Sets for Text Communication - Part 7: Greek Graphic Characters
DIS 6937-8	Coded Character Sets for Text Communication - Part 8: Cyrillic Graphic Characters
ISO 7350	Registration of Graphic Character Subrepertoires
DIS 7350.2	Registration of Graphic Character Subrepertoires, Draft Second Edition, 1987
ISO 8859-1	8-Bit Single-Byte Coded Graphic Character Sets - Part 1: Latin Alphabet No. 1
ISO 8859-2	8-Bit Single-Byte Coded Graphic Character Sets - Part 2: Latin Alphabet No. 2
ISO 8859-3	8-Bit Single-Byte Coded Graphic Character Sets - Part 3: Latin Alphabet No. 3
ISO 8859-4	8-Bit Single-Byte Coded Graphic Character Sets - Part 4: Latin Alphabet No. 4
DIS 8859-5.2	8-Bit Single-Byte Coded Graphic Character Sets - Part 5: Latin/Cyrillic Alphabet
ISO 8859-6	8-Bit Single-Byte Coded Graphic Character Sets - Part 6: Latin/Arabic Alphabet
ISO 8859-7	8-Bit Single-Byte Coded Graphic Character Sets - Part 7: Latin/Greek Alphabet
DIS 8859-8	8-Bit Single-Byte Coded Graphic Character Sets - Part 8: Latin/Hebrew Alphabet
DIS 8859-9	8-Bit Single-Byte Coded Graphic Character Sets - Part 9: Latin Alphabet No. 5
DIS 8859-10	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 10: Latin/ Alphabet, June 1991
DIS 9541-1	Font and Character Information Exchange - Part 1: Introduction (second DIS ballot closed 17 November 1990)
ISO 9541-2	Font and Character Information Exchange - Part 2: Registration and Naming Procedures
DIS 9541-3	Font and Character Information Exchange - Part 3: Glyph Shape Representation
DIS 9541-4	Font and Character Information Exchange - Part 4: Character Collections
DIS 9541-5	Font and Character Information Exchange - Part 5: Font Attributes and Character Model
DIS 9541-6	Font and Character Information Exchange - Part 6: Font and Character Attribute Subsets and Application
DP 9541-7	Font and Character Information Exchange - Part 7: Font Interchange Format
DIS 10036	Procedure for Registration of Glyph and Glyph Collection Identifiers (ballot closed 17 November 1990)
DP 10646	Multiple Octet Coded Character Set, SC27, November 1989

F. MAN-MACHINE LANGUAGE (MML):

CCITT Z.301	Introduction to the CCITT Man-Machine Language (MML)
CCITT Z.302	The Meta-Language for Describing MML Syntax and Dialogue Procedures
CCITT Z.311	Introduction to Syntax and Dialogue Procedures (MML)
CCITT Z.312	Basic Format Layout (MML)
CCITT Z.314	The Character Set and Basic Elements (MML)

CCITT Z.315	Input (Command) Language Syntax Specification (MML)
CCITT Z.316	Output Language Syntax Specification (MML)
CCITT Z.317	Man-Machine Dialogue Procedures (MML)
CCITT Z.321	Introduction to the Extended MML for Visual Display Terminals
CCITT Z.322	Capabilities of Visual Display Terminals
CCITT Z.323	Man-Machine Interaction
CCITT Z.331	Introduction to the Specification of the Man-Machine Interface
CCITT Z.332	Methodology for the Specification of the Man-Machine Interface - General Working Procedures
CCITT Z.333	Methodology for the Specification of the Man-Machine Interface - Tools and Methods
CCITT Z.341	Glossary of Terms (MML)

G. SOFTWARE DEVELOPMENT AND DOCUMENTATION:

ISO 1538	Programming Languages - ALGOL 60, 1984
ISO 1539	Programming Languages - FORTRAN
DIS 1539.2	Programming Languages - FORTRAN Extended, 1991
ISO 1989	Programming Languages - COBOL
ISO 6160	Programming Languages - PL/1
ISO 6373	Programming Languages - BASIC
ISO 6522	Programming Languages - PL/1 General Purpose Subset
ISO 6592	Guidelines for the Documentation of Computer-Based Application Systems
ISO 7185	Programming Languages - Pascal, revised 1990
DIS 8485	Programming Languages - APL, 1991
ISO 8652	Programming Languages - Ada
ISO 9001-3	Quality Systems - Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software, November 1990
TR 9294	Guidelines for the Management of Software Documentation, Technical Report Type 3, 1990
ISO 9496.2	Programming Languages - CCITT High Level Language (CHILL)
TR 9547	Programming Language Processors - Test Methods - Guidelines for Their Development and Acceptability, April 1988
ISO 9899	Programming Languages - C, 1990
DTR 10034	Guidelines for the Preparation of Conformity Clauses in Programming Language Standards
PDTR 10182	Binding Techniques for Programming Languages [SC22/WG11 N 754], February 1990
ISO 10206	Object Oriented Extensions to Pascal, 1991
DIS 10279	Programming Languages - Full BASIC, 1991
DIS 10967	Language Compatible Arithmetic Standard (LCAS) [SC22 N 796], Version 2.2A, May 1990 (undergoing public review July 1991)
ISO 11404	Information Technology - Programming Languages - Common Language-Independent Datatypes (CLID), 1991
BSI 91/64912	Ad Hoc Meeting on PCTE, 14 June 1991
BSI 91/64913	Background Information on PCTE Standardization, ECMA, ECMA TC33, April 1991
BSI 91/64914	ECMA PCTE, J. Dawes and H. Davis, ICL Secure Systems, March 1991
BSI 91/64915	Extract of PCTE Standards, ECMA, 28 February 1991

ECMA	PCTE, March 1991
ECMA	Background Information on PCTE Standardization, 12 April 1991
IST21 N 3057	Standardization of PCTE, 11 September 1991
IST21 N xxxx	Report of IST/-/1 Ad Hoc Meeting on PCTE, 19 July 1991
SC22 N 190	Specification for a Set of Common Language-Independent Data Types, working draft 4, September 1990
SC22 N 194R	Specification for a Model for Common Language-Independent Procedure Calling Mechanisms, Version 2, December 1990
SC21 N 5583	Report of Liaison Meeting with SC22/WG11, Amsterdam, September 1990, January 1991
SC21 N 5682	Contribution from WG11, Binding Techniques for Languages, February 1991
CCITT Z.200	CCITT High Level Language (CHILL) [see ISO 9496.2]

H. INFORMATION PROCESSING EQUIPMENT:

DIS 8884	Keyboards for Multiple Latin-Alphabet Languages - Layout and Operation Using Four Levels
ISO 9171-1	130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 1: Unrecorded Optical Disk Cartridge, 1990
ISO 9171-2	130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 2: Recording Format, 1990
ISO 9660	Volume and File Structure of CD-ROM for Information Exchange
DIS 9995-1	Keyboard Layouts for Text and Office Systems, Part 1: General Principles Governing Keyboard Layouts
DIS 9995-2	Keyboard Layouts for Text and Office Systems, Part 2: Alphanumeric Section
DIS 9995-3	Keyboard Layouts for Text and Office Systems, Part 3: Common Secondary Layout of Alphanumeric Zone of Alphanumeric Section
DIS 9995-4	Keyboard Layouts for Text and Office Systems, Part 4: Principles Governing the Placement of Characters and Symbols on Keys
DIS 9995-5	Keyboard Layouts for Text and Office Systems, Part 5: Editing Section
DIS 9995-6	Keyboard Layouts for Text and Office Systems, Part 6: Functional Section
DIS 9995-7	Keyboard Layouts for Text and Office Systems, Part 7: Symbols Used to Represent Functions
DP 10033	Recording of Documents Conforming to ISO 8613 on Flexible Disk Cartridges Conforming to ISO 9293
DIS 10222	Enhanced Small Device Interface, 1991
DIS 10149	Data Interchange on Read-Only 120-mm Optical Data Disks (CD-ROM)
DIS 10994	Data Interchange on 90 mm Flexible Disk Cartridges Using MFM Recording at 31 831 FTPRAD on 80 Tracks on Each Side, June 1991
DIS 11319	8 mm Wide Magnetic Tape Cartridge for Information Interchange -- Helical Scan Recording, June 1991
DIS 11321	3,81 mm Wide Magnetic Tape Cartridge for Information Interchange -- Helical Scan Recording-- Data/Dat Format, June 1991

(This page intentionally left blank.)

APPENDIX E

NUMERICAL LISTING OF ISO STANDARDS AND CCITT RECOMMENDATIONS RELEVANT TO CCISs

I. ISO Standards
II. CCITT Recommendations

NUMERICAL LISTING OF ISO STANDARDS AND CCITT RECOMMENDATIONS RELEVANT TO CCISs[1]

I. ISO STANDARDS

ISO 646	Information Processing - ISO 7-Bit Coded Character Set for Information Exchange, July 1983
ISO 1155	Use of Longitudinal Parity to Detect Errors in Information Messages
ISO 1177	Character Structure for Start/Stop and Synchronous Character Oriented Transmission
ISO 1538	Programming Languages - ALGOL 60, 1984
ISO 1539	Programming Languages - FORTRAN, 1980
DIS 1539.2	Programming Languages - FORTRAN Extended, 1991
ISO 1745	Information Processing - Basic Mode Control Procedures for Data Communication Systems, February 1975
ISO 1989	Programming Languages - COBOL, 1978
ISO 2022	Information Processing - ISO 7-Bit and 8-Bit Coded Character Sets - Code Extension Techniques, Third Edition, May 1986
ISO 2110.3♦[2]	Data Communication - 25-Pin DTE/DCE Interface Connector and Pin Assignments, Third Edition, 10 April 1989
ISO 2110 DAM 1	Data Communication - 25-Pin DTE/DCE Interface Connector and Pin Assignments, Amendment 1, Interface Connector and Contact Number Assignments for a DTE/DCE for Data Signalling Rates Above 20 kbit/s, (ballot closed 28 December 1990)
ISO 2111	Data Communication - Basic Mode Control Procedures - Code Independent Information Transfer, Second Edition, February 1985
ISO 2375	Data Processing - Procedures for the Registration of Escape Sequences, November 1985
ISO 2382-9	Data Processing - Vocabulary - Part 9: Data Communications, March 1984
CD 2382-17.4	Data Processing - Vocabulary - Part 17: Databases, fourth committee draft, 21 August 1991 [SC21 N 1281]
ISO 2382-18	Data Processing - Vocabulary - Part 18: Distributed Data Processing, 1987
DIS 2382-25	Data Processing - Vocabulary - Part 25: Local Area Networks
DP 2382-26.3	Data Processing - Vocabulary - Part 26: OSI Architecture, third CD, August 1991
ISO 2593.3♦	Data Communication - 34-Pin DTE/DCE Interface Connector and Pin Assignments, Third Edition, awaiting publication

---

1 Based on data initially provided by OMNICON in September 1988. Revised July 1990 based on *The OMNICON Index of Standards for Distributed Information and Telecommunications*, 1989, OMNICON, Inc., and status of standards papers from ISO/IEC JTC1, ANSI X3, and the British Standards Institution (BSI).

Revised December 1991 based on multiple sources including "Status of OSI (and Related) Standards," in *Computer Communication Review*, January 1991, pp. 111-131.

Two BSI documents (*ISO/IEC JTC1/SC21 Project File*, IST21 N 2933, August 1991; and *Project Overview*, IST21 N 2844, 13 June 1991) were additional major sources for updating the list of standards.

2 The symbol ♦ is used throughout this Appendix to identify those standards included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

ISO 2628	Basic Mode Control Procedures - Complements, June 1973
ISO 2629	Basic Mode Control Procedures - Conversational Information Message Transfer, February 1973
ISO 3307	Information Interchange - Representations of Time of the Day, March, 1975
ISO 3309♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Frame Structure, Third Edition, 1984
DIS 3309.4♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Frame Structure, Draft Fourth Edition (second DIS ballot closed 26 October 1990)
ISO 3309 AD 1♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Frame Structure - Addendum 1: Start/Stop transmission, 12 March 1990
ISO 3309 DAM 2♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Frame Structure - Amendment 2: Extended Transparency Option for Start/Stop Transmission (awaiting DAM ballot)
ISO 3309 PDAM 3	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Frame Structure - Amendment 3: Seven-bit Transparency Option for Start/Stop Transmission (ballot closed 10 March 1991)
ISO 3534	Statistics - Vocabulary and Symbols, 1977
ISO 4031	Information Interchange - Representation of Local Time Differentials, December 1987
ISO 4335	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures, Elements of Procedures, Third Edition, August 1987
DIS 4335.4	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures, Elements of Procedures, Draft Fourth Edition (ballot closed 26 October 1990)
ISO 4335 AD 1♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures, Elements of Procedures - Addendum 1: Asynchronous (Start/Stop) Transmission Operation, 1989
ISO 4335 AD 2♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures, Elements of Procedures - Addendum 2: Enhancement of the XID Function Utility, 1989
ISO 4335 AD 3♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Element of Procedures - Addendum 3: Start/Stop Transmission, 12 March 1990
ISO 4335 DAM 4	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Element of Procedures - Amendment 4: Flow Control Unnumbered Information (FUI), (ballot closed 24 November 1990)
ISO 4335 PDAD 5♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Element of Procedures - Addendum 5: Multi-Selective Reject, 1989
ISO 4873	Information Processing - 8-Bit Code for Information Interchange - Structure and Rules for Implementation, July 1986
ISO 4902.3♦	Data Communication - 37-Pin and 9-Pin DTE/DCE Interface Connectors and Pin Assignments, Third Edition, 1989
ISO 4903.3♦	Data Communication - 15-Pin DTE/DCE Interface Connector and Pin Assignments, Third Edition, 1989
ISO 6093	Information Processing - Representation of Numeric Values in Character Strings for Information Exchange, November 1985 (REAFFIRMED July 1991)
ISO 6160	Programming Languages - PL/1, 1979
ISO 6373	Programming Languages - BASIC
DIS 6429	ISO 7-Bit and 8-Bit Coded Character Sets - Control Functions for Coded Character Sets, May 1987

ISO 6522	Programming Languages - PL/1 General Purpose Subset, 1985
ISO 6523	Data Interchange - Structure for the Identification of Organizations, February 1984
ISO 6592	Information Processing - Guidelines for the Documentation of Computer-Based Application Systems, November 1985
ISO 6936	Information Processing - Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2), May 1983
DIS 6936.2	Informat on Processing - Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2), Draft Second Edition, October 1987
ISO 6937-1	Information Processing - Coded Character Sets for Text Communication - Part 1: General Introduction, November 1983
ISO 6937-2	Information Processing - Coded Character Sets for Text Communication - Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters, December 1983
ISO 6937-2 DAD 1	Information Processing - Coded Character Sets for Text Communication - Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters, Addendum 1, September 1987
DIS 6937-3	Information Processing - Coded Character Sets for Text Communication - Part 3: Control Functions for Page-Image Format, March 1988
DIS 6937-7	Information Processing - Coded Character Sets for Text Communication - Part 7: Greek Graphic Characters, April 1987
DIS 6937-8	Information Processing - Coded Character Sets for Text Communication - Part 8: Cyrillic Graphic Characters, April 1987
ISO 7185	Programming Languages - Pascal, 1983, revised 1990
ISO 7350	Text Communication - Registration of Graphic Character Subrepertoires, March 1984
DIS 7350.2	Text Communication - Registration of Graphic Character Subrepertoires, Draft Second Edition, October 1987
TR 7477♦	Data Communication - Arrangement for DTE to DTE Physical Connection Using V.24 and X.24 Interchange Circuits, September 1985
ISO 7478♦	Information Processing Systems - Data Communication - Multilink Procedures, July 1987
ISO 7478/Cor 1	Information Processing Systems - Data Communication - Multilink Procedures, Technical Corrigendum 1, 1 March 1989 [SC21 N 2738, June 1988]
DIS 7480.2	Information Processing - Start-Stop Transmission Signal Quality at DTE/DCE Interfaces, Second Edition (awaiting DIS ballot)
ISO 7498♦	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 1: General Aspects, October 1984 [SC21 N 3273, December 1988] (CD text for revision incorporating AD 1 is 7498-1 below)
ISO 7498/Cor 1	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 1: General Aspects, Technical Corrigendum 1, 15 December 1988
ISO 7498 AD 1♦	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 1: General Aspects, Addendum 1: Connectionless-Mode Transmission, July 1987
ISO 7498 PDAD 2♦	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 1: General Aspects, Addendum 2: Multipeer Data Transmission (MPDT) [SC21 N 3287] (Reassessment Report, SC21 N 3906, September 1989; project suspended in November 1989, SC21 N 4276). Comments on reactivation of project requested in SC21 N 6197.
CD 7498-1♦	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 1: General Aspects, 11 November 1991 [SC21 N 6152] (revised text incorporates AD 1; DIS expected in March 1992, IS in March 1993)

ISO 7498-2♦	Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture, February 1989
ISO 7498-3♦	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 3: Naming and Addressing, March 1989
ISO 7498-4♦	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework, November 1989 [SC21 N 3502, 24 April 1989]
ISO 7776♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Description of the X.25 LAPB-Compatible DTE Data Link Procedures, December 1986
ISO 7776/Cor 1	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Description of the X.25 LAPB-Compatible DTE Data Link Procedures, Technical Corrigendum 1, 1 April 1989
ISO 7776/Cor 2	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Description of the X.25 LAPB-Compatible DTE Data Link Procedures, Technical Corrigendum 2, 1 September 1989
ISO 7776 DAM 1	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Description of the X.25 LAPB-Compatible DTE Data Link Procedures, Amendment 1: PICS Proforma, (awaiting DAM ballot)
ISO 7809♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Consolidation of Classes of Procedures, February 1984
DIS 7809.2	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Consolidation of Classes of Procedures, Draft Second Edition (second DIS ballot closed 26 October 1990)
ISO 7809 AD 1♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Consolidation of Classes of Procedures - Addendum 1 (no title; contains UI Command/Responses), June 1986
ISO 7809 AD 2♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Consolidation of Classes of Procedures, Addendum 2: Descriptions of Optional Functions, June 1987
ISO 7809 AD 3♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures - Addendum 3: Start/Stop Transmission, 12 March 1990
ISO 7809 PDAD 4♦	Information Processing Systems - Data Communication - High Level Data Link Control (HDLC) Procedures - Consolidation of Classes of Procedures - Addendum 4: List of Standard Data Link Layer Protocols That Utilize HDLC Classes of Procedures, March 1988 (DP) [see DTR 10171, March 1989]
ISO 7809 DAM 5	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures - Amendment 5: Connectionless Class of Procedure, December 18, 1991)
ISO 7809 DAM 6	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures - Amendment 6: Extended Transparency Option, (awaiting DAM ballot)
ISO 7809 AM 7	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures - Amendment 7: Multi-Selective Reject, 1991
ISO 7809 PDAM 9	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures - Amendment 9: Seven-bit Transparency Option for Start/Stop Transmission (ballot closed 10 March 1991)
DP 7826	Representation of Data Elements
ISO 7942	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Functional Description, August 1985
ISO 7942 DAD 1	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Functional Description, Addendum 1: Audit Trail Metafile, 1989

ISO 8072♦	Information Processing Systems - Open Systems Interconnection - Transport Service Definition, 15 June 1986
ISO 8072 AD 1♦	Information Processing Systems - Open Systems Interconnection - Transport Service Definition - Addendum 1: Connectionless-Mode Transmission, 15 July 1986
ISO 8073♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification, 15 July 1986
ISO 8073 AD 1♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Addendum 1: Network Connection Management Subprotocol, June 1988
ISO 8073 AD 2♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Addendum 2: Class Four Operation Over Connectionless Network Service, July 1987
ISO 8073 DAM 3♦	Information Processing System - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Amendment 3: Protocol Implementation Conformance Statement Proforma (ballot closed 11 April 1991)
ISO 8073 DAM 4♦	Information Processing System - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Amendment 4: Transport Protocol Enhancements
ISO 8073/Cor 1♦	Information Processing System - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Technical Corrigendum 1, 15 January 1990
ISO 8073/Cor 2♦	Information Processing System - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Technical Corrigendum 2, 1 May 1990
ISO 8073/Cor 3♦	Information Processing System - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Technical Corrigendum 3, 1 June 1990
ISO 8208	Information Processing Systems - Data Communications - X.25 Packet Level Protocol (PLP) for Data Terminal Equipment, Second edition published March 1990
ISO 8208 AM 1	Information Processing Systems - X.25 Packet Level Protocol (PLP) for Data Terminal Equipment - Amendment 1: Alternative Logical Channel Identifier Assignment, 15 September 1990
ISO 8208 PDAD 2♦	Information Processing Systems - X.25 Packet Level Protocol (PLP) for Data Terminal Equipment - Addendum 2 - Extensions for Private and Switched Use (project cancelled; addendum WITHDRAWN, 1989)
ISO 8208 AM 3	Information Processing Systems - Data Communications - X.25 Packet Level Protocol (PLP) for Data Terminal Equipment - Amendment 3: Static Conformance Requirements, 12 October 1990
ISO 8211	Information Processing - Specification for a Data Descriptive File for Information Interchange, December 1985 (revision in progress, July 1991)
WD 8211.2	Information Processing - Specification for a Data Descriptive File for Information Interchange, July 1991 [SC21 N 6128] (CD text expected December 1991, DIS in August 1992, IS in March 1993]
ISO 8326♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Session Service Definition, 15 August 1987; revised to incorporate AD 1, AD 2, and AD 3 (draft 19 April 1990, SC21 N 4657); Technical Corrigendum, 30 April 1990 [SC21 N 4637 and 4638]
ISO 8326 AD 1♦	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Service Definition - Addendum 1: Session Symmetric Synchronization for the Session Service [SC21 N 3507, October 1989]; incorporated into ISO 8326, April 1990
ISO 8326 AD 2♦	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Service Definition - Addendum 2: Incorporation of Unlimited User Data, [SC21 N 2495, 27 June 1988]; incorporated into ISO 8326, April 1990
ISO 8326 AD 3♦	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Service Definition - Addendum 3: Connectionless-Mode Session Service [SC21 N 3462, August 1989]; incorporated into ISO 8326, April 1990

ISO 8326 DAM 4.2	Information Technology - Open Systems Interconnection - Basic Connection Oriented Session Service Definition - Addendum 4: Additional Resynchronization Functionality, 9 May 1991 [SC21 N 5921]
ISO 8327♦	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification, 15 August 1987; revised to incorporate AD 1 and AD 2 (draft 19 April 1990, SC21 N 4656); Technical Corrigendum, 30 April 1990 [SC21 N 4663-4666]
ISO 8327 AD 1♦	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification - Addendum 1: Session Symmetric Synchronization for the Session Protocol [SC21 N 3508, October 1989]; incorporated into ISO 8327, April 1990
ISO 8327 AD 2♦	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification - Addendum 2: Incorporation of Unlimited User Data [SC21 N 2494, 27 June 1988]; incorporated into ISO 8327, April 1990
ISO 8327 DAM 3.2	Information Technology - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification - Amendment 3 to Incorporate Additional Synchronization Functionality, 10 July 1991 [SC21 N 5922 revised]
ISO 8327 WDAM 4	Information Technology - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification - Amendment 4: Session Layer Extension to Support Re-use of Transport Connections when Transport Expedited is Available, July 1991 [SC21 N 6110] (PDAM expected May 1994)
CD 8327-2.2♦	Information Technology - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification - Part 2: Protocol Implementation Conformance Statement (PICS) Proforma, 9 September 1991 [SC21 N 6374] (second CD went out for ballot September 1991)
ISO 8348♦	Information Processing Systems - Data Communications - Network Service Definition, 15 April 1987
ISO 8348 AD 1♦	Information Processing Systems - Data Communications - Network Service Definition - Addendum 1: Connectionless-Mode Transmission, 15 April 1987
ISO 8348 AD 2♦	Information Processing Systems - Data Communications - Network Service Definition - Addendum 2: Network Layer Addressing, 1 June 1988
ISO 8348 AD 3♦	Information Processing Systems - Data Communications - Network Service Definition - Addendum 3: Additional Features of the Network Service, 15 October 1988
ISO 8348 PDAM 4	Information Processing Systems - Data Communications - Network Service Definition - Addendum 4: Removal of the Preferred Decimal Encoding of the NSAP Address (awaiting PDAM ballot)
ISO 8372	Information Processing - Modes of Operation for a 64-bit Block Cipher Algorithm, 1987
ISO 8471♦	Data Communication - High-Level Data Link Control (HDLC) Balanced Classes of Procedures - Data-Link Layer Address Resolution/ Negotiation in Switched Environments, April 1987
ISO 8473♦	Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service (CLNS), January 1988
ISO 8473 PDAD 1♦	Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service (CLNS) - Addendum 1: Provision of Underlying Service Assumed by ISO 8473 Over Point-to-Point Subnetworks Which Provide the OSI Data Link Service, July 1987 (DP)
ISO 8473 PDAD 2♦	Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service (CLNS) - Addendum 2: Estelle Formal Description of ISO 8473, Revised Edition, April 1988 (to be reballoted as a DTR)
ISO 8473 AD 3♦	Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service (CLNS) - Amendment x:PICS Proforma (new work item)

ISO 8473 PDAM x	Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service (CLNS) - Addendum 3: Provision of the Underlying Service Assumed by ISO 8473 over Subnetworks Which Provide the OSI Data Link Service, 15 February 1989
ISO 8473 PDAM y	Information Processing Systems - Data Communications - Protocol for Providing the Connectionless-Mode Network Service (CLNS) - Amendment y: Provision of the Underlying Service Assumed by ISO 8473 over ISDN Circuit-Switched B-channels (new work item)
ISO 8480♦	Information Processing - Data Communication - DTE/DCE Interface Back-up Control Operation Using the 25-Pole Connector, November 1987
ISO 8481♦	Data Communication - DTE to DTE Physical Connection Using X.24 Interchange Circuits with DTE Providing Timing, September 1986
ISO 8482♦	Information Processing Systems - Data Communication - Twisted Pair Multipoint Interconnections, November 1987
DIS 8485	Programming Languages - APL, 1991
DIS 8505	Information Processing Systems - Text Communication - Functional Description and Service Specification for Message Oriented Text Interchange Systems (MOTIS), February 1986 (WITHDRAWN, superceded by ISO 10021)
TR 8509♦	Information Processing Systems - Open Systems Interconnection - Service Conventions, September 1987
ISO 8571-1♦	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 1: General Introduction, Revised Edition, October 1988; Technical Corrigendum 1, February 1990 [SC21 N 4371]
ISO 8571-1 AM 1♦	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 1: General Introduction, Amendment 1: Filestore Management, July 1990 [SC21 N 4994, October 1990] July 1991
ISO 8571-1 DAM 2♦	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 1: General Introduction, Amendment 2: Overlapped Access, 27 June 1991 [SC21 N 5872] (DIS balloting ends 27 December 1991; IS expected June 1992)
ISO 8571-1 PDAM 3	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 1: General Introduction, Amendment 3: Service Enhancement, July 1991 [SC21 N 6218] (DIS text expected in June 1992, IS in June 1993)
ISO 8571-1 WDAM 4	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 1: General Introduction, Amendment 4: Enhancement to FTAM Security Services (CD text expected October 1992)
ISO 8571-2♦	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 2: Virtual Filestore Definition, Revised Edition, October 1988; Technical Corrigendum 1, February 1990 [SC21 N 4372]
ISO 8571-2 AM 1♦	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 2: Virtual Filestore Definition, Amendment 1: Filestore Management, July 1990 [SC21 N 4995, October 1990] July 1991
ISO 8571-2 DAM 2♦	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 2: Virtual Filestore Definition, Addendum 2: Overlapped Access, 13 April 1990, 27 June 1991 [SC21 N 5873] (DIS balloting ends 27 December 1991; IS expected June 1992)
ISO 8571-2 PDAM 3	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 2: Virtual Filestore Definition, Amendment 3: Service Enhancement, July 1991 [SC21 N 6219] (DIS text expected in June 1992, IS in June 1993)
ISO 8571-2 WDAM 4	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 2: Virtual Filestore Definition,

Amendment 4: Enhancement to FTAM Security Services (CD text expected October 1992)

ISO 8571-3♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 3: File Service Definition, Revised Edition, October 1988; Technical Corrigendum 1, February 1990 [SC21 N 4373]

ISO 8571-3 AM 1♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 3: File Service Definition, Amendment 1: Filestore Management, July 1990 [SC21 N 4996, October 1990] July 1991

ISO 8571-3 DAM 2♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 3: File Service Definition, Addendum 2: Overlapped Access, 27 June 1991 [SC21 N 5874] (DIS balloting ends 27 December 1991; IS expected June 1992)

ISO 8571-3 PDAM 3 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 3: File Service Definition, Amendment 3: Service Enhancement, July 1991 [SC21 N 6220] (DIS text expected in June 1992, IS in June 1993)

ISO 8571-3 WDAM 4 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 3: File Service Definition, Amendment 4: Enhancement to FTAM Security Services (CD text expected October 1992)

ISO 8571-4♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 4: File Protocol Specification, Revised Edition, October 1988; Technical Corrigendum 1, February 1990 [SC21 N 4374]

ISO 8571-4 AM 1♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 4: File Protocol Specification, Amendment 1: Filestore Management, July 1990 [SC21 N 4997, October 1990] July 1991

ISO 8571-4 DAM 2♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 4: File Protocol Specification, Addendum 2: Overlapped Access, 27 June 1991 [SC21 N 5875] (DIS balloting ends 27 December 1991; IS expected June 1992)

ISO 8571-4 PDAM 3 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 4: File Protocol Specification, Amendment 3: Service Enhancement, July 1991 [SC21 N 6221] (DIS text expected in June 1992, IS in June 1993)

ISO 8571-4 WDAM 4 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 4: File Protocol Specification, Amendment 4: Enhancement to FTAM Security Services (CD text expected in October 1992)

ISO 8571-5:1990(E)♦ Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 5: Protocol Implementation Conformance Statement Proforma, July 1990 [SC21 N 3467, April 1989] [SC21 N 5493, November 1990]

ISO 8571-5 WDAM 1 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 5: Protocol Implementation Conformance Statement Proforma, Amendment 1: Filestore Management, November 1991 [SC21 N 6665] (PDAM expected June 1992)

ISO 8571-5 WDAM 2 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 5: Protocol Implementation Conformance Statement Proforma, Amendment 2: Overlapped Access, June 1991 [SC21 N 6274] (PDAM expected June 1992)

ISO 8571-5 WDAM 3 Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 5: Protocol Implementation Conformance Statement Proforma, Amendment 3: Service Enhancement, June 1991 [SC21 N 6223] (PDAM text expected October 1992, DAM in June 1993, AM in June 1994)

ISO 8571-5 WDAM 4	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM) - Part 5: Protocol Implementation Conformance Statement Proforma, Amendment 4: Enhancement to FTAM Security Services (CD text expected October 1992)
DIS 8601	Data Elements and Interchange Formats - Information Exchange - Representation of Dates and Times, June 1986
ISO 8602♦	Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless-Mode Transport Service, 15 December 1987
ISO 8602 DAM 1	Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless-Mode Transport Service, Amendment 1: PICS Proforma
ISO 8613-1♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 1: Introduction and General Principles, July 1988 [CCITT T.411]
ISO 8613-1 AM 1	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 1: Introduction and General Principles, Amendment 1: Document Application Profile Proforma and Notation (ballot closed 1 July 1990)
ISO 8613-1 AM 2	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 1: Introduction and General Principles, Amendment 2: Conformance Testing Methodology
ISO 8613-2♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 2: Document Structures, July 1988 [CCITT T.412]
ISO 8613-2 PDAD 1	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 2: Document Structures - Addendum 1: Formal Specification of ODA Document Structures, June 1988
WD 8613-3♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 3: Document Processing Reference Model, September 1986 (WITHDRAWN)
ISO 8613-4♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 4: Document Profile, July 1988 [CCITT T.414]
ISO 8613-5♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 5: Office Document Interchange Format (ODIF), July 1988 [CCITT T.415]
ISO 8613-6♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 6: Character Content Architectures, July 1988 [CCITT T.416]
ISO 8613-7♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 7: Raster Graphics Content Architectures, July 1988 [CCITT T.417]
ISO 8613-8♦	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 8: Geometric Graphics Content Architectures, July 1988 [CCITT T.418]
ISO 8613-8 AM 2	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Amendment 2: Color
ISO 8613-8 AD 3	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Addendum 3: Alternative Representation
ISO 8613-8 AD 4	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Addendum 4: Security
ISO 8613-8 AD 5	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Addendum 5: Streams
ISO 8613-8 AD 6	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Addendum 6: Styles

WD 8613-9	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 9: Audio Content Architectures, WD 1991; CD 1992 (1Q); DIS 1992 (4Q), IS 1993 (3Q)
ISO 8613-10	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 10: Formal Specifications
ISO 8613-10 AM 1	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 10: Formal Specifications, Amendment 1: Formal Specification of the Document Profile (ballot closed 1 March 1991)
ISO 8613-10 AM 2	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format - Part 10: Formal Specifications, Amendment 2: Formal Specification of the Raster Graphics Content Architectures (ballot closed 1 March 1991)
ISO 8632-1	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information - Part 1: Functional Specification, 1 August 1987
ISO 8632-1 DAD 1	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information - Part 1: Functional Specification, Addendum 1: Audit Trail Metafile, 1989
ISO 8632-1 PDAD 2	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information - Part 1: Functional Specification, Addendum 2: 3D Static Picture Capture Metafile, 1989
ISO 8632-2	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information - Part 2: Character Encoding, 1 August 1987
ISO 8632-3	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information - Part 3: Binary Encoding, 1 August 1987
ISO 8632-4	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information - Part 4: Clear Text Encoding, 1 August 1987
ISO 8648♦	Information Processing Systems - Open Systems Interconnection - Internal Organization of the Network Layer, 15 February 1988
ISO 8648/Cor 1	Information Processing Systems - Open Systems Interconnection - Internal Organization of the Network Layer, Technical Corrigendum 1 (awaiting publication)
ISO 8649♦	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE), 15 December 1988 [SC21 N 2326, January 1988] (defect report ballots SC21 N 4447-49, February 1990)
ISO 8649 AM 1♦	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE) - Amendment 1: Peer-Entity Authentication During Association Establishment, November 1990 [SC21 N 5462]
ISO 8649 AM 2♦	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE) - Connectionless-Mode ACSE Service, 1 June 1990 [SC21 N 4937], 1991
ISO 8649 WDAM 3♦	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE) - Application Context Management, 1989 (formal WD text expected June 1992, CD Amendment in June 1993, DIS in June 1994, IS in June 1995)
ISO 8650♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE), 15 December 1988; Technical Corrigendum, 1 June 1990; Amendment, February 1990, SC21 N 4286]
ISO 8650 AM 1♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE) - Amendment 1:

	Peer-Entity Authentication During Association Establishment, November 1990 [SC21 N 5463]
ISO 8650 WDAM 2♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE) - Amendment 2: Application Context Management (PDAM expected June 1993)
DIS 8650-2♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE) - Part 2: PICS Proforma, July 1990 [SC21 N 5024] (document will not be balloted until session PICS is at DIS status; IS status expected November 1992)
ISO 8651-1	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings - Part 1: FORTRAN, October 1988
ISO 8651-2	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings - Part 2: Pascal, October 1988
ISO 8651-3	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings - Part 3: Ada, October 1988
DIS 8651-4	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings - Part 4: C, (ballot closed 2 December 1990)
ISO 8652	Programming Languages - Ada
ISO 8790	Information Processing Systems - Computer System Configuration Diagram Symbols and Conventions, September 1987
DP 8800-1	Information Processing Systems - IRDS - Part 1: Command Language and Panel Interface, April 1987 [SC21 N 1789] (projected suspended until the IRDS services interface reaches DIS status; the command language and panel interface are expected to be split into separate standards) (published as ANSI X3.138)
ISO 8802-1♦	Information Processing Systems - Local Area Networks - Part 1: General Introduction, 1989
DIS 8802-1.2♦	Information Processing Systems - Local Area Networks - Part 1: General Introduction with System Load Protocol (ballot closed 7 March 1991)
ISO 8802-2.2♦	Information Processing Systems - Local Area Networks - Part 2: Logical Link Control, Second Edition, 16 March 1990
ISO 8802-2.2 DAM 1	Information Processing Systems - Local Area Networks - Part 2: Logical Link Control - Amendment 1: Flow Control Techniques for Bridged Local Area Networks, (ballot closed 19 November 1988)
ISO 8802-2.2 DAM 2	Information Processing Systems - Local Area Networks - Part 2: Logical Link Control - Amendment 2: Type 3 Operation-Acknowledge Connectionless Service, (ballot closed 2 May 1990)
ISO 8802-2.2 PDAM 3	Information Processing Systems - Local Area Networks - Part 2: Logical Link Control - Amendment 3: PICS Proforma, (ballot closed 10 September 1990)
ISO 8802-2.2 DAM 4	Information Processing Systems - Local Area Networks - Part 2: Logical Link Control - Amendment 4: Editorial Changes and Technical Corrections, ballot closed 24 November 1990)
ISO 8802-3♦	Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, November 1987
ISO 8802-3 DAM 1	Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 1: Physical Signalling, Medium Attachment, and Baseband Medium Specifications for Type 1BASE5, 1989
ISO 8802-3 DAM 2	Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 2: Repeater Set and Repeater Unit Specification for Use with 10BASE5 and 10BASE2 Networks, July 1987
ISO 8802-3 DAM 3	Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 3: Broadband

Medium Attachment Unit and Broadband Medium Specifications, Type 10BROAD36, (ballot closed 28 October 1990)

ISO 8802-3 DAM 4♦ Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 4: Broadband Medium Attachment Unit and Broadband Medium Specifications, Type 1BASE5 (StarLAN), (ballot closed January 1990)

ISO 8802-3 DAM 5♦ Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 5: Medium Attachment Unit and Baseband Medium Specification for a Vendor-Independent Fibre Optic Inter-Repeater Link (FOIRL), 1989

ISO 8802-3 DAM 6 Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 6: Summary of IEEE 802.3 First Maintenance Ballot (awaiting DAM ballot)

ISO 8802-3 PDAM 7 Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 7: LAN Layer Management (awaiting PDAM ballot)

ISO 8802-3 PDAM 9 Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Amendment 9: Physical Medium, Medium Attachment, and Baseband Medium Specifications, Type 10baseT (new work item)

ISO 8802-4.2♦ Information Processing Systems - Local Area Networks - Part 4: Token-Passing Bus Access Method and Physical Layer Specifications, Second Edition, November 1987

ISO 8802-5♦ Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification, February 1987

DIS 8802-5.2♦ Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification, Revised Edition (second DIS ballot on consolidated document containing Part 5 and its first 3 addenda closed 1 September 1990)

ISO 8802-5 PDAM 1 Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification - Amendment 1: 4 and 16 Mbit/s Specification, June 1989

ISO 8802-5 PDAM 2 Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification - Amendment 2: MAC Sublayer Enhancement, July 1989

ISO 8802-5 PDAM 3 Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification - Amendment 3: Management Entity Specification, July 1989

ISO 8802-5 DAM 4 Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification - Amendment 4: Source Routing MAC Bridge, (awaiting DAM ballot)

ISO 8802-5 DAM 5 Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical Layer Specification - Amendment 5: PICS Proforma, (awaiting DAM ballot)

DIS 8802-6♦ Information Processing Systems - Local Area Networks - Part 6: Distributed Queue Dual Bus (DQDB) Media Access Control (MAC), 1989

ISO 8802-7♦ Information Processing Systems - Local Area Networks - Part 7: Slotted Ring Access Method and Physical Layer Specification, 1989

DIS 8802-9♦ Information Processing Systems - Local Area Networks - Part 9: Integrated Voice and Data (IVD) LAN

ISO 8805 Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Functional Description, October 1988

ISO 8805 WDAD 1 Working Draft for Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Addendum 1: Name Set Addendum, April 1987 (WD)

DIS 8806-1	Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Language Bindings - Part 1: FORTRAN, November 1988
DIS 8806-3	Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Language Bindings - Part 3: Ada, 1989
DIS 8806-4	Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Language Bindings - Part 4: C, (ballot closed 2 December 1990)
ISO 8807♦	LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour, 15 February 1989
ISO 8807 DAM 1	LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behavior, Addendum 1, Graphical Representation of LOTOS (G-LOTOS), July 1991 [SC21 N 4228, December 1989] (IS expected December 1992) (although the new work item was not accepted, work is proceeding)
ISO 8822♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Service Definition, 15 August 1988 [SC21 N 2335, April 1988; defect report SC21 N 3761, August 1989]
ISO 8822 AM 1♦	Information Processing Systems - Open Systems Interconnection - Amendment 1: Connectionless-Mode Presentation Service, 1 June 1990 [SC21 N 4933], 1991
ISO 8822 PDAM 2	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Service Definition, Amendment 2: Unlimited User Data, July 1991 [SC21 N 5065, July 1990] (DIS text expected June 1992, IS text in June 1993)
ISO 8822 PDAM 3	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Service Definition, Amendment 3: Abstract Syntax Registration, 20 July 1990 [SC21 N 5067] (DIS text expected August 1991, IS text in June 1992)
ISO 8822 PDAM 4♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Service Definition, Amendment 4: Support of Session Symmetric Synchronization Service, February 1990 (DIS text expected June 1992, IS in October 1993)
ISO 8822 DAM 5	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Service Definition, Amendment 5: Delivery of additional session synchronizaton functionality to the presentation service user, July 1991 [SC21 N 5923] (IS text expected in March 1992)
ISO 8822 WDAM 6	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Service Definition, Amendment 6: Confidentiality and Integrity, July 1990 [SC21 N 5054] (CD text expected June 1992, but may be merged or replaced by Amendment 3)
ISO 8823♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, 15 August 1988 [SC21 N 2336, April 1988] (defect reports SC21 N 3751-3760, August 1989)
ISO 8823 DAD 1	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Amendment 1: Presentation protocol implementation conformance statement (PICS) proforma, [renumbered as DIS 8823-2, see below]
ISO 8823 PDAM 2	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Amendment 2: Unlimited User Data, July 1991 [SC21 N 5066, July 1990]
ISO 8823 PDAM 3	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Amendment 3: Transfer Syntax Registration, 20 July 1990 [SC21 N 5068] (DIS text expected August 1991, IS text in June 1992)
ISO 8823 WDAM 4♦	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Amendment 4: Support of Session Symmetric Synchronization Service, February 1990 (PDAM expected August 1991)

ISO 8823 DAM 5	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Amendment 5: Additional Resynchronization Functionality, July 1991 [SC21 N 5924] (IS text expected in March 1992)
ISO 8823 WDAM 6	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Amendment 6: Confidentiality and Integrity, July 1990 [SC21 N 3164, July 1989] (PDAM expected June 1992, but may be merged with or replaced by Amendment 3)
DIS 8823-2.2♦	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification - Part 2: Presentation Protocol Implementation Conformance Statement (PICS) Proforma, June 1990 [SC21 N 5258] (IS text expected November 1992)
ISO 8824♦	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), December 1987; Revised Edition incorporates AM 1, April 1990 [SC21 N 4720]
ISO 8824 AD 1	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) - Addendum 1: ASN.1 Extensions, June 1988 [SC21 N 2341]; incorporated in Revised Edition of ISO 8824, April 1990
ISO 8824 PDAM 2	Amendments to ISO 8824 to Give ISO 8824 Part 1: Basic ASN.1, 8 July 1991 [SC21 N 6294] (balloting ends 29 October 1991; DIS text expected December 1991, IS in October 1992)
WD 8824-1	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) - Part 1: Basic ASN.1, 8 July 1991 [SC21 N 6294]
CD 8824-2	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) - Part 2: Information Object Specification, 8 July 1991 [SC21 N 6289]
CD 8824-3	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) - Part 3: Constraint Specification, 8 July 1991 [SC21 N 6290]
CD 8824-4	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1) - Part 3: Parameterisation of ASN.1 Specifications, 8 July 1991 [SC21 N 6291]
ISO 8825♦	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), November 1987; Revised Edition incorporates AM 1, April 1990 [SC21 N 4721]
ISO 8825 AD 1	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Addendum 1: ASN.1 Extensions, June 1988 [SC21 N 2342]; incorporated in Revised Edition of ISO 8825, April 1990
ISO 8825 PDAM 2	Amendments to ISO 8825 to Give ISO 8825 Part 1: Basic Encoding Rules, 8 July 1991 [SC21 N 6295] (balloting ends 29 October 1991; DIS text expected December 1991, IS in October 1992)
WD 8825-1	Information Technology - Open Systems Interconnection - Specification of Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 1: Basic Encoding Rules, 8 July 1991 [SC21 N 6295]
CD 8825-2	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 2: Packed Encoding Rules, 8 July 1991 [SC21 N 6292]
CD 8825-3	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) - Part 3: Distinguished Encoding Rules, 8 July 1991 [SC21 N 6293]
WD 8825-4	Conformance Test Suite for the Presentation Protocol - Part 4: Test Suite Structure and Test Purposes for ASN.1 Encodings, SC21/WG6, July 1990 [SC21 N 5019] (CD text expected in February 1991, DIS text in November 1991, IS text in November 1992)

ISO 8831♦	Information Processing Systems - Open Systems Interconnection - Job Transfer and Manipulation (JTM) Concepts and Service, June 1989 [SC21 N 2613, January 1989]
DIS 8831.2	Information Processing Systems - Open Systems Interconnection - Job Transfer and Manipulation (JTM) Concepts and Service, June 1991 (IS second edition text expected November 1991)
ISO 8832♦	Information Processing Systems - Open Systems Interconnection - Specification of the Basic Class Protocol for Job Transfer and Manipulation (JTM), June 1989 [SC21 N 3633, January 1989]; draft Revised Edition of 12 December 1989 incorporates AD 1 [SC21 N 4183]
ISO 8832 AM 1♦	Information Processing Systems - Open Systems Interconnection - Specification of the Basic Class Protocol for Job Transfer and Manipulation, Addendum 1: JTM Full Protocol Specification, 28 May 1990 [SC21 N 5225, text with amendment incorporated; and SC21 N 5224, amendment alone] (approved 12 June 1991; IS text expected November 1991)
ISO 8859-1	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 1: Latin Alphabet No. 1, February 1987
ISO 8859-2	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 2: Latin Alphabet No. 2, February 1987
ISO 8859-3	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 3: Latin Alphabet No. 3, April 1988
ISO 8859-4	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 4: Latin Alphabet No. 4, April 1988
DIS 8859-5.2	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 5: Latin/Cyrillic Alphabet, December 1987
ISO 8859-6	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 6: Latin/Arabic Alphabet, August 1987
ISO 8859-7	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 7: Latin/Greek Alphabet, November 1987
DIS 8859-8	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 8: Latin/Hebrew Alphabet, July 1987
DIS 8859-9	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 9: Latin Alphabet No. 5, August 1988
DIS 8859-10	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets - Part 10: Latin/ Alphabet, June 21, 1991
ISO 8877♦	Information Processing Systems - Interface Connector and Contact Assignments for ISDN Basic Access Interface Located at Reference Points S and T, August 1987
ISO 8877 DAM 1	Information Processing Systems - Interface Connector and Contract Assignments for ISDN Basic Access Located at Reference Points S and T - Amendment 1: Standard ISDN Basic Access TE Connecting Cord, (awaiting second DAM ballot)
ISO 8878♦	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), September 1987 (X.223)
ISO 8878 AD 1	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Addendum 1: Protection and Priority, 15 June 1990
ISO 8878 AD 2	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Addendum 2: Use of an X.25 PVC to Provide the OSI CONS, 15 June 1990
ISO 8878 DAM 3	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Amendment 3: Conformance, (ballot closed 11 March 1990)
ISO 8878 PDAM 4	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Amendment 4: PICS Proforma, (awaiting second PDAM ballot)

ISO 8878/Cor 1	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Technical Corrigendum 1, published 1 March 1990
ISO 8878/Cor 2	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Technical Corrigendum 2, published 15 June 1990
ISO 8878/Cor 3	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Technical Corrigendum 3, awaiting publication
ISO 8879	Information Processing - Text and Office Systems - Standard Generalized Markup Language (SGML), 15 October 1986
ISO 8879 AM 1	Information Processing - Text and Office Systems - Standard Generalized Markup Language (SGML) - Amendment 1, 1 July 1988
ISO 8880-1♦	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service - Part 1: General Principles, 21 October 1988, 1990
ISO 8880-2♦	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service - Part 2: Provision and Support of the Connection-Mode Network Services, 21 October 1988, 1990
ISO 8880-2 DAM 1	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service - Part 2: Provision and Support of the Connection-Mode Network Services, Amendment 1: Addition of the ISDN Environment (awaiting DAM ballot)
ISO 8880-2 PDAM 2	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service - Part 2: Provision and Support of the Connection-Mode Network Services, Amendment 2: Addition of the PSTN and CSDN Environments (awaiting PDAM ballot)
ISO 8880-3♦	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service - Part 3: Provision and Support of the Connectionless-Mode Network Service, 21 October 1988, 1990
WD 8880-4♦	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service - Part 4: Interconnection of OSI Environments, 1989
ISO 8881.3♦	Information Processing Systems - Data Communications - Use of the X.25 Packet Level Protocol (PLP) in Local Area Networks, Third Edition, January 1989
ISO 8882-1	Information Processing Systems - X.25-DTE Conformance Testing - Part 1: General Principles, 1989
DIS 8882-1.2	Information Processing Systems - X.25-DTE Conformance Testing - Part 1: General Principles, Revised Edition (awaiting second DIS ballot)
DIS 8882-2♦	Information Processing Systems - X.25-DTE Conformance Testing - Part 2: Data Link Layer Conformance Test Suite
ISO 8882-3♦	Information Processing Systems - X.25-DTE Conformance Testing - Part 3: Packet Level Conformance Suite, Third Edition (awaiting publication)
DIS 8883	Information Processing Systems - Text Communication - Message Oriented Text Interchange System, Message Transfer Sublayer, Message Interchange Service and Message Transfer Protocol, February 1986 [WITHDRAWN, superceded by ISO 10021-6]
DIS 8884	Information Processing - Text and Office Systems - Keyboards for Multiple Latin-Alphabet Languages - Layout and Operation Using Four Levels, October 1986
ISO 8885♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format, August 1987
ISO 8885 AD 1♦	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Addendum 1: Additional Operational Parameters for the Parameter Negotiation Data Link Subfield and Definition of a Multilink Parameter Negotiation Data Link Subfield, 22 March 1988

ISO 8885 AD 2	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Addendum 2: Start/Stop Transmission, 12 March 1990
ISO 8885 DAM 3	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Amendment 3: Definition of a Private Parameter Negotiation Data Link Layer Subfield, (second DAM ballot closed 11 April 1991)
ISO 8885 DAM 4	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Amendment 4: Extended Transparency Option, (awaiting DAM ballot)
ISO 8885 DAM 5	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Amendment 5: Multi-Selective Reject, (ballot closed 17 November 1990)
ISO 8885 PDAM 6	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Amendment 6: Seven-bit Transparency Option for Start/Stop Transmission (ballot closed 10 March 1991)
ISO 8885 PDAM 7	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format - Amendment 7: Frame Check Sequence Negotiation Using the Parameter Negotiation Subfield, (ballot closed 21 August 1990)
ISO 8886.3♦	Information Processing Systems - Data Communication - Data Link Service Definition for Open Systems Interconnection, Third Edition, 1989
ISO 8907♦	Information Processing Systems - Database Language NDL, June 1987
ISO 9001-3	Quality Systems - Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software, November 1990
TR 9007	Information Processing Systems - Concepts and Terminology for the Conceptual Schema and the Information Base, July 1987
ISO 9040♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Service - Base Class, Revised Edition, April 1990 [SC21 N 4718]; 1990 Revised Edition incorporates AD 1
ISO 9040 AD 1♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Service - Addendum 1: Extended Facility Set, August 1988 [SC21 N 3006]; incorporated into 1990 Revised Edition of ISO 9040
ISO 9040 AM 2♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Service - Amendment 2: Additional Functional Units Service Specification, May 1990 [SC21 N 5030] (approved 12 June 1991; IS text expected late 1991)
ISO 9041-1♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Protocol - Basic Class, Revised Edition, April 1990 [SC21 N 4719]; 1990 Revised Edition incorporates AD 1
ISO 9041 AD 1♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Protocol - Addendum 1: Extended Facility Set, March 1989 [SC21 N 3531]; incorporated into 1990 Revised Edition of ISO 9041
ISO 9041 AM 2♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Protocol - Amendment 2: Additional Functional Units, May 1990 [SC21 N 5031] (approved 12 June 1991; IS text expected late 1991)
ISO 9041-2♦	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Protocol - Part 2: VT PICS Proforma, February 1992
DIS 9065	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) User Agent Sublayer - Interpersonal Messaging User Agent - Message Interchange Formats and Protocols, February 1986 [WITHDRAWN, superceded by ISO 10021]

ISO 9066-1.2♦	Information Processing Systems - Text Communication - Reliable Transfer (RT) - Part 1: Model and Service Definition, Second Edition, September 1989 [SC21 N 3883] (CCITT X.218)
ISO 9066-2.2♦	Information Processing Systems - Text Communication - Reliable Transfer (RT) - Part 2: Protocol Specification, Second Edition, September 1989 [SC21 N 3884] (CCITT X.228)
ISO 9067♦	Information Processing Systems - Data Communication - Automatic Fault Isolation Procedures Using Test Loops, September 1987
DIS 9068♦	Information Processing Systems - Provision of the Connectionless Network Service (CONS) Using ISO 8208, 1989
ISO 9069	Information Processing - SGML Support Facilities - SGML Document Interchange Format (SDIF), 15 September 1988
ISO 9070	Information Processing - SGML Support Facilities - Registration Procedures for Public Text Owner Identifiers, 1 February 1990
DP 9071-1.2	Text and Office Systems - Basic and Optional Requirements - Part 1: Facsimile Equipment, Second Edition, January 1987
DP 9071-2.2	Text and Office Systems - Basic and Optional Requirements - Part 2: Text Communications Terminals, Second Edition, January 1987
ISO 9072-1.2♦	Information Processing Systems - Text Communication - Remote Operations - Part 1: Model, Notation and Service Definition, Second Edition, September 1989 [SC21 N 3881] (CCITT X.219)
ISO 9072-1 PDAM 1	Information Processing Systems - Text Communication - Remote Operations - Enhancements [SC21 N 6151] (subject to Transfer of ROSE from SC18)
ISO 9072-2.2♦	Information Processing Systems - Text Communication - Remote Operations - Part 2: Protocol Specification, Second Edition, September 1989 [SC21 N 3882] (CCITT X.229)
ISO 9074♦	Estelle - A Formal Description Technique Based on an Extended State Transition Model, 15 July 1989
ISO 9074 DAM 1	Estelle - A Formal Description Technique Based on an Extended State Transition Model, Addendum 1: Estelle Tutorial, 23 May 1991 [SC21 N 5710] (ballot closes 23 November 1991; IS expected June 1992)
ISO 9075.2♦	Information Processing Systems - Database Language SQL, April 1989 (1989 text incorporates AD 1) [SC21 N 3158]
ISO 9075 AD 1	Information Processing Systems - Database Language SQL - Addendum 1: Integrity Enhancements, December 1987
DIS 9075.3♦	Information Processing Systems - Database Language SQL2, Draft Second Edition, 13 June 1991 [SC21 N 5739] (ballot closes 13 December 1991; IS status expected June 1992)
WD 9075.4♦	Information Processing Systems - Database Language SQL3 (CD text expected June 1993)
ISO 9160	Information Processing Systems - Physical Layer Interoperability Requirements, February 1988
ISO 9171-1	Information Technology: 130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 1: Unrecorded Optical Disk Cartridge, 1990
ISO 9171-2	Information Technology: 130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 1: Recording Format, 1990
DIS 9234	Industrial Asynchronous Data Link for Two-Way Simultaneous or Two-Way Alternate Mode, 1989
ISO 9241-1	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 1: Introduction
ISO 9241-2	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 2: Task Requirements

DIS 9241-3	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 3: Visual Display Requirements
DIS 9241-4	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 4: Keyboard Requirements
CD 9241-5	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 5: Workstation Layout and Postural Requirements
CD 9241-6	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 6: Environmental Requirements
CD 9241-7	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 7: Display Requirements with Reflections
CD 9241-8	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 8: Requirements for Displayed Colors
CD 9241-9	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 9: Requirements for Non-Keyboard Input Devices
WD 9241-10	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 10: Dialogue Principles
CD 9241-11	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 11: Usability Statements
CD 9241-12	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 12: Presentation of Information
WD 9241-13	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 13: User Guidance
CD 9241-14	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 14: Menu Dialogues
WD 9241-15	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 15: Command Dialogues
WD 9241-16	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 16: Direct Manipulation Dialogues
WD 9241-17	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 17: Form-Filling Dialogues
XX 9241-18	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 18: Question and Answer Dialogues (not yet started)
XX 9241-19	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 19: Natural Language Dialogues (not yet started)
DIS 9281	Information Processing Systems - Identification of Picture Coding Methods, May 1987
DIS 9282-1	Information Processing Systems - Coded Representation of Pictures - Part 1: Encoding Principles for Picture Representation in a 7- or 8-Bit Environment, May 1987
DIS 9282-2	Information Processing Systems - Coded Representation of Pictures - Part 2: Encoding Principles for Photographic Images, 1987
TR 9294	Information Processing - Guidelines for the Management of Software Documentation, Technical Report Type 3, 1990
ISO 9314-1♦	Information Processing Systems - Fibre Distributed Data Interface (FDDI) - Part 1: Physical Layer Protocol (PHY), 1989
ISO 9314-2♦	Information Processing Systems - Fibre Distributed Data Interface (FDDI) - Part 2: Media Access Control (MAC), 1989
ISO 9314-3	Interconnection of Equipment - Fibre Distributed Data Interface (FDDI) - Part 3: Physical Layer Medium Dependent (PMD), 1 August 1990
CD 9314-4	Interconnection of Equipment - Fibre Distributed Data Interface (FDDI) - Part 4: Single Mode Fiber/Physical Layer Medium Dependent Physical Connectors
CD 9314-5	FDDI-Part 5: Hybrid Ring Control (FDDI-II), 24 May 1990

DP 9314-6	FDDI-Part 6: Station Management (SMT) Standard
DIS 9316	Information Processing Systems - Small Computer System Interface (SCSI), July 1987
DIS 9318-1	Information Processing Systems - Intelligent Peripheral Interface - Part 1: Physical Level, August 1987
ISO 9318-2	Information Processing Systems - Intelligent Peripheral Interface - Part 2: Device Specific Command Set for Magnetic Disk Drives, 1990
ISO 9318-3	Information Processing Systems - Intelligent Peripheral Interface - Part 3: Device Generic Command Set for Magnetic and Optical Disk Drives, 1990
ISO 9318-4	Information Processing Systems - Intelligent Peripheral Interface - Part 4: Device Generic Command Set for Magnetic Tape Drives, 1990
DIS 9324	Information Processing - Storage Module Interfaces, September 1988
ISO 9496.2	Information Processing - Programming Languages - CCITT High Level Language (CHILL), August 1989 (CCITT Z.200)
ISO 9506-1♦	Industrial Automation Systems - Systems Integration and Communications - Manufacturing Message Specification - Part 1: Service Definition, 1990
ISO 9506-2♦	Industrial Automation Systems - Systems Integration and Communications - Manufacturing Message Specification - Part 2: Protocol Specification, 1990
DIS 9541-1	Information Processing Systems - Font and Character Information Exchange - Part 1: Introduction, (second DIS ballot closed 17 November 1990)
ISO 9541-2	Information Processing Systems - Font and Character Information Exchange - Part 2: Registration and Naming Procedures, 1991
DIS 9541-3	Information Processing Systems - Font and Character Information Exchange - Part 3: Character Identification Method, 20 October 1991
DIS 9541-4	Information Processing Systems - Font and Character Information Exchange - Part 4: Character Collections, December 1987
DIS 9541-5	Information Processing Systems - Font and Character Information Exchange - Part 5: Font Attributes and Character Model, December 1987
DIS 9541-6	Information Processing Systems - Font and Character Information Exchange - Part 6: Font and Character Attribute Subsets and Application, December 1987
DP 9541-7	Information Processing Systems - Font and Character Information Exchange - Part 7: Font Interchange Format, May 1987
ISO 9542♦	Information Processing Systems - Data Communications - End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service, Revised Edition, 1989
ISO 9542/Cor 1	Information Processing Systems - Data Communications - End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service, Revised Edition, 1989, Technical Corrigendum 1 (awaiting publication)
ISO 9542 PDAM 1	Information Processing Systems - Data Communications - End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service, Amendment 1: Dynamic Discovery of OSI NSAP Addresses by End Systems (New Work Item)
ISO 9543♦	Information Processing Systems - Information Exchange Between Systems - Synchronous Transmission Signal Quality at DTE/DCE Interfaces, May 1989
DTR 9544	Information Processing - Computer-Assisted Publishing - Vocabulary, December 1986
ISO 9545♦	Information Processing Systems - Open Systems Interconnection - Application Layer Structure (ALS), December 1989 [SC21 N 3825, August 1989]
ISO 9545 DAM 1♦	Information Processing Systems - Open Systems Interconnection - Application Layer Structure (ALS), Amendment 1: Extended Application Layer Structures (XALS), July 1991 [SC21 N 6301, July 1991] (AM expected in June 1994)

ISO 9545 WDAM 2	Information Processing Systems - Open Systems Interconnection - Application Layer Structure (ALS), Amendment: Connectionless Mode Transmission, June 1988 [SC21 N 2470] (PDAM expected late 1991)
TR 9547	Programming Language Processors - Test Methods - Guidelines for Their Development and Acceptability, April 1988
ISO 9548♦	Information Processing Systems - Open Systems Interconnection - Session Connectionless Protocol to Provide the Connectionless-Mode Session Service, August 1989 [SC21 N 3460]
DIS 9548–2	Information Processing Systems - Open Systems Interconnection - Session Connectionless Protocol to Provide the Connectionless-Mode Session Service - Part 2: PICS Proforma, 7 October 1991 (IS expected December 1992)
ISO 9549	Information Processing Systems - Galvanic Isolation of Balanced Interchange Circuits, 15 October 1990
TR 9571♦	Information Processing Systems - Open Systems Interconnection - LOTOS Description of the Session Service, 15 September 1989 [SC21 N 3149, 25 January 1989]
TR 9572♦	Information Processing Systems - Open Systems Interconnection - LOTOS Description of the Session Protocol, 15 September 1989 [SC21 N 3148, 25 January 1989]
TR 9573	Information Processing - SGML Support Facilities - Techniques for Using SGML, 1 December 1988
ISO 9574♦	Information Processing Systems - Data Communications - Provision of the OSI Connection-Mode Network Service (CONS) by Packet Mode Terminal Equipment Connected to an Integrated Services Digital Network (ISDN), May 1988
ISO 9574 DAM 1	Information Processing Systems - Data Communications - Provision of the OSI Connection-Mode Network Service (CONS) by Packet Mode Terminal Equipment Connected to an Integrated Services Digital Network (ISDN) - Amendment 1: Provision of the CONS on an ISDN Circuit-Switch Channel Connecting Directly to the Remote Terminal (awaiting DAM ballot)
TR 9575	OSI Routing Framework, 1 June 1990
ISO 9576-1♦	Information Technology - Open Systems Interconnection - Presentation Protocol to Provide the Connectionless-Mode Presentation Service, 1 July 1990 [SC21 N 4934]
DIS 9576–2♦	Information Technology - Open Systems Interconnection - Presentation Protocol to Provide the Connectionless-Mode Presentation Service - Part 2: PICS Proforma for Connectionless Presentation Protocol, 4 July 1991 [SC21 N 5930] (balloting ended 4 January 1991; IS expected February 1992)
TR 9577♦	Protocol Identification in the OSI Network Layer, 15 October 1990
TR 9578♦	Communication Interface Connectors Used in Local Area Networks, 24 May 1990
DIS 9579-1♦	Information Technology - Database Languages - Remote Database Access (RDA) - Part 1: Generic Model, Service and Protocol, July 1991 [SC21 N 6375, 30 August 1991] (IS expected in 1992)
DIS 9579-1 WDAM 1	Amendment 1 (PDAM expected June 1992)
DIS 9579-2♦	Information Technology - Database Languages - Remote Database Access (RDA) - Part 2: SQL Specialization, July 1991 [SC21 N 6376, 30 August 1991] (IS expected in 1992)
DIS 9579-2 WDAM 1	Information Technology - Database Languages - Remote Database Access (RDA) - Part 2: SQL Specialization, Amendment 1: Support for SQL 2, 29 March 1990 (PDAM text expected June 1993)
ISO 9592-1	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 1: Functional Description, May 1989

ISO 9592-1 AM 1	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 1: Functional Description, Amendment 1: PHIGS Plus Support
ISO 9592-2	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 2: Archive File Format, May 1989
ISO 9592-2 AM 1	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 2: Archive File Format, Amendment 1: PHIGS Plus Support
ISO 9592-3	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 3: Clear-Text Encoding of Archive File, May 1989
ISO 9592-3 AM 1	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 3: Clear-Text Encoding of Archive File, Amendment 1: PHIGS Plus Support
ISO 9592-4	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 4: PHIGS Plus (ballot closed 1 September 1990) [SC24 N 224]
ISO 9593-1	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 1: FORTRAN Binding, 22 August 1990
DIS 9593-2	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 2: Extended Pascal, (awaiting DIS ballot)
ISO 9593-3	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 3: Ada, 16 July 1990
DIS 9593-4	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings - Part 4: C, (ballot closes 21 March 1991)
ISO 9594-1♦	Information Processing Systems - Open Systems Interconnection - The Directory - Part 1: Overview of Concepts, Models and Services, December 1990 [SC21 N 4701] (CCITT X.500)
ISO 9594-1 PDAM 1.2	Information Processing Systems - Open Systems Interconnection - The Directory - Part 1: Overview of Concepts, Models and Services, Amendment 1: Replication, Schema and Access Control, 15 May 1991 [SC21 N 5942] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)
ISO 9594-2♦	Information Processing Systems - Open Systems Interconnection - The Directory - Part 2: Models, December 1990 [SC21 N 4702] (CCITT X.501)
ISO 9594-2 PDAM 1.3	Information Processing Systems - Open Systems Interconnection - The Directory - Part 2: Models, Amendment 1: Access Control, 16 May 1991 [SC21 N 5952] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)
ISO 9594-2 PDAM 2.2	Information Processing Systems - Open Systems Interconnection - The Directory - Part 2: Models, Amendment 2: Schema Extensions, 16 May 1991 [SC21 N 5943] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)
ISO 9594-2 PDAM 3.2	Information Processing Systems - Open Systems Interconnection - The Directory - Part 2: Models, Amendment 3: Replication, 16 May 1991 [SC21 N 5944] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)
ISO 9594-3♦	Information Processing Systems - Open Systems Interconnection - The Directory - Part 3: Abstract Service Definition, December 1990 [SC21 N 4703] (CCITT X.511)
ISO 9594-3 PDAM 1.3	Information Processing Systems - Open Systems Interconnection - The Directory - Part 3: Abstract Service Definition, Amendment 1: Access Control,

16 May 1991 [SC21 N 5953] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-3 PDAM 2.2 Information Processing Systems - Open Systems Interconnection - The Directory - Part 3: Abstract Service Definition, Amendment 2: Replication, Schema and Enhanced Search, 16 May 1991 [SC21 N 5945] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-4♦ Information Processing Systems - Open Systems Interconnection - The Directory - Part 4: Procedures for Distributed Operations, December 1990 [SC21 N 4704] (CCITT X.518)

ISO 9594-4 PDAM 1.3 Information Processing Systems - Open Systems Interconnection - The Directory - Part 4: Procedures for Distributed Operations, Amendment 1: Access Control, 16 May 1991 [SC21 N 5954] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-4 PDAM 2.2 Information Processing Systems - Open Systems Interconnection - The Directory - Part 4: Procedures for Distributed Operations, Amendment 2: Replication, Schema and Enhanced Search, 16 May 1991 [SC21 N 5946] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-5♦ Information Processing Systems - Open Systems Interconnection - The Directory - Part 5: Protocol Specifications, December 1990 [SC21 N 4705] (CCITT X.519)

ISO 9594-5 PDAM 1.2 Information Processing Systems - Open Systems Interconnection - The Directory - Part 5: Protocol Specifications, Amendment 1: Replication, 16 May 1991 [SC21 N 5947] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-6♦ Information Processing Systems - Open Systems Interconnection - The Directory - Part 6: Selected Attribute Types, December 1990 [SC21 N 4706] (CCITT X.520)

ISO 9594-6 PDAM 1.2 Information Processing Systems - Open Systems Interconnection - The Directory - Part 6: Selected Attribute Types, Amendment 1: Schema Extensions, 16 May 1991 [SC21 N 5946] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-7♦ Information Processing Systems - Open Systems Interconnection - The Directory - Part 7: Selected Object Classes, December 1990 [SC21 N 4707] (CCITT X.521)

ISO 9594-7 PDAM 1.2 Information Processing Systems - Open Systems Interconnection - The Directory - Part 7: Selected Object Classes, Amendment 1: Schema Extensions, 16 May 1991 [SC21 N 5946] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

ISO 9594-8♦ Information Processing Systems - Open Systems Interconnection - The Directory - Part 8: Authentication Framework, December 1990 [SC21 N 4708] (CCITT X.509)

ISO 9594-8 PDAM 1.2 Information Processing Systems - Open Systems Interconnection - The Directory - Part 8: Authentication Framework, Amendment 1: Access Control, 16 May 1991 [SC21 N 5955] (balloting ends 3 September 1991; DIS text expected in November 1991, IS in October 1992)

CD 9594-9.2 Information Technology - Open Systems Interconnection - The Directory - Part 9: Replication, 14 May 1991 [SC21 N 5951]

WD 9594-10♦ Information Technology - Open Systems Interconnection - The Directory - Part 10: Directory PICS Proforma, July 1990 [SC21 N 4913] (CD text expected in June 1992, DIS text in June 1993, and IS text in June 1994)

WD 9594-X♦ Information Technology - Open Systems Interconnection - The Directory - Part X: Text Suite Structure and Test Purposes and Abstract Test Suite for the OSI Directory, August 1990 [SC21 N 4951] (NWI not accepted]

WD 9594-Y♦ Information Technology - Open Systems Interconnection - The Directory - Part Y: Replication and Knowledge Management, July 1990 [SC21 N 4913] (CD text expected November 1991)

ISO 9595:1991(E) Information Technology - Open Systems Interconnection - Common Management Information Service (CMIS) Definition, CCITT X.710, April 1991 [SC21 N 5302] (April 1991 edition incorporates AD 1 and AD 2)

ISO 9595 PDAM 3	Information Technology - Open Systems Interconnection - Common Management Information Service (CMIS) Definition, Amendment 3: Support of Allomorphism, 26 November 1990 [SC21 N 4966] (PDAM expected June 1993, IS in March 1994, IS in March 1995)
ISO 9595 DAM 4♦	Information Technology - Open Systems Interconnection - Common Management Information Service (CMIS) Definition, Amendment 4: Access Control, 8 July 1991 [SC21 N 6286] (IS status expected in June 1992)
ISO 9595 WDAM 5♦	Information Technology - Open Systems Interconnection - Common Management Information Service (CMIS) Definition, Amendment 5: Enhanced Functionality, July 1991 [SC21 N 6039] (PDAM expected in 1993)
ISO 9596-1:1991(E)	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) Specification,CCITT X.711, April 1991 [SC21 N 5303] (April 1991 edition incorporates AD 1 and AD 2)
ISO 9596 PDAM 3♦	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) Specification, Amendment 3: Support of Allomorphism, July 1990 [SC21 N 4967] [JTC1 N 761] (CD text expected June 1993) (PDAM expected June 1993, IS in March 1994, IS in March 1995)
ISO 9596 PDAM 4♦	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) Specification, Amendment 4: State Table, January 1990 [SC21 N 4058] (new work item June 1990; terminated June 1991)
ISO 9596 WDAM 5♦	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) Specification, Amendment 5: Enhanced Functionality, July 1991 [SC21 N 6039] (PDAM expected in 1993)
DIS 9596-2♦	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) Specification, Part 2: PICS Proforma, 8 July 1991 [SC21 N 6287] (CCITT X.712) (IS status expected June 1992)
DIS 9636-1	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 1: Overview, Profiles, and Conformance, (ballot closed 8 September 1990)
DIS 9636-2	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 2: Control, Negotiation, and Errors, (ballot closed 8 September 1990), IS status expected June 1992
DIS 9636-3	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 3: Output and Attributes, (ballot closed 8 September 1990)
DIS 9636-4	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 4: Segmentation, (ballot closed 8 September 1990)
DIS 9636-5	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 5: Input and Echoing, (ballot closed 8 September 1990)
DIS 9636-6	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 6: Raster, (ballot closed 8 September 1990)
WD 9636-8	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 8: FORTRAN Language Binding of CGI, 1989
WD 9636-11	Information Processing Systems - Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification - Part 11: C Language Binding of CGI, 1989
DIS 9637-1	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 1: Character Encoding (review period ends 19 November 1991)

DIS 9637-2 Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 2: Binary Encoding, November 4, 1991

DIS 9637-3 Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 3: Clear Text Encoding

DIS 9638-1 Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 1: FORTRAN

DIS 9638-2 Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 2: Pascal

DIS 9638-3 Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 3: Ada

DIS 9638-4 Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings - Part 4: C (review period ends 10 September 1991)

ISO 9646-1.2♦ Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 1: General Concepts, Second Edition, May 1991 [SC21 N 5865] (CCITT X.290)

ISO 9646-1 PDAM 1 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 1: General Concepts, Amendment 1: Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6173] (DIS text expected March 1992; IS in December 1992)

ISO 9646-1 PDAM 2 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 1: General Concepts, Amendment 2: Multi-Party Testing Methodology, June 1991 [SC21 N 6178] (DIS text expected March 1992; IS in December 1992)

ISO 9646-2.2♦ Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 2: Abstract Test Suite Specification (Excluding Annexes E and F on TTCN), May 1991 [SC21 N 5867]

ISO 9646-2 Annex Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 2: Abstract Test Suite Specification, Annex: Guidelines for PICS Proformas [SC6 N 6243]

ISO 9646-2 PDAM 1 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 2: Abstract Test Suite Specification, Amendment 1: Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6174] (DIS text expected March 1992; IS in December 1992)

ISO 9646-2 PDAM 2 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 2: Abstract Test Suite Specification, Amendment 2: Multi-Party Testing Methodology, June 1991 [SC21 N 6179] (DIS text expected March 1992; IS in December 1992)

ISO 9646-3♦ Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 3: The Tree and Tabular Combined Notation (TTCN), October 1991

ISO 9646-3 PDAM 1 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 3: The Tree and Tabular Combined Notation (TTCN), Addendum 1: TTCN Extensions, November 1991 [SC21 N 6666] (DAM expected June 1992, AM June 1993)

ISO 9646-3 WDAM 2 Addendum 2: Further TTCN Extensions, 26 November 1991 [SC21 N 6641]

ISO 9646-4♦ Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 4: Test Realization, May 1991 [SC21 N 5869]

ISO 9646-4 PDAM 1 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 4: Test Realization, Amendment 1: Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6175] (DIS text expected March 1992; IS in December 1992)

ISO 9646-4 PDAM 2 Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 4: Test Realization, Amendment 2: Multi-Party Testing Methodology, June 1991 [SC21 N 6181] (DIS text expected March 1992; IS in December 1992)

ISO 9646-5♦	Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process, May 1991 [SC21 N 5871]
ISO 9646-5 PDAM 1	Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process, Amendment 1: Protocol Profile and Multi-Protocol Testing, June 1991 [SC21 N 6176] (DIS text expected March 1992; IS in December 1992)
ISO 9646-5 PDAM 2	Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process, Amendment 2: Multi-Party Testing Methodology, June 1991 [SC21 N 6182] (DIS text expected March 1992; IS in December 1992)
CD 9646-6	Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 6: Protocol Profile Test Specification, June 1991 [SC21 N 6177] (DIS text expected March 1992; IS in December 1992)
WD 9646-7	Information Processing Systems - OSI Conformance Testing Methodology and Framework - Part 7: Requirements and Guidelines on Implementation Conformance Statement (ICS) and ICS Proformas, June 1991 (new work item) (CD expected June 1992)
ISO 9660	Information Processing - Volume and File Structure of CD-ROM for Information Exchange, April 1988
ISO 9735	Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application Level Syntax Rules, July 1988
ISO 9796	Information Processing - Digital Signature Scheme Giving Message Recovery, 1991
ISO 9797	Information Processing - Data Cryptographic Techniques - Data Integrity Mechanisms Using a Cryptographic Check Function Employing a Block Cypher Algorithm, 1989
ISO 9798-1	Information Processing - Entity Authentication Mechanisms - Part 1: General Model, 1991
DP 9798-2	Information Processing - Entity Authentication Mechanisms - Part 2: Entity Authentication Mechanisms Using Symmetric Algorithms
ISO 9804♦	Information Processing Systems - Open Systems Interconnection - Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, July 1990 [SC21 N 4611, 20 April 1990] (CCITT X.237)
ISO 9804 WDAM 1♦	Information Processing - Open Systems Interconnection - Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, Amendment 1: Enhancements, 4th working draft, 1 October 1991 [SC21 N 6433] (DIS text expected March 1993, IS in March 1994)
ISO 9804 PDAM 2	Information Processing - Open Systems Interconnection - Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, Amendment 2: Session Mapping Changes (Additional Resynchronization Functionality), 10 July 1991 [SC21 N 5925] (IS text expected in March 1992)
ISO 9804 WDAM 3♦	Information Processing - Open Systems Interconnection - Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, Amendment 3: Restart (CD text expected May 1992)
ISO 9805♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol, July 1990 [SC21 N 4612, 20 April 1990] (CCITT X.247)
ISO 9805 WDAM 1♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol, Amendment 1: Enhancements, 4th working draft, 24 September 1991 [SC21 N 6429] (DIS text expected March 1993, IS text March 1994)
ISO 9805 PDAM 2	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service

	Element, Amendment 2: Session Mapping Changes (Additional Resynchronization Functionality), 10 July 1991 [SC21 N 5926] (IS text expected in March 1992)
ISO 9805 WDAM 3♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol, Amendment 3: Restart (CD text expected May 1992, DIS in May 1993, IS in May 1994)
CD 9805-2.2♦	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol - Part 2: CCR PICS Proforma, August 1991 [SC21 N 6332] (DIS text expected November 1991, IS text November 1992)
ISO 9834-1	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part 1: General Procedures, March 1990 [SC21 N 4352] (ballot closed 2 February 1991;, July 1991 editing meeting recommended progression to IS)
ISO 9834-2♦	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part 2: Registration Procedures for OSI Document Types, November 1990 [SC21 N 5275] (approved 12 June 1991; IS text expected in late 1991)
ISO 9834-3	Information Technology - Open Systems Interconnection - Procedures for OSI Registration Authorities - Part 3: Procedures for Specific Registration of Joint Object Identifier Component Values for Joint ISO-CCITT Use, 27 September 1990 [SC21 N 4718, April 1990]
ISO 9834-4	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities - Part 4: Register of VTE Profiles, 1 November 1991 [SC21 N 6541]
ISO 9834-5♦	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part 5: Register of VT Control Objects Identifiers, 1 November 1991 [SC21 N 6543]
DIS 9834-6♦	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part 6: Registration Authority Procedures for Application Process Titles and Application Entity Titles, September 1990 [SC21 N 5218, July 1990] (DIS ballot failed 25 April 1991)
WD 9834-B	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part B: Registration of Abstract Syntaxes, 1990
WD 9834-C	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part C: Registration of Transfer Syntaxes, 1990
WD 9834-D	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part D: Registration of Application Contexts, 1990 (work suspended by SC21, November 1989)
WD 9834-E	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part E: Registration of System Titles, 1990 (will probably be incorporated in OSI management standards)
WD 9834-F	Information Technology - Open Systems Interconnection - Procedures for Specific OSI Registration Authorities - Part F: Registration of Authentication Mechanisms, 1990 (WITHDRAWN; cancelled by SC21, November 1989)
ISO 9899	Programming Languages - C, 1990
ISO 9945-1	Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Interface, 1990
DP 9945-1.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.1: Language Independent Base (WG15 work item based on IEEE P1003.1c)
DP 9945-1.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.2: Real-time and Extensions (WG15 work item based on IEEE P1003.4 and .1b)
DP 9945-1.3	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3: Distribution Services (WG15 work item based on IEEE P1003.8)

DP 9945-1.3.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.1: Transparent File Access (WG15 work item based on IEEE P1003.8)
DP 9945-1.3.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.2: Remote Procedure Call (WG15 work item based on IEEE P1237)
DP 9945-1.3.3	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.3: Transport Interface (WG15 work item based on IEEE P1003.11)
DP 9945-1.3.4	Portable Operating System Interface for Computer Environments (POSIX) - Part 1.3.4: Name Space/Directory Services (WG15 work item based on IEEE P1003.12)
DP 9945-2	Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities, 1990 [failed registration ballot; new draft requested for registration (on hold)]
DP 9945-2.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 2.1: Shell and Utilities (WG15 work item based on IEEE P1003.2)
DP 9945-2.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 2.2: User Portability Extensions (WG15 work item based on IEEE P1003.2a)
DP 9945-3	Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Management
DP 9945-3.1	Portable Operating System Interface for Computer Environments (POSIX) - Part 3.1: General Services ((WG15 work item based on IEEE P1003.7)
DP 9945-3.2	Portable Operating System Interface for Computer Environments (POSIX) - Part 3.2: Batch Services ((WG15 work item based on IEEE P1003.10)
TR 9973	Registration of Graphical Items, 1989
ISO 9979	Information Processing - Data Encipherment - Procedures for the Registration of Cryptographic Algorithms, July 1990 [SC27 N 88]
DIS 9995-1	Information Technology, Keyboard Layouts for Text and Office Systems, Part 1: General Principles Governing Keyboard Layouts, November 4, 1991
DIS 9995-2	Information Technology, Keyboard Layouts for Text and Office Systems, Part 2: Alphanumeric Section, November 4, 1991
DIS 9995-3	Information Technology, Keyboard Layouts for Text and Office Systems, Part 3: Common Secondary Layout of Alphanumeric Zone of Alphanumeric Section, November 4, 1991
DIS 9995-4	Information Technology, Keyboard Layouts for Text and Office Systems, Part 4: Principles Governing the Placement of Characters and Symbols on Keys, November 4, 1991
DIS 9995-5	Information Technology, Keyboard Layouts for Text and Office Systems, Part 5: Editing Section, November 4, 1991
DIS 9995-6	Information Technology, Keyboard Layouts for Text and Office Systems, Part 6: Functional Section, November 4, 1991
DIS 9995-7	Information Technology, Keyboard Layouts for Text and Office Systems, Part 7: Symbols Used to Represent Functions, November 4, 1991
TR 10000-1♦	Information Technology - Framework of International Standardized Profiles (ISPs) - Part 1: Taxonomy Framework, [SGFS N 184. 9 February 1990], 16 July 1990
TR 10000-2♦	Information Technology - Framework of International Standardized Profiles (ISPs) - Part 2: Taxonomy of Profiles, [SGFS N 185. 9 February 1990], 16 July 1990
DTR 10000-2.2(E)	Information Technology - Framework of International Standardized Profiles (ISPs) - Part 2: Taxonomy of Profiles, 28 June 1991 [SGFS N 384]
ISO 10021-1♦	Information Processing - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 1: System and Service Overview, June 1988 (see CCITT X.400), 1990
ISO 10021-2♦	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 2: Overall Architecture, June 1988 (see CCITT X.402), 1990

ISO 10021-3♦	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 3: Abstract Service Definition Conventions, June 1988 (see CCITT X.407), 1990
ISO 10021-4♦	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures, June 1988 (see CCITT X.411), 1990
ISO 10021-5♦	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 5: Message Store: Abstract Service Definition, June 1988 (see CCITT X.412), 1990
ISO 10021-6♦	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 6: Protocol Specifications, June 1988 (see CCITT X.419), 1990
ISO 10021-7♦	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) - Part 7: Interpersonal Messaging System, June 1988 (see CCITT X.420), 1990
ISO 10022♦	Information Processing Systems - Open Systems Interconnection - Physical Service Definition, (CCITT X.211), 1 August 1990
PDTR 10023♦	Telecommunications and Information Exchange Between Systems - A Formal Description of ISO 8072 in LOTOS, March 1988 (awaiting decision concerning further progression)
CD 10024♦	Telecommunications and Information Exchange Between Systems - A Formal Description of ISO 8073 in LOTOS, April 1988
DIS 10025-1♦	Information Processing Systems - Transport Conformance Testing for Connection Oriented Transport Protocol Operating Over the Connection Oriented Network Service (CONS) - Part 1: General Principles, 1989
CD 10025-2♦	Information Processing Systems - Transport Conformance Testing for Connection Oriented Transport Protocol Operating Over the Connection Oriented Network Service (CONS) - Part 2: Test Suite Structure and Test Principles, 1989
DP 10025-3♦	Information Processing Systems - Transport Conformance Testing for Connection Oriented Transport Protocol Operating Over the Connection Oriented Network Service (CONS) - Part 3: Abstract Test Suite Specification, 1989
DIS 10026-1.2♦	Distributed Transaction Processing (TP) - Part 1: Model, July 1991 [SC21 N 5671] (text is considered stable, but a second DIS was issued)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Security, WDAMs, July 1991 [SC21 N 6232] (CD text expected June 1992)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Association Management, WDAMs, July 1991 [SC21 N 6233] (CD text expected June 1992)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Heuristic Decisions, WDAMs, January 1990 [SC21 N 4167] (inactive; target dates dependent on national body input)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Commitment Optimization, WDAMs, July 1991 [SC21 N 6239] (CD text expected in November 1992, DIS in November 1993, IS in November 1994)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Distributed Transaction Processing Dialogue Recovery and User Suspension of a Dialogue, WDAMs, July 1990 [SC21 N 6235] (CD text expected June 1992, DIS in June 1993, IS in June 1994)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Distributed Transaction Processing Savepoints, January 1990 [SC21 N 4171] (new work item; not accepted by JTC1, June 1990)
DIS 10026-1/3	Draft Amendments to Parts 1-3: Transaction Processing Sub-Transactions, SC21/WG5, WDAMs, July 1991 [SC21 N 6236] (formal WD text expected June 1992, CD text in June 1993, DIS in June 1994, IS in June 1995)
DIS 10026-1/4	Draft Amendments to Parts 1-3: Transaction Processing Separate Data and Commit Associations, WDAMs, July 1991 [SC21 N 6240] (formal WD text expected June 1992, CD text in June 1993, DIS in June 1994, IS in June 1995)

DIS 10026-2.2♦ Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 2: Service Definition, July 1991 [SC21 N 5673] (text is considered stable, but a second DIS was issued)

DIS 10026-2.2 WDAM 1 Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 2: Service Definition, Amendment 1: Commit Optimizations, February 1991 [SC21 N 5187]

DIS 10026-3.2♦ Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 3: Transaction Processing Protocol Specification, 15 November 1991 [SC21 N 5675]

DIS 10026-3.2 WDAM 1 Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 3: Transaction Processing Protocol Specification, Amendment 1: Commit Optimizations, February 1991 [SC21 N 5187]

CD 10026-4.2 Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 4: PICS Proforma, SC21/WG5, October 1991 [SC21 N 6476] (DIS expected in June 1992, IS in June 1993)

CD 10026-5 Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 5: Application Context Proforma, SC21/WG5, July 1990 [SC21 N 5160] [JTC1 N 774] (CD ballot closed 9 July 1991; DIS text expected October 1991, IS in October 1992)

CD 10026-6 Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 6: Unstructured Data Transfer, July 1991 [SC21 N 6222, 23 August 1991; JTC1 N 775] (DIS text expected in October 1991, IS in October 1992)

WD 10026-z Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing (TP) - Part 7: Other Data Transfer, January 1990 [SC21 N 4166] (new work item; CD text expected November 1992]

ISO 10027 Information Technology - Information Resource Dictionary System (IRDS) Framework, June 1990 [SC21 N 4727, 2 May 1990]

DIS 10028-1♦ Definition of the Relaying Functions of a Network Layer Intermediate System, Part 1: Connection-mode Network Service (awaiting DIS ballot)

CD 10028-2♦ Definition of the Relaying Functions of a Network Layer Intermediate System, Part 2: Connectionless Network Service (awaiting CD ballot)

TR 10029♦ Information Processing Systems - Data Communications - Operation of an X.25 Interworking Unit, 15 March 1989

ISO 10030–1 Information Processing Systems - Open Systems Interconnection - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP) [SC6 N 5006], 11 October 1990

ISO 10030-1 PDAM 1 Information Processing Systems - Open Systems Interconnection - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP), Amendment 1: Dynamic Discovery of OSI NASP Addresses by End Systems (New Work Item)

ISO 10030-1 PDAM 3 Information Processing Systems - Open Systems Interconnection - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP), Amendment 3: Specification of IS-SNARE Interactions (ballot closed 8 February 1991)

CD 10030-2 Information Processing Systems - Open Systems Interconnection - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP), Part 2: PICS Proforma (awaiting CD ballot)

ISO 10031-1 Information Processing - Text Communication - Distributed-Office-Applications Model (DOAM) - Part 1: General Model, 1991

ISO 10031-2 Information Processing - Text Communication - Distributed-Office-Applications Model (DOAM) - Part 2: Referenced Data Transfer, 1991

DIS 10032♦ Information Technology - Reference Model of Data Management, 13 May 1991 [SC21 N 5991] (balloting ends 4 January 1992)

DP 10033	Information Processing - Text and Office Systems - Recording of Documents Conforming to ISO 8613 on Flexible Disk Cartridges Conforming to ISO 9293, May 1988
DTR 10034	Guidelines for the Preparation of Conformity Clauses in Programming Language Standards (Technical Report, Type 3), July 1988
ISO 10035♦	Information Processing Systems - Open Systems Interconnection Connectionless ACSE Protocol Specification, 1 June 1990 [SC21 N 4938]
WD 10035-2	Information Processing Systems - Open Systems Interconnection Connectionless ACSE Protocol Specification - Part 2: PICS Proforma for Connectionless ACSE Protocol, July 1989 [SC21 N 3218] (CD text possible in June 1991)
DIS 10036	Procedure for Registration of Glyph and Glyph Collection Identifiers (ballot closed 17 November 1990)
TR 10037	Information Processing - SGML and Text-Entry Systems - Guidelines for SGML Syntax-Directed Editing Systems, (awaiting publication)
DIS 10038♦	Information Processing Systems - Local Area Networks - MAC Sublayer Interconnection (MAC Bridging), (awaiting DIS ballot)
DIS 10038 PDAM 1	Information Processing Systems - Local Area Networks - MAC Sublayer Interconnection (MAC Bridging), Amendment 1: Specification of Management Information for CMIP (awaiting PDAM ballot)
DIS 10038 PDAM 2	Information Processing Systems - Local Area Networks - MAC Sublayer Interconnection (MAC Bridging), Amendment 2: Source Routing Supplement (ballot closed 7 March 1991)
ISO 10039♦	Information Processing Systems - Local Area Networks - MAC Service Definition, 26 October 1990
ISO 10040♦	Information Processing Systems - Open Systems Interconnection - Systems Management Overview, August 1991 [SC21 N 6353, September 1991] (CCITT X.701)
ISO 10116	Information Processing - Modes of Operation for an N-bit Block Cipher Algorithm, 1991 [SC27 N 86, 1989]
DIS 10148	Information Processing Systems - Basic Remote Procedure Call (RPC) Using OSI Remote Operations, 9 March 1989 [SC21 N 3463; fast-track ballot failed; DIS 10148 WITHDRAWN; proposal for new work item, SC21 N 4153, January 1990] (WG6 has requested authorization to progress to CD status) [SC21 N 6111, third working draft, 25 June 1991]
DIS 10149	Information Processing Systems - Data Interchange on Read-Only 120-mm Optical Data Disks (CD-ROM), August 1988
ISO 10164-1♦	Information Technology - Open Systems Interconnection - Systems Management - Part 1: Object Management Function, October 1991 [SC21 N 6355]
ISO 10164-2♦	Information Technology - Open Systems Interconnection - Systems Management - Part 2: State Management Function, October 1991 [SC21 N 6356]
ISO 10164-3♦	Information Technology - Open Systems Interconnection - Systems Management - Part 3: Attributes for Representing Relationship, October 1991 [SC21 N 6357]
ISO 10164-4♦	Information Technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Reporting Function, October 1991 [SC21 N 4858, September 1990]
ISO 10164-5♦	Information Technology - Open Systems Interconnection - Systems Management - Part 5: Event Report Management Function, October 1991 [SC21 N 4860, September 1990] (name changed from Management Service Control Function)
ISO 10164-6♦	Information Technology - Open Systems Interconnection - Systems Management - Part 6: Log Control Function, October 1991 [SC21 N 4862, September 1990]
ISO 10164-7♦	Information Technology - Open Systems Interconnection - Systems Management - Part 7: Security Alarm Reporting Function, October 1991 [SC21 N 6367]
DIS 10164-8	Information Technology - Open Systems Interconnection - Systems Management - Part 8: Security Audit Trail Function, 8 July 1991 [SC21 N 6283] (CCITT X.740) (IS status expected in June 1992)

CD 10164-9.2	Information Technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control, 11 October 1991 [SC21 N 5764] (second CD ballot failed October 1991) (CCITT X.741) (cannot progress to DIS until CD 10181-3 on access control framework is issued) (IS status expected December 1992)
CD 10164-10.2	Information Technology - Open Systems Interconnection - Systems Management - Part 10: Accounting Meter Function, July 1991 [SC21 N 6296, 24 July 1991] (DIS text expected in March 1992, IS in March 1993) (CCITT X.742)
CD 10164-11.2	Information Technology - Open Systems Interconnection - Systems Management - Part 11: Workload Monitoring Function, 11 October 1991 [SC21 N 6452] (failed second CD ballot) (CCITT X.739) (IS status expected December 1992)
DIS 10164-12	Information Technology - Open Systems Interconnection - Systems Management - Part 12: Test Management Function, CCITT X.745, November 1991 [SC21 N 5517] (IS text expected December 1992)
CD 10164-13.2	Information Technology - Open Systems Interconnection - Systems Management - Part 13: Measurement Summarization Function, CCITT X.738, 12 November 1991 [SC21 N 6485] (IS text expected December 1992)
CD 10164-14	Information Technology - Open Systems Interconnection - Systems Management - Part cdt: Confidence and Diagnostic Test Categories, CCITT X.737, June 1991 [SC21 N 6307] (DIS expected in August 1992, IS in August 1993)
WD 10164-X	Information Technology - Open Systems Interconnection - Systems Management - Part X: Software Management Function, July 1991 [SC21 N 6040] second WD inproduction January 1952 (CD text expected June 1993, DIS in March 1994, IS in March 1995)
WD 10164-A	Information Technology - Open Systems Interconnection - Systems Management - Part A: Time Management Function, July 1990 [SC21 N 4953] [JTC1 N 763] (new work item; standard will have two parts: representation of time and mechanisms for the distribution and synchronization of time; CD text expected June 1993, DIS in March 1994, IS in March 1995) (CCITT X.743)
WD 10164-sm	Information Technology - Open Systems Interconnection - Systems Management - Part sm: Systems Management Relationship Model, June 1991 [SC21 N 6041] (CD expected in December 1992, DIS in August 1993, IS in August 1994)
WD 10164-rtm	Information Technology - Open Systems Interconnection - Systems Management - Part rtm: Response Time Monitoring, August 1990 [SC21 N 4949; JTC1 N 963] (CD text expected December 1993, DIS in August 1994, IS in August 1995)
WD 10164-s	Information Technology - Open Systems Interconnection - Systems Management - Part s: Scheduling Function, June 1991 [SC21 N 6021] (CD text expected June 1992, DIS in March 1993, IS in March 1994)
WD 10164-pm	Information Technology - Open Systems Interconnection - Systems Management - Part pm: Performance Management, July 1991 [SC21 N 6306]
ISO 10165-1♦	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 1: Management Information Model, November 1991 [SC21 N 6351]
ISO 10165-2♦	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information, September 1991 [SC21 N 6363] (incorporated Part 3)
ISO 10165-4♦	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects, November 1991 [SC21 N 6359]
CD 10165-5♦	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 5: Generic Management Information, August 1991 [SC21 N 6360] (previously entitled Generic Managed Objects) failed November 1991 ballot
CD 10165-6♦	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 6: Requirements and Guidelines for Management Information Conformance Statement (MICS) Proformas, July 1991 [SC21 N 6027] (DIS text expected in March 1992, IS in March 1993) failed November 1991 ballot

WD 10165-7♦	Information Technology - Open Systems Interconnection - Structure of Management Information - Part 7: Management Information Register and Registration Procedures, (CD expected in June 1992, DIS in December 1992, IS in December 1993)
WD 10165-x	Information Technology - Open Systems Interconnection - Managed Object Conformance Statement (MOCS) Proforma, 14 February 1991 [SC21 N 5686]
ISO 10166-1	Document Filing and Retrieval (DFR) - Part 1: Abstract Service Definition and Procedures, 1991 [SC18 N 2069, February 1989]
ISO 10166-2	Document Filing and Retrieval (DFR) - Part 2: Protocol Specification, 1991 [SC18 N 2070, February 1989]
TR 10167♦	Information Processing Systems - Open Systems Interconnection - Draft Technical Report on Guidelines for the Application of Estelle, LOTOS, and SDL, July 1991 [SC21 N 4259, 18 January 1990] (IS text expected December 1991)
DIS 10168-1♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol - Part 1: Test Suite Structure and Test Purposes, January 1991 [SC21 N 4159, 11 December 1989]
WD 10168-2♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol - Part 2: Generic Test Suite, July 1989 [SC21 N 3667] (CD text expected October 1993, DIS in October 1994, IS in October 1995)
WD 10168-3♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol - Part 3: Session Generic Test Suite, July 1989 [SC21 N 3667] (CD text expected October 1993)
DIS 10168-4♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol - Part 4: Session Test Management Protocol Specification, March 1991 [SC21 N 5026, December 1990]
ISO 10169-1♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the ACSE Protocol - Part 1: Test Suite Structure and Test Purposes, 24 September 1991 [SC21 N 6421]
WD 10169-2	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol - Part 2: Abstract Test Suite (CD expected October 1992)
ISO 10170-1♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol - Part 1: Test Suite Structure and Test Purposes, June 1991 [SC21 N 6269]
WD 10170-2♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol - Part 2: FTAM Abstract Test Suite, June 1989 [SC21 N 3665] (CD text expected October 1992, DIS in June 1993, IS in June 1994)
WD 10170-3♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol - Part 3: ACSE Abstract Test Suite Embedded Under FTAM, 1989 (formal WD text expected June 1992, CD text in June 1993, DIS in June 1994, IS in June 1995)
WD 10170-4♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol - Part 4: Presentation Abstract Test Suite Embedded Under FTAM, 1989 (formal WD text expected June 1992, CD text in June 1993, DIS in June 1994, IS in June 1995)
WD 10170-5♦	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol - Part 5: Session Abstract Test Suite Embedded Under FTAM, 1989 (formal WD text expected June 1992, CD text in June 1993, DIS in June 1994, IS in June 1995)
TR 10171	List of Standard Data Link Layer Protocols that Utilize HDLC Classes of Procedures (awaiting publication)
TR 10171 PDAM 1	List of Standard Data Link Layer Protocols that Utilize HDLC Classes of Procedures, Amendment 1: Registration of XID Format Identifiers and Private Parameter Set Identifiers (ballot closed 10 March 1991)
TR 10172	Information Processing Systems - Data Communications - Network/Transport Protocol Interworking Specification [SC6 N 5906, 29 March 1990], 15 October 1990

ISO 10173	ISDN Primary Access Connector at Reference Points S and T, 1991
DTR 10174	Logical Link Control (type 2 Operation) Test Purposes (awaiting DTR publication)
DIS 10177	Information Processing Systems - Data Communications - Intermediate-System Support of the OSI Connection-Mode Network Service Using ISO 8208 in Accordance with ISO 10028, (ballot closed 23 February 1991)
PDTR 10178	Structure and Coding of Link Service Access Point Addresses in LANs
DIS 10179	Document Style Semantics and Specification Language (DSSSL), 28 June 1991
DIS 10180	Standard Page Description Language (SPFL) March 1991
WD 10181-1♦	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 1: Overview, July 1991 [SC21 N 6166] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
DIS 10181-2	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 2: Authentication Framework, 13 May 1991 [SC21 N 5727] (IS status expected in March 1992)
DIS 10181-2 WDAM 1	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 2: Authentication Framework, Amendment 1: Authentication Elements, July 1991 [SC21 N 6172] (new work item in WG1)
CD 10181-3♦	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 3: Access Control Framework, July 1991 [SC21 N 6168] (DIS text expected in March 1992; IS status in December 1992)
WD 10181-4♦	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 4: Non-Repudiation Framework, July 1991 [SC21 N 6165] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
WD 10181-5♦	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 5: Confidentiality Framework, July 1991 [SC21 N 6164] (CD status expected in June 1992, DIS in June 1993, IS in June 1994)
WD 10181-6	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 6: Integrity Framework, July 1991 [SC21 N 6163] (CD status expected in June 1992, DIS in June 1993, IS in June 1994) .
CD 10181-7	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 7: Security Audit Framework, July 1991 [SC21 N 6169] failed CD ballot (DIS text expected in March 1992; IS status in December 1992)
WD 10181-8	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Part 8: Key Management
PDTR 10182	Binding Techniques for Programming Languages [SC22/WG11 N 754]
DTR 10183	Text and Office Systems - ODA and Interchange Format - Testing Methodology and Abstract Cases - Implementation Testing, 1991
CD 10184-1.2	Terminal Management - Model, July 1991 [SC21 N 4176, June 1990] (DIS text expected in July 1992, IS in July 1993)
WD 10184-2	Terminal Management - Service, July 1991 [SC21 N 4176, June 1990] (CD text expected July 1992, DIS in December 1992, IS in December 1993)
WD 10184-3	Terminal Management - Protocol, July 1991 [SC21 N 4176, June 1990] (CD text expected July 1992, DIS in December 1992, IS in December 1993)
PDTR 10182	Binding Techniques for Programming Languages [SC22 /WG11 N 754], 6 February 1990
ISO 10206	Object Oriented Extensions to Pascal, 1991
DIS 10222	Enhanced Small Device Interface, 1991
DIS 10279	Programming Languages - Full BASIC, 1991
DP 10303	Standard for Exchange of Product Model Data (STEP)
DIS 10588	Use of the X.29 PLP in Conjunction with X.21/X.21 bis to Provide the OSI CONS (awaiting DIS ballot)

DIS 10589	Intermediate System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8473 (awaiting DIS ballot)
ISP 10607-1	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM, 17 January 1991 [SGFS N 284] (submitted by SPAG) (ISP accepted December 1990)
ISP 10607-2	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 2: Definition of Document Types, Constraint Sets and Syntaxes, 17 January 1991 [SGFS N 285] (submitted by SPAG), reprinted April 1991 to correct error in Foreword
ISP 10607-2 AD 1	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 2: Definition of Document Types, Constraint Sets and Syntaxes, Addendum 1: Additional Definitions, Approved 27 May 1991 [SGFS N 363]
ISP 10607-3	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 3: AFT 11 - Simple File Transfer Service (Unstructured), 17 January 1991 [SGFS N 286] (submitted by SPAG), reprinted April 1991 to correct error in Foreword
ISP 10607-4	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 4: AFT 12 - Positional File Transfer Service, Approved 27 May 1991 [SGFS N 360]
ISP 10607-4 DAD 1	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 4: AFT 12 - Positional File Transfer Service, Addendum 1: Additional Definitions, 17 July 1990 [SGFS N 245]
ISP 10607-5	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 5: AFT 22 - Positional File Access Service, Approved 27 May 1991 [SGFS N 361]
ISP 10607-6	Information Technology - International Standard Profile - AFT nn - File Transfer, Access, and Management - Part 6: AFT 3 - File Management Service, Approved 27 May 1991 [SGFS N 362]
pDISP 10608-1	International Standardized Profile TA-Connection-mode Transport Service over Connectionless Network Service, Part 1: General Overview and Subnetwork-Independent Requirements
pDISP 10608-2	International Standardized Profile TA-Connection-mode Transport Service over Connectionless Network Service, Part 2: TA51 Profile Including Subnetwork-dependent Requirements for CSMA/CD LANs (ballot closed 13 December 1990)
pDISP 10608-5	International Standardized Profile TA-Connection-mode Transport Service over Connectionless Network Service, Part 5: TA1111/TA1121 Profiles Including Subnetwork-dependent Requirements for X.25 Packet Switched Data Networks Using Switched Virtual Circuits, (ballot closed 13 December 1990)
DISP 10609-1	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 1: Subnetwork-type Independent Requirements for Group TB (ballot closed 13 December 1990)
DISP 10609-2	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 2: Subnetwork-type Independent Requirements for Group TC, (ballot closed 13 December 1990)
DISP 10609-3	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 3: Subnetwork-type Independent Requirements for Group TD (ballot closed 13 December 1990)
DISP 10609-4	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 4: Subnetwork-type Independent Requirements for Group TE (ballot closed 13 December 1990)
DISP 10609-5	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 5: Definition of Profile TB 1111/TB 1121, (ballot closed 13 December 1990)

DISP 10609-6	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 6: Definition of Profile TC 1111/TC 1121(ballot closed 13 December 1990)
DISP 10609-7	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 7: Definition of Profile TD 1111/TD 1121(ballot closed 13 December 1990)
DISP 10609-8	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 8: Definition of Profile TE 1111/TE 1121(ballot closed 13 December 1990)
DISP 10609-9	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 9: Subnetwork-type Dependent Requirements for Network Layer, Data Link Layer, and Physical Layer Concerning Permanent Access to a Packet Switched Data Network Using Virtual Call, (ballot closed 13 December 1990)
CD 10641	Conformance Testing of Implementations of Graphics Standards, 1991
DP 10646	Information Processing - Multiple Octet Coded Character Set, SC27, 14 November 1989 [SC21 N 4627]
DIS 10728	Information Resource Dictionary System (IRDS) Services Interface, July 1991 [SC21 N 6315, 1 August 1991]
DIS 10729-1♦	Conformance Test Suite for the Presentation Protocol, Part 1: Test Suite Structure and Test Purposes for the Presentation Protocol, SC21/WG6, April 1991 [SC21 N 5927] (IS expected June 1992)
CD 10729-2	Conformance Test Suite for the Presentation Layer, Part 2: Test Suite for ASN.1 Encodings and Test Purposes for Presentation Protocol, 20 December 1991 [SC21 N 6634] (DIS text expected in June 1992, IS in June 1993)
WD 10729-3	Conformance Test Suite for the Presentation Layer, Part 3: Common Presentation Abstract Test Suite, October 1991 (CD text expected June 1992)
DTR 10730	Information Technology - Open Systems Interconnection - Tutorial on Naming and Addressing, August 1991 [SC21 N 6335] (IS text expected June 1992)
DIS 10731	Information Technology - Open Systems Interconnection - Conventions for the Definition of OSI Services, August 1991 [SC21 N 6341] (will supersede TR 8509; IS expected March 1992)
CD 10732	Use of X.25 PLP to Provide the OSI CONS Over the Telephone Network (ballot closed 20 February 1991)
DIS 10733	Information Technology - Telecommunications and Information Exchange Between Systems - Elements of Management Information Related to OSI Network Layer Standards [SC21 N 5560, 3 January 1991; SC6 N 6413, 11 December 1990] (IS status expected June 1992)
PDTR 10734	Guidelines for Bridged LAN Source Routing Operation by End Systems (ballot closed 8 March 1991)
PDTR 10735	Standard Group MAC Addresses (ballot Closed 10 March 1991)
DIS 10736	Transport Layer Security Protocol, JTC1/SC6, July 1991 (balloting ends June 1992)
DIS 10736 PDAM 1	Transport Layer Security Protocol - Amendment 1, Security Association Establishment Protocol, JTC1/SC6, July 1991 (balloting ends April 1992)
DIS 10737	Specification of the Elements of Management Information Related to OSI Transport Layer Standards (ballot closed 9 March 1991) (IS status expected June 1992)
DIS 10739-1	Information Technology - Open Systems Interconnection - Conformance Test Suite for 9041 - Virtual Terminal Basic Class Protocol - Part 1: Test Suite Structure and Test Purposes, 31 October 1991 [SC21 N 6499] (IS expected July 1992)
CD 10744	Information Technology - Hypermedia/Time-based Structuring Language (HyTime), April 1, 1991
CD 10745	Information Technology - Open Systems Interconnection - Upper Layer Security Model, 28 June 1991 [SC21 N 6095] (CD ballot closes 22 October 1991)

WD 10746-1♦	Basic Reference Model for Open Distributed Processing - Part 1: Overview, 30 May 1991 [SC21 N 6083] (CD text expected June 1993)
CD 10746-2♦	Basic Reference Model for Open Distributed Processing - Part 2: Descriptive Model, 30 May 1991 [SC21 N 6079]
WD 10746-3♦	Basic Reference Model for Open Distributed Processing - Part 3: Prescriptive Model, 30 May 1991 [SC21 N 6080] (CD text expected June 1992)
WD 10746-4♦	Basic Reference Model for Open Distributed Processing - Part 4: User Model, 30 May 1991 [SC21 N 6083] (CD text expected May 1993)
WD 10746-5	Basic Reference Model for Open Distributed Processing - Part 5: Architectural Semantics, Specification Techniques and Formalisms, 30 May 1991 [SC21 N 6082] (CD text expected May 1993)
CD 10918-1	Digital Compression and Coding of Continuous-Tone Still Images, Part 1: Requirements and Guidelines, February 1991
CD 10918-2	Digital Compression and Coding of Continuous-Tone Still Images, Part 2: Compliance Testing
DIS 10967	Language Compatible Arithmetic Standard (LCAS), [SC22 N 796], Version 2.2A, 31 May 1990 (undergoing public review July 1991)
DIS 10994	Information Technology - Data Interchange on 90 mm Flexible Disk Cartridges Using MFM Recording at 31 831 FTPRAD on 80 Tracks on Each Side, 21 June 1991
CD 11072	Information Processing Systems - Computer Graphics - Reference Model of Computer Graphics, 1991
CD 11172	Coding of Moving Pictures and Associated Audio, December 1990
pDISP 11183-1	Information Technology - International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by ROSE and CMISE, Second Version, 27 April 1991 [SGFS N 357 and 358, 24 May 1991]
pDISP 11183-2	Information Technology - International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 2: Enhanced Management Communications, Fourth Version, 27 April 1991 [SGFS N 359, 24 May 1991]
pDISP 11183-3	Information Technology - International Standardized Profiles AOMnn OSI Management - Management Communications Protocols - Part 3: AOM11 - Basic Management Communications, Draft pDISP text, First Version, 23 May 1991 [IST/21:2808]
DIS 11319	Information Technology - 8 mm Wide Magnetic Tape Cartridge for Information Interchange -- Helical Scan Recording, 21 June 1991
DIS 11321	Information Technology - 3,81 mm Wide Magnetic Tape Cartridge for Information Interchange -- Helical Scan Recording-- Data/Dat Format, 21 June 1991
ISO 11404	Information Technology - Programming Languages - Common Language-Independent Datatypes (CLID), 1991
CD 11577	Network Layer Security Protocol, JTC1/SC6, July 1991 (balloting ends April 1992)
CD 11578-1	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 1: Model, June 1991 [SC21 N 6111]
CD 11578-2	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 2: Interface Definition Notation, June 1991 [SC21 N 6111]
CD 11578-3	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 3: Service Definition, June 1991 [SC21 N 6111]
CD 11578-4	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 4: Protocol Specification, June 1991 [SC21 N 6111]
CD 11578-5	Information Technology - Open Systems Interconnection - Remote Procedure Call - Part 5: PICS Proforma, June 1991 [SC21 N 6111]

JTC1 N 474	Proposal for a New Work Item: OSI Upper Layers Security Model, 21 July 1989 [SC21 N 5447, 30 October 1990]
JTC1 N 535	Directives for the Work of ISO/IEC Joint Technical Committee 1 (JTC1) on Information Technology, Secretariat, 31 August 1989
JTC1 N 598	JTC1 Strategic Plan, Editing Team, 20 November 1989
JTC1 N 996	IST/21 N 2478, Catalogue of Security Related Projects for consideration at the JTC 1 Workshop on Security 5-7 November 1990, 30 May 1990
JTC1 N 1011	Results of National Body Survey for Consideration at the JTC1 Workshop on Security, 5-7 November 1990, London, 10 October 1990
JTC1 N 1015	ISO/IEC JTC1/SC21 Presentation Materials for the Workshop on Security (Topic: Security for OSI Management), 10 October 1990
JTC1 N 1016	ISO/IEC JTC1/SC21 Presentation Materials for the Workshop on Security (Topic: OSI Security Architecture and Security Frameworks), 10 October 1990
JTC1 N 1161	Report of the Meeting of the Ad Hoc Technical Study Group on Multimedia and Hypermedia, 8 January 1991.
JTC1 N 1240	Presentation to the JTC 1 Advisory Group Regarding the Recommendations by the Technical Study Group on Multimedia and Hypermedia, 26 February 1991.
JTC1 N 1252	Summary of Voting on Document JTC1 N 1021, Proposal for a New Work Item on Data Management Export/Import for SQL and IRDS, JTC1 Secretariat, 20 February 1991
JTC1 N 1254	Summary of Voting on Document JTC1 N 1023, Proposal for a New Work Item on Information Resource Dictionary Systems (IRDS), JTC1 Secretariat, 20 February 1991
JTC1 N 1260	SC21 Request to Modify its Programme of Work, ISO/IEC JTC1, 5 March 1991
JTC1 N 1387	Contribution from JTC1/SC21 on Proposed Changes to JTC1 Organization, 10 June 1991
JTC1 N 1440	Use of Systems Management for Administration of the Directory, 23 August 1991
JTC1 N 1484	Final Disposition of Proposal for a New Work Item on Data Export/Import for SQL and IRDS, 16 August 1991
JTC1 N 1485	Final Disposition of Proposal for a New Work Item on RDA Support for Stored DBL Statements, 16 August 1991
JTC1 N 1486	Final Disposition of Proposal for a New Work Item on Information Resource Dictionary Systems, 16 August 1991
JTC1 N 1562	ISO/IEC JTC1/SC21 Contribution to the JTC1/SWG on Procedures Regarding Maintenance and Correction of Defects, 9 September 1991
JTC1 SWG-EDI N 177	Conceptual Model for Electronic Data Interchange Standards and Services, 6 December 1990.
SGFS N 100	Information Technology - Framework and Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein, Revision 3, 10 September 1991
SGFS N 151	CCITT Liaison Statement on Work of SGFS, 6 November 1989 (includes X.220)
SGFS N 201	Information Processing Systems - International Standardized Profiles - Taxonomy Update, ISP Approval, and Maintenance Process, 7 May 1990 (standing SGFS document)
SGFS N 214	Catalogue of PICS Proforma Notations, SC21, 17 January 1991
SGFS N 219	An Example of T-Profiles Multi-Part ISP Structure, 11 June 1990
SGFS N 224	Documents Relating to Applications Portability Profile Work from JTC1/TSG-1, 11 June 1990
SGFS N 225	Resolutions of JTC1 Advisory Group, 11 June 1990
SGFS N 226	Liaison Statement to JTC1 on Multi-Part ISDN ISP Structures, 11 June 1990

SGFS N 228	Liaison Statement to JTC1 SGFS on the Inclusion of a Profile for MMS in the Taxonomy of Profiles TR 100000-2, 11 June 1990
SGFS N 229	Resolutions of the 3rd Regional Workshop Coordinating Committee Meeting; AOW - EWOS - NIST OIW, 11 June 1990
SGFS N 236	EWOS Organization and Activities, 11 June 1990
SGFS N 282	Resolutions of the 4th RWS-CC Meeting, 18-19 October 1990, 17 January 1991
SGFS N 300	List of documents (N 182 - N 300), Secretariat, 12 February 1991
SGFS N 373	Output from the 5th Regional Workshop Coordinating Committee (RWS-CC), March 18-19, 1991, 13 June 1991
SGFS N 401	Information Processing Systems, International Standardized Profiles, Taxonomy Update, ISP Approval and Maintenance Process, 23 September 1991
SC21 SD-1	Report of the Secretariat to the Plenary Meeting of ISO/IEC JTC1 SC21, 5-6 June 1990, Seoul, Republic of Korea, SC21 Secretariat, 12 April 1990 [SC21 N 4588] (provides terms of reference and points of contact for working groups)
SC21 SD-2	ISO/IEC JTC1 SC21 Programme of Work (POW) - Target Date Summary for All Active and Published Projects, SC21 Secretariat, April 1990
SC21 SD-7	Security Management Plan, 4 June 1990 [SC21 N 5130]
SC21 SD-8	SC21 Schedule of Meetings, 20 June 1991 [SC21 N 6261]
SC21 SD-9	Approved Commentaries on the Basic Reference Model for Open System Interconnection, OSI Reference Model Editor, July 1991 [SC21 N 6198]
CD xxxx♦	A Formal Description of the Transport Service Definition in Estelle
CD xxxx♦	A Formal Description of the Transport Protocol Specification in Estelle
CD xxxx	Transport Test Management Protocol (awaiting CD ballot)
DP xxxx♦	Operating System Command and Response Language (OSCRL)
DP xxxx♦	System Software Interface for Application Programmes (SSI)
DP xxxx	Mailbox Access Service and Protocol
WD xxxx	Information Resource Dictionary System (IRDS) - Design Support for SQL Applications (CD text expected January 1991)
WD xxxx	Information Resource Dictionary System (IRDS) - Export/Import (CD text expected November 1990)
WD xxxx	Information Resource Dictionary System (IRDS) - Extensions, July 1990 [SC21 N 5139] (CD text expected June 1992)
WD xxxx	Registration of System Titles (DP expected November 1990)
WD xxxx	Service and Protocol for Authentication Exchange Application Service Element (ASE), January 1990 [SC21 N 4110] [JTC1 N 767] (WD expected October 1990, CD expected June 1992; collaborative work with CCITT SG VII)
WD xxxxx	Applications with Multi-Parties [SC21 N 6197]
WD xxxx-1	Cryptographic Mechanisms for Key Management, Part 1: Key Management Overview [SC27/WG2]
WD xxxx-2	Cryptographic Mechanisms for Key Management, Part 2: Key Management Using Secret Key Techniques [SC27/WG2]
WD xxxx-3	Cryptographic Mechanisms for Key Management, Part 3: Key Management Using Public Key Techniques [SC27/WG2]
WD xxxx-4	Cryptographic Mechanisms for Key Management, Part 4: Key Management Using Public Key Register [SC27/WG2]

WD xxxxx-1	Security Exchange Application Service Element (ASE) Part 1: Model and Specification Framework, WG6, 3 June 1991 [SC21 N 6096]
WD xxxxx-2	Security Exchange Application Service Element (ASE) Part 2: Service Definition, WG6, 3 June 1991 [SC21 N 6096]
WD xxxxx-3	Security Exchange Application Service Element (ASE) Part 3: Protocol Specification, WG6, 3 June 1991 [SC21 N 6096]
WD xxxxx-4	Security Exchange Application Service Element (ASE) Part 4: PICS Proforma, WG6, 3 June 1991 [SC21 N 6096]
PDTR xxxx	Information Processing - Methodology and Guidelines for the Development of Application Layer Protocols, June 1990 [SC21 N 4903] (new work item of June 1988 failed but programme of work with CDTR is still active; status uncertain)
PDTR xxxx	Estelle Formal Description of ISO 8473 (awaiting PDTR ballot)
WDTR xxxx	Systems Management Tutorial, July 1990, SC21/WG4 [JTC1 N 957] [SC21 N 4942] (CCITT X.702)
WDTR xxxx, Ann A	Systems Management Tutorial - Annex A: Access Control, 30 May 1990 [SC21 N 4970]
WDTR xxxx	Application Layer Guidelines, November 1989 [SC21 N 3206, December 1988] (CD text expected in 1990)
WDTR xxxx	Tutorial on the Reference Model for Data Management (PDTR expected June 1992)
WDTR xxxx♦	Architectural Semantics for FDTs (new work item, October 1987) [SC21 N 2010]
WDTR xxxx♦	Information Processing Systems - Open Systems Interconnection - Remote Database Access (RDA) Tutorial, January 1989 [SC21 N 3343] (PDTR text expected June 1992)
WDTR xxxx	Catalogue of PICS Proforma Notations, July 1991 (joint work of WG1 and CCITT SG VII; meeting scheduled for February 1991) [SC21 N 6160]
EWOS/EGTP/91/12	Draft Taxonomy for Distributed Transaction Processing, EWOS, 13 February 1991
IST18 N 2694	Final Report on the Framework for Open Systems, July 1990
IST21 N 2361	UK Comment Accompanying Vote of Disapproval on CD 10728, Information Resource Dictionary System Services Interface, UK, 24 October 1990
IST21 N 2393	Proposals for Corrigenda to OSI Standards - Reprint from BSI News, November 1990
IST21 N 2433	EWOS/TA/PT N004 Final Report on the Framework for Open Systems
IST21 N 2478	Catalogue of Security Related Projects for consideration at the JTC 1 Workshop on Security 5-7 November 1990, 30 May 1990
IST21 N 2499	Report on the Anaheim IRDS Services Interface Meetings, David JL Gradwell, 18 January 1991
IST21 N 2508	PICS Proforma Notations, 17 January 1991
IST21 N 2514	Information Technology - International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the use by FTAM, Project Editor, 17 January 1991
IST21 N 2531	Discussion Paper on the Nature of Protocol Profiles, BSI, 6 February 1991
IST21 N 2551	UK Response to SC21 N 5110 on the Technical Structure of Quality-of-Service (QOS) Architecture, February 1991
IST21 N 2552	Proposed UK Contribution on QOS, Joint Meeting on QOS, 29 January 1991
IST21 N 2555	Work on security within SC21, 15 February 1991

IST21 N 2589	Minutes of the 20th meeting of EWOS EGLL from October 8 to October 11, 1990, in Brussels, 1 February 1991
IST21 N 2604	Relaying the MAC Service using Transparent Bridging (CSMA/CD-CSMA/CD), 26 February 1991
IST21 N 2605	Connection-mode Transport Service over Connectionless-mode Network Service, 26 February 1991
IST21 N 2652	Security Features in International Standardized Profiles (ISPs), 31 January 1991
IST21 N 2659	EWOS Releases More IT Functional Standard Proposals for Open Systems, 12 March 1991
IST21 N 2670	Prospective vs Traditional Standardization, 21 March 1991
IST21 N 2685	Access to Public and Private MHS (1988) Common Facilities MTS end-user to MTS end-user and MTA, 4 March 1991
IST21 N 2731	Proposed EN 41204, Simple File Transfer Service, 22 April 1991
IST21 N 2734	Part 1: Specification of ACSE, Presentation and Session Protocols for the use by ROSE and CMISE; Part 2: Enhanced Management Communications; 15 April 1991
IST21 N 2742	Information Technology - International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 2: Definition of document types, constraint sets and syntaxes, Project Editor, 17 January 1991
IST21 N 2743	Information Technology - International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 3: AFT 11 - Simple File Transfer Service (unstructured), Project Editor, 17 January 1991
IST21 N 2744	A Mapping of the X Window System over and OSI Stack, EWOSEG VT, April 1991
IST21 N 2754	Extension of M-IT-01 and M-IT-02 for the Open System Environment, European Workshop for Open Systems, EWOSTA9181, April 1991
IST21 N 2755	EWOS Contribution to ISO/IEC JTC1 SGFS, April 1991
IST21 N 2756	Extension of TR 10000-2 Taxonomy for the Directory (ADI and FDI), 17 April 1991
IST21 N 2758	Liaison Statement to ISO/IEC JTC1 SGFS on the Relationship of ISPs to Registration Authorities, 12 April 1991
IST21 N 2759	EWOS/TLG Report to TA 13, May 14/15, 1991
IST21 N 2760	Liaison Statement to ISO/IEC JTC1 SGFS on the Virtual Terminal Taxonomy in TR 10000-2, 12 April 1991
IST21 N 2766	Resolutions RWS-CC, March 1991
IST21 N 2767	Report to EWOS/TA (14/15 May, 1991) From EGTP Chair, May 1991
IST21 N 2772	Project Team Proposal on Production of Standardized Conformance Test Specifications for FTAM, 30 April 1991
IST21 N 2773	The Future of European Standardization, 10 May 1991
IST21 N 2793	Status of Project Teams, 29 May 1991
IST21 N 2794	1st Workshop on Open Information Interchange, May 1991
IST21 N 2795	EWOS Work Programme, May 1991
IST21 N 2765	EWOS Proposed Taxonomy for OSI-TP, 10 May 1991
IST21 N 2766	March 1991 Resolutions RWS-CC, 10 May 1991
IST21 N 2769	Summary of EWOS Contribution to JTC1 SGFS, June 1991, 10 May 1991
IST21 N 2770	AD HOC Meeting on an Open Systems Framework, 10 May 1991
IST21 N 2799	The COSINE Concise Information Service Project, May 1991
IST21 N 2835	Report on SC21/WG6 Meetng, Arles, May 1991, 4 June 1991
IST21 N 2836	Report on SC21/WG6 ULA Rapporteur Meeting, Arles, May 1991, 5 June 1991
IST21 N 2837	Report on the Arles IRDS Meetings, 4 June 1991
IST21 N 2838	Report on Work Item 21.11/Virtual Terminals, June 1991

IST21 N 2840	Resolutions of the Seventh Plenary Meeting of ISO/IEC JTC1/SC21, Arles, France, 4-5 June 1991
IST21 N 2842	ISO/IEC JTC1/SC21 Subcommittee Report Part IV: Programme of Work, 3 June 1991
IST21 N 2852	POSIX Security Call for New Work Items, SC22/WG15, June 1991
IST21 N 2854	Memorandum M-IT-02 on Taxonomy of Profiles and Directory of Functional Standards, May 1991
IST21 N 2860	EWOS Technical Guide: Routing in the Context of OSI, EWOS-EGLL9172, Final Draft, 27 May 1991
IST21 N 2879	Status of ISO Work on OSI TP Standards, EWOS/EGTP/90/19r, 26 June 1991
IST21 N 2880	Interim Report on the Feasibility of Profiling Database Enquiry, EWOSPT N 014, June 1991
IST21 N 2889	Documents Relating to Functional Standards, 17 July 1991
IST21 N 2938	Identification of ENV/ENs with Equivalent ISO/IEC ISPs, 13 August 1991
IST21 N 2948	EWOS/EGTP #4 Main Results, Brussels, 25-28 June 1991
IST21 N 2949	EWOS Active Work Items - Status, 6 August 1991
IST21 N 2950	EWOS Internal Schedule of Deliverables, 6 August 1991
IST21 N 2951	EWOS Active Work Items - Information, 6 August 1991
IST21 N 2952	EWOS Completed Work Items, 6 August 1991
IST21 N 2956	EWOS Documents: Their Status and Processing in European and International Contexts, 7 August 1991
IST21 N 2967	UK Report on ISO/IEC JTC1/SC21/WG1 meeting held in Arles, France (22-30 May 1991), June 1991
IST21 N 2968	ISO/IEC JTC1/SC21 WG3 Data Base, UK Delegate's Report, August 1991
IST21 N 2981	Report of the SC21 Upper Layers Conformance Testing (ULCT) Meeting, May 1991
IST21 N 2982	A Mapping of the X Window System Over an OSI Stack, August 1991
IST21 N 3037	EWOS/EG/NM/91/115: Management Information Catalogue (Sixth Draft), 11 September 1991
IST21 N 3038	Informal Notes of the ISO/IEC JTC1 & CCITT Cooperation Meeting, 17-18 September, 1991
IST21 N 3044	An Informal Quality Service for Functional Standards, 30 August 1991
IST21 N 3045	Resolutions 7th ISO/IEC JTC1/SGFS meeting, June 18-21, 1991, Berlin, 15 August 1991
IST21 N 3046	JTC1 Directives Annex C, 20 September 1991
IST21 N 3050	UK Comments Accompanying Vote of Disapproval on CD 10745, Upper Layers Securities Model, 2 October 1991
IST21 N 3055	Report on the ANSI "Harmonizing Around IRDS" Meeting, 19 August 1991
IST21 N 3057	Standardization of PCTE, 11 September 1991
IST21 N 3058	Report of Joint IST/21 - UK SGVII Panel on OSI Management, October 1991
IST21 N 3059	RDA Issues and Recommended Positions, September 1991
IST21 N xxxx	Report of IST/-/1 Ad Hoc Meeting on PCTE, 19 July 1991
BSI 91/64912	Ad Hoc Meeting on PCTE, 14 June 1991
BSI 91/64913	Background Information on PCTE Standardization, ECMA, ECMA TC33, 12 April 1991
BSI 91/64914	ECMA PCTE, J. Dawes and H. Davis, ICL Secure Systems, March 1991
BSI 91/64915	Extract of PCTE Standards, ECMA, 28 February 1991

SC5 N 220	Interim Report of the TCCA Rapporteurs' Group of Time-Critical Communications Architecture and Systems, 15 April 1991
SC6 N 4053	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with ISO 8473
SC6 N 4782	An Architectural Framework for Private Networks, Pre-Publication Version of ECMA TR 44, December 1987
SC6 N 5006	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with ISO 8208 (X.25/PLP), May 1988
SC6 N 5447	Liaison Statement to SC21/WG4 on Lower Layer Management, 13 October 1990
SC6 N 5784	General Principles for the Definition of Lower Layer Management, Second Draft, JTC1 SC6/WG2/WG4, April 1990
SC6 N 6219	Liaison to SC21 on Lower Layer Security, ISO/IEC/JTC1/SC6, 4 October 1990
SC6 N 6221	Draft Network Layer Security Protocol, SC6/WG2, 28 September 1990 (incomplete editor's Draft B)
SC6 N 6227	Lower Layer Security Guidelines, SC6/WG2/WG4, 28 September 1990
SC6 N 6285	Working Draft OSI Transport Layer Security Protocol, SC6/WG4, 28 September 1990
SC6 N 6413	Elements of Management Information Related to OSI Network Layer Standards, December 1990 (see CD 10733]
SC21 N 197	Concepts and Terminology for the Conceptual Schema and the Information Base, TC97/SC5, March 1982
SC21 N 236	Assessment Guidelines for Conceptual Schema Language Proposals, TC97/SC21/WG5-3, 31 August 1985
SC21 N 2507	ODP: Report on Topic 1 - The Problem of Distributed Processing, March 1988 [SC21/WG7]
SC21 N 2511	ODP: Definitions and Glossary - March 1988 Version, March 1988 [SC21/WG7]
SC21 N 2524	SC21/WG1 Overview - OSI Architecture, 29 January 1991
SC21 N 2525	IST/21 Project File: January 1991, 30 January 1991
SC21 N 2555	Work in Security within SC21, Gray Girling, 15 February 1991
SC21 N 2652	Security Features in International Standards Profiles (ISPs), E.J. Humphreys, Chair of IST33, 14 March 1991
SC21 N 3109	Architectural and Descriptive Issues Identified During the Workshop on Application Layer Standardization, December 1988 [SC21/WG1]
SC21 N 3122	Informal Guide for ISO/IEC JTC1 and CCITT Cooperation, 15 January 1989
SC21 N 3132	TTCN Operational Semantics, November 1988
SC21 N 3141	Response to SC21 N 2864, Issues Concerning the Requirements for Security Services in the Presentation Layer, November 1988 [SC21/WG1]
SC21 N 3167	Response to SC18 Liaison on Encryption, January 1989 [SC21/WG3]
SC21 N 3174	Working Document on ASN.1, Including Timetable, March 1989 [SC21/WG6]
SC21 N 3180	Possible CCR Extensions - Base Text, January 1989 [SC21/WG6]
SC21 N 3194	ODP: Working Document on Topic 2.3 - Framework of Abstractions, December 1988 [SC21/WG7]
SC21 N 3202	ODP: Recommendations of SC21/WG7, Sydney, 9 December 1988
SC21 N 3205	Proposed Modus Operandi and Programme of Work of SC21/WG6 ULA Rapporteur Group, December 1988 [SC21/WG6]
SC21 N 3207	Relationship Between Objects in Peer Open Systems, December 1988 [SC21/WG6]
SC21 N 3208	Requirements for More Efficient Use of Application Associations, December 1988 [SC21/WG6]

SC21 N 3266	Guide for Open Systems Security, December 1988 [SC21/WG1]
SC21 N 3267	Plan for Work on Security in SC21, December 1988 [SC21/WG1]
SC21 N 3283	Working Draft for Lower-Layer Security Model, December 1988 [SC21/WG1]
SC21 N 3288	ODP: Working Document on Topic 2.2 - Properties and Design Freedoms, December 1988 [SC21/WG7]
SC21 N 3307	WG4 Architecture Issues List, December 1988 [SC21/WG4]
SC21 N 3311♦	Configuration Management Overview, December 1988 [SC21/WG4]
SC21 N 3316	Access Control for OSI Management and the Directory, December 1988 [SC21/WG4]
SC21 N 3317	Working Document on Extended Information Models, December 1988 [SC21/WG4]
SC21 N 3318	Working Document on the Directory Schema, December 1988 [SC21/WG4]
SC21 N 3319	Working Document on Replication and Knowledge Distribution, December 1988 [SC21/WG4]
SC21 N 3320	Working Document on Access Control, December 1988 [SC21/WG4]
SC21 N 3321	Working Document on Enhanced Search, December 1988 [SC21/WG4]
SC21 N 3322	Working Document on Atribute Classes, December 1988 [SC21/WG4]
SC21 N 3323	Request for National Body and CCITT Member Contributions on Directory PICS Proforma, December 1988 [SC21/WG4]
SC21 N 3337	Security Management Domain and Security Policies, December 1988 [SC21/WG4]
SC21 N 3344	IRDS Rapporteur Group Position on Need for IRDS Specialization for RDA, April 1989 [SC21/WG3]
SC21 N 3346	RDA Use of Remote Operation Notation of ROSE, December 1988 [SC21/WG3]
SC21 N 3351	RDA Requirements for CCR, December 1988 [SC21/WG3]
SC21 N 3352	Harmonization of RDA and TP, December 1988 [SC21/WG3]
SC21 N 3365	Guide to ISO Virtual Terminal Standards, February 1989 [SC21/WG5]
SC21 N 3369	Terminal Management (TM) Issues List, February 1989 [SC21/WG5]
SC21 N 3372	Sharing an Association Between FTAM and Other ASE, February 1989 [SC21/WG5]
SC21 N 3381	Statement on TM Strategic Direction, February 1989 [SC21/WG5]
SC21 N 3383	Relationship Between TM and User Interfaces, February 1989 [SC21/WG5]
SC21 N 3390	NWI Proposal for an Addendum to CMIS/CMIP on Suppress Relay, July 1989
SC21 N 3665	Specific Partial Abstract Test Suite (ATS) for Response Tests (CD text expected in October 1992; DIS in October 1993; IS in October 1994)
SC21 N 3666	Abstract Test Suite (ATS) for CS Test Method (WD text expected in June 1992; CD in October 1992; DIS in October 1993; IS in October 1994)
SC21 N 3674	Information Processing Systems - International Standardized Profiles - Directory of ISPs and Profiles Contained Therein, June 1989
SC21 N 3675	Information Processing Systems - International Standardized Profiles - ISP Approval and Maintenance Process, June 1989
SC21 N 3678	Information Processing Systems - International Standardized Profiles - Proposed New AMH Taxonomy, June 1989
SC21 N 3711	Requirements for Multipeer Data Transmission, July 1989
SC21 N 3733	Access Control for OSI Applications, July 1989
SC21 N 3801	Support Environment for Open Distributed Processing, ECMA, September 1989
SC21 N 3806	Request for New Question on Conceptual Schema Standardization, September 1989
SC21 N 3903	Modelling, Specification, Use, and Role of Conceptual Schemas, October 1989
SC21 N 3906	Final Report to SC21 in Florence on the Reassessment of Project JTC 1.21.9.1 on Multipeer Data Transmission, October 1989

SC21 N 3925	Liaison Statement to JTC1 SC21 from JTC1 SWG-EDI, JTC1 SWG-EDI, 19 October 1989
SC21 N 3930	Liaison Statement from JTC1/SC18 to JTC1/SC21/WG5 on Comments on Terminal Management, SC18/WG4, 19 October 1989
SC21 N 3991	Security Exchange Service Element, CCITT Q19/VII(DAF), November 1989 (CD text in SC21/WG6 expected in 1992)
SC21 N 4002	Extended Application Layer Structure, ANSI Contribution to SC21/WG6, 19 October 1989
SC21 N 4019	ODP: Topics List - November 1989 Version - for the Basic Reference Model of Open Distributed Processing, 8 November 1989
SC21 N 4020	ODP: List of Open and Resolved Issues - November 1989 Version, 11 December 1989
SC21 N 4021	ODP: Document Register and Bibliography - November 1989 Version, 11 December 1989
SC21 N 4022	ODP: Working Document on Topic 4.1 - Structures and Functions, 11 December 1989 [superseded by SC21 N 4885]
SC21 N 4023	ODP: Working Document on Topic 6.1 - Modelling Techniques and Their Use in ODP, 11 December 1989
SC21 N 4024	ODP: Working Document on Topic 6.2 - Formalisms and Specifications, 11 December 1989
SC21 N 4025	ODP: Working Document on Topic 8.1 - Draft Basic Reference Model of Open Distributed Processing, 11 December 1989
SC21 N 4026	ODP: Recommendations of SC21/WG7, Florence, 11 December 1989
SC21 N 4027	ODP: Meeting Minutes of the Florence Working Group Meeting of WG7, 11 December 1989
SC21 N 4028	ODP: SC21/WG7 Convener's Report to SC21 Plenary Meeting 11 December 1989
SC21 N 4029	ODP: Liaison Statement to JTC1/TSG-1 on IAP, 11 December 1989
SC21 N 4030	ODP: Cooperation between SC21/WG7 and CCITT SG VII (Q19/DAF), 11 December 1989
SC21 N 4031	ODP: Session Report on Joint Meeting on FDT, 11 December 1989
SC21 N 4032	ODP: Liaison Statement to JTC1/SWG-EDI on EDI Modelling, 11 December 1989
SC21 N 4033	ODP: Proposal for Future Cooperation Between SC21/WG6 and SC21/WG7 on ULA and ODP, 11 December 1989
SC21 N 4058	State Tables for CMIP, January 1990
SC21 N 4077♦	Fault Management Working Document, SC21/WG4, December 1989
SC21 N 4085♦	Accounting Management Working Document, Third Version, SC21/WG4, November 1989
SC21 N 4091♦	OSI Security Management Working Document, 15 November 1989
SC21 N 4106	Application Layer Recover, January 1990 (new work item; CD text expected June 1991)
SC21 N 4107	Modelling for Communications Aspects of Distributed Applications, January 1990 [JTC1 N 765] (new work item; CD text expected June 1991)
SC21 N 4108	Management Information in the Upper Layers, January 1990 (new work item; CD expected June 1991)
SC21 N 4162	Proposal for a NWI for Enhancement of FTAM Services to Satisfy Additional User Requirements, December 1989
SC21 N 4167	TP Heuristic Decisions, January 1990 [PDAMs dependent on National Body input]
SC21 N 4168	TP Commitment Optimizations, January 1990 [PDAMs expected June 1991]
SC21 N 4170	TP Dialogue Recovery and User Suspension of a Dialogue, January 1990 [PDAMs expected June 1992]
SC21 N 4171	TP Savepoints, January 1990 [NWI not accepted]

SC21 N 4184	Request for National Body Comment on Security Enhancements to FTAM, SC21/WG5, November 1989
SC21 N 4188	Response to SC18/WG4 N 1183, Comments on Terminal Management, and SC18/WG3 and CCITT SG VII(Q27) Liaison Statement on Terminal Management, SC21/WG5, December 1989
SC21 N 4189	Comments on the Integration of X-Windows into the OSI Environment, December 1989
SC21 N 4192	Proposed FTAM Document Type to Support CGM, SC21/WG5, December 1989
SC21 N 4195	Draft WG3 Position on Conceptual Schema Question, February 1990
SC21 N 4199	Liaison Statement to JTC1/SC1 on SC21/WG3 Terminology, contains the Reference Model on Data Management (8 August 1989), February 1990
SC21 N 4215	Formal Methods in Conformance Testing (new work item, January 1990) (CD expected June 1994)
SC21 N 4279	CCR Conformance Test Suite, January 1990 (new work item) (WD text expected June 1992, CD text June 1993)
SC21 N 4280	Proposed New Work Item: Conceptual Data Modelling Facility, SC21/WG3, February 1990
SC21 N 4354	Topics Proposed for Discussion at the JTC1 Workshop on Distributed Applications, Phoenix, March 1990, U.K. Contribution, January 1990
SC21 N 4383	Development of the Extended Information Model, January 1990
SC21 N 4472	Liaison Statement from JTC1/SC18 to JTC1/SC21 on Changes to ASN.1, SC18/WG3 (title is in error--changes are for ODA, ISO 8613), 22 February 1990
SC21 N 4511	U.S. Comments on Conceptual Schema, ANSI, 15 March 1990
SC21 N 4519	Clarification of ALS Modelling Concepts, Workshop on Distributed Applications, 18 April 1990
SC21 N 4520	Issues for Consideration by Joint ULA/ODP Meeting, Seoul, May/June 1990, Workshop on Distributed Applications, 18 April 1990
SC21 N 4523	Modelling of Application Program Interfaces and Remote Procedure Calls, Distributed Applications Workshop, 2 April 1990
SC21 N 4524	Consideration of the Data Management Component of Application Standards, Workshop of Distributed Applications, 23 April 1990
SC21 N 4526	Application Layer Security Considerations, Workshop of Distributed Applications, 18 April 1990
SC21 N 4564	ODP: Liaison Statement to SC21/WG7 on Relationship of DAF Architecture/Infrastructure with ODP Topic 4 - Functions and Interfaces, CCITT SG VII, March 1990
SC21 N 4593	Metadata Use and Standards for Managing Metadata, ANSI, 4 April 1990
SC21 N 4603	Position on Reassessment of JTM Full Class Protocol, AFNOR, March 1990
SC21 N 4641	U.S. Position on JTM Reassessment, March 1990
SC21 N 4647	Requirements for Service Conventions, May 1990
SC21 N 4648	Security and Security Exchange Information, 28 February 1990, Canadian Contribution to SC21/WG6
SC21 N 4655	Architectural Semantics for ODP - Reassessment Report, SC21/WG7, April 1990
SC21 N 4672	Liaison Statement on Character Internationalization, SC21/WG3 on Database Language Extended SQL, 26 May 1990
SC21 N 4674	Liaison Statement Regarding Common Application Interfaces for the Telematic Services, CCITT SG I, 23 May 1990
SC21 N 4679	Reassessment of Project 1.21.13.03 (JTM Full Class), SC21, 10 June 1990
SC21 N 4681	User Requirements for Multi-Party Communications (MPC), Canada, May 1990
SC21 N 4682	Establishment of User Requirements, Canada, May 1990
SC21 N 4709	Directory Implementor's Guide, CCITT WG VII(Q.20), June 1990

SC21 N 4716	Initial List of Planned pDISPs, 30 April 1990
SC21 N 4728	Collections of Definitions of OSI Vocabulary, SC21, April 1990
SC21 N 4744	Development of the DSA Information Model: Extended Distribution Knowledge Model, SC21/WG4, May 1990
SC21 N 4758	Request to ISO/IEC SC21 from OSF for Establishment of Liaison Relationship, 4 May 1990
SC21 N 4763	On-Going Multipeer Projects Within JTC1, ANSI, May 1990
SC21 N 4764	Progression of Association Pools, ANSI, 9 May 1990
SC21 N 4766	U.S. Response to SC21/WG6 N 770 on Requirements for Extended ALS, ANSI, May 1990
SC21 N 4767	US Response to SC21/WG6 N 7889 on Requirements for RPC Interface Definition Notation, 11 May 1990
SC21 N 4769	Discussion of Initial Schema Information Acquisition for Directory, SC21/WG4, May 1990
SC21 N 4770	Short-Form Names for Directory, SC21/WG4, May 1990
SC21 N 4771	US Positions on SC21 N 433, Working Draft on the Schema, SC21/WG4, May 1990
SC21 N 4773	Development of the DSA Information Model: Basic Distribution Knowledge, SC21/WG4, May 1990
SC21 N 4799	Letter for Information on Disposition of EDIMS Use of Directory, 21 May 1990
SC21 N 4801	Liaison Statement to SC21 on Joint Efforts Between SG VII(Q20) and SG I(Q16), CCITT SG I(Q.16), 21 May 1990
SC21 N 4802	Liaison Statement to SC21 on Comments on Short Form Names and Other Name Forms, CCITT SG I(Q.16), 21 May 1990
SC21 N 4803	Publication of Directory Schema and Other Registered Object Definitions, Canada, 2 May 1990
SC21 N 4804	Proposed DIT Structure Rule Definition, 10 May 1990
SC21 N 4806	Use of External Data Transfer Systems for Shadow Updates, 10 May 1990
SC21 N 4833	Report to JTC1 from SC27 on Security Techniques, SC27 Secretariat, 21 May 1990 [SC27 N 94, 3 May 1990]
SC21 N 4834	Liaison Statement from SC27 to JTC1 Advisory Group, SC27 Secretariat, 21 May 1990 [SC27 N 93, 3 May 1990]
SC21 N 4835	Report of the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, SC27 Secretariat, 21 May 1990 [SC27 N 92, 1 May 1990]
SC21 N 4836	Resolutions Taken at the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, 21 May 1990 [SC27 N 94, 3 May 1990]
SC21 N 4875	Recommendation on SQL2 Progress ISO 9075 Revised, 31 May 1990
SC21 N 4885	ODP: Working Document in Topic 4.3 - Function and Interface Definitions, 13 July 1990
SC21 N 4903	Methodology and Guidelines for the Development of Application Layer Standards, SC21/WG6, June 1990
SC21 N 4904	Request for Comment on Characteristics of an Application Service Element and Application Service Object, SC21/WG6, May 1990
SC21 N 4905	Request for Comment on Introduction of a New Relationship in ALS, SC21/WG6, June 1990
SC21 N 4906	Upper Layer Management - Call for Contributions, SC21/WG6, June 1990
SC21 N 4908	Liaison to CCITT SG VII(Q19,Q25) on ULA Topics, SC21/WG6, June 1990
SC21 N 4918	Question on Standardization of Directory API, July 1990
SC21 N 4922	Information on Distributed Entries, SC21/WG4, July 1990
SC21 N 4924	Extensions to Directory Abstract Service, Working Draft, SC21/WG4, July 1990

SC21 N 4925	Liaison to SC22/WG11 Concerning Remote Procedure Call Interface Definition Notation (IDN), June 1990
SC21 N 4926	Liaison to CCITT SG VII(Q19) on DAF, SC21/WG6, June 1990
SC21 N 4927	Working Draft, Information Processing Systems - Open Systems Interconnection - Remote Procedure Call, SC21/WG6, 1 June 1990
SC21 N 4928	Remote Procedure Call Definitions and Requirements, SC21/WG6, June 1990
SC21 N 4943	Extended Systems Management Architecture, SC21/WG4, July 1990 [JTC1 N 958] (new work item; planned to be an amendment to ISO 10040)
SC21 N 4944	Generic Managed Objects, SC21/WG4, July 1990 (new work item) [It has yet to be decided whether this work will result in an addendum to 10165-2, a new part to 10165, or a standard in its own right]
SC21 N 4945	Definition of a Management Information Register and Registration Procedures, SC21/WG4, July 1990 (new work item)
SC21 N 4946	Requirements and Guidelines for Managed Object Conformance Statement (MOCS) Proformas, SC21/WG4, July 1990 (new work item)
SC21 N 4947	Formal Descriptions of CMIP, SC21/WG4, July 1990 (new work item)
SC21 N 4951	Test Suites for OSI Directory, SC21/WG4, July 1990 (new work item)
SC21 N 4953	Time Management: Representation of Time, SC21/WG4, July 1990
SC21 N 4960	Generic Managed Objects, Working Draft, SC21/WG4, July 1990
SC21 N 4961	Request for Contributions to Progress Work on the Definition of State Tables for CMIP, May 1990
SC21 N 4968	Synchronization Across Multiple Managed Objects, SC21/WG4, July 1990
SC21 N 4969	Call for National Body Contributions on Time Management, SC21/WG4, May 1990
SC21 N 4973	The Use of System Title by OSI Management, SC21/WG4, July 1990
SC21 N 4974	Use of Global Naming for Identification of Managed Objects, SC21/WG4, July 1990
SC21 N 4975	A General Model for Relationship Management, SC21/WG4, 31 May 1990
SC21 N 4977	Use of Action to Invoke State Changes, SC21/WG4, July 1990
SC21 N 4979	Request for National Body Comment on the Need for an Access Control Information Management Function, SC21/WG4, May 1990
SC21 N 4980	Security Audit Framework Working Document, SC21/WG4, July 1990
SC21 N 4981 ♦	Performance Management Working Document, Sixth Working Draft, 4 July 1990
SC21 N 4982	WG4 Systems Management Issues, SC21/WG4, July 1990
SC21 N 5001	Upper Layers Security Model, Third Working Draft, SC21/WG6, 5 June 1990 (CD text expected in 1991)
SC21 N 5002	Commencement of Work on Security ASEs, SC21/WG6, 31 May 1990
SC21 N 5003	Distributed Applications Security Modelling and Infrastructure, SC21/WG6, y 1991
SC21 N 5011	odelling Recovery in the Application Layer, SC21/WG6, 1 June 1990 (new work item; CD text expected June 1991)
SC21 N 5012	Proposed Draft Amendment 1 to ALS on Extended Application Layer Structure, ISO/IEC JTC WG6 ULA, November 1990
SC21 N 5014	Liaison Statement to CCITT SG VII (Q.23) on Collaborative Work on OSI Registration, 6 June 1990
SC21 N 5016	Meeting Report for SC21/WG1/WG4/WG6/WG7 Joint Meeting on Service Conventions, ODP, and ULA on 29 May 1990, SC21, June 1990
SC21 N 5017	Relationship Between Concepts and Models for OSI and ODP, SC21/WG6, July 1990
SC21 N 5051	Working Document on ASN.1 Extensions, Character Sets, Version 3, SC21/WG6, 19 July 1990 supercedes N 4141]

SC21 N 5052	Working Document on ASN.1 Extensions, Table Types and Functions, Version 4, SC21/WG6, 11 July 1990 supercedes N 4143]
SC21 N 5053	Working Document on ASN.1 Extensions, Machine Processibility, Version 3, SC21/WG6, 31 May 1990 supercedes N 4140]
SC21 N 5054	Working Document on Basic Connection-Oriented Presentation Service Definition - Presentation Service to Give Confidentiality and Integrity Protection, SC21/WG6, 11 July 1990
SC21 N 5055	Working Document on ASN.1 Extensions, Miscellaneous Enhancements, Version 3, SC21/WG6, 31 May 1990 supercedes N 4139]
SC21 N 5061	Handling of Exception Cases in ASN.1, SC21/WG6, 11 July 1990
SC21 N 5063	Liaison on Handling of Character Sets in ASN.1, JTC1/SC2, 14 June 1990
SC21 N 5064	Working Document on Basic Connection-Oriented Presentation Protocol Specification - Amendment to the Presentation Protocol to Give Confidentiality and Integrity Protection, SC21/WG6, 11 July 1990
SC21 N 5069	Call for Comments on Technical Approval for Development of ASN.1 Work Plan, SC21/WG6, 11 July 1990
SC21 N 5071	Recommendations Approved by SC21/WG1 at its Seoul Meeting, 23-31 May 1990, SC21/WG1, May 1990
SC21 N 5072	List of Output Documents of SC21/WG1 Meeting, Seoul, 23-31 May 1990, SC21/WG1, July 1990
SC21 N 5073	Final Answer to Q1/30.5 on Definition of the Term "Quality of Service," SC21/WG1, May 1990
SC21 N 5074	Final Answer to Q1/330.6 on Relay, Routing, and Network Management, SC21/WG1, May 1990
SC21 N 5075	Protocol Profile Testing Methodology, Second Working Draft, SC21/WG1, July 1990
SC21 N 5078	Catalogue of PICS Proforma Notations, SC21/WG1, July 1990
SC21 N 5079	Draft Answer to Q1/63.1 on Conformance to Objects in the Context of OSI Management, SC21/WG1, May 1990
SC21 N 5080	Call for Contributions on OSI Management Conformance Issues, SC21/WG1, July 1990
SC21 N 5081	Draft Answer to Q1/61 on Consistency Among ISO Standards Related to the OSI Reference Model, May 1990
SC21 N 5093	Status and Method of Operation for the Reference Model Revision, SC21/WG1, May 1990
SC21 N 5095	Liaison to SC6 on Revision of the Reference Model, May 1990
SC21 N 5096	Liaison to CCITT SG VII on Revision of the Reference Model, June 1990
SC21 N 5099	Liaison Statement to CCITT SG VII(Q.25) on Service Conventions, SC21/WG1, May 1990
SC21 N 5105	Final Answer to Q1/56.6.1 on Positioning of Circuit Switched Networks, SC21/WG1, May 1990
SC21 N 5108 ADD	Report of the Conformance Testing Meeting, Held in Seoul, 22-30 May 1990, December 1990
SC21 N 5109	Liaison Statement to CCITT SG VII(Q23) on Naming and Addressing, SC21/WG1, July 1990
SC21 N 5110	Call to National Bodies and Liaison Organizations for Contributions on Technical Structure of Quality of Service (QoS) Architecture, May 1990
SC21 N 5112	Discussion Paper on Formal Methods in Conformance Testing, SC21/WG1, July 1990
SC21 N 5117	Multi-Party Testing for MHS, SC21/WG1, July 1990
SC21 N 5130	Security Management Plan, 4 June 1990

SC21 N 5131	Recommendations of the SC21/WG6 Meeting, 23 May - 1 June 1990, Seoul, SC21/WG6, June 1990
SC21 N 5136	Recommendations of SC21/WG3 Meeting in Seoul, May/June 1990, SC21/WG3, 19 June 1990
SC21 N 5137	Data Management Export/Import for SQL and IRDS, SC21/WG3, October 1990 (new work item). CD text expected December 1992
SC21 N 5138	RDA Support for Shared DBL Statements, SC21/WG3, October 1990 (new work item; rapporteur meeting January 1991)
SC21 N 5139	IRDS Extensions, SC21/WG3, July 1990 (new work item)
SC21 N 5154	Recommendations of the SC21/WG5 Meeting, Seoul, 24 May - 1 June 1990, SC21/WG5, June 1990
SC21 N 5155	Enhancement of FTAM Security Services, New Work Item Proposal, SC21/WG5, July 1990 [PDAM expected January 1992]
SC21 N 5156	TP Sub-Transactions, New Work Item Proposal, SC21/WG5, July 1990
SC21 N 5157	TP Separate Data and Commit Associations, New Work Item Proposal, SC21/WG5, July 1990
SC21 N 5158	Conformance Test Suite for the VT Protocol, July 1990 [JTC1 N 770] (new work item; CD text expected November 1990)
SC21 N 5162	WD xxxx, Information Processing Systems - Open systems Interconnection Interconnection - Conformance Test Suite for the VT Protocol - Test Suite and Test Procedures, June 1990
SC21 N 5164	Planned Work Schedule for FTAM, SC21/WG5, June 1990
SC21 N 5165	FTAM Constraint Set and Document Types for CGM, SC21/WG5, June 1990
SC21 N 5170	OSI TP Association Management - Statement of Requirements, SC21/WG5, June 1990
SC21 N 5171	OSI TP Security - Statement of Requirements, SC21/WG5, June 1990
SC21 N 5172	Combined Use of RPC and OSI TP, SC21/WG5, June 1990
SC21 N 5173	Working Draft Unstructured Data Transfer (UDT) for TP, SC21/WG5, May 1990
SC21 N 5176	OSI TP Security, New Work Item, June 1990
SC21 N 5177	OSI TP Association Management - Revised New Work Item, SC21/WG5, June 1990
SC21 N 5179	Proposed Replacement Text for the NWI Proposal on Commitment Optimizations in SC21 N 4168 (JTC1 N 631), SC21/WG5, June 1990
SC21 N 5183	Combined Use of CMISE and OSI TP, SC21/WG5, June 1990
SC21 N 5184	Queued Data Transfer for TP, SC21/WG5, May 1990
SC21 N 5189	Liaison Statement to JTC1/SWG-EDI on EDIFACT Document Types for FTAM, SC21/WG5, June 1990
SC21 N 5193	Conceptual Schema HOD/C Meeting report Held on 31 May 1990 in Seoul, July 1990
SC21 N 5194	Resolutions of the Fourth Plenary Meeting of SC21, 5 June 1990, Seoul, SC21, 5 June 1990
SC21 N 5196	Report of the Special Meeting on User Requirements, SC21, 7 June 1990
SC21 N 5197	Report of the Standards Maintenance Group, SC21, 4 June 1990
SC21 N 5203	SC21/WG1 Convenor's Report to SC21 Plenary Meeting, Seoul, 5-6 June 1990, SC21/WG1, 3 June 1990
SC21 N 5219	Draft Management Guidelines for SC21, Rapporteur for Strategic Planning, July 1990
SC21 N 5228	Report of the ISO/IEC JTC1/SC21 Plenary Meeting, 5 June 1990, Seoul, Korea, 30 July 1990
SC21 N 5228	Proposed Technical Corrigenda to ISO 9595 and ISO 9596
SC21 N 5229	Report of the JTC1/SC21 Plenary Meeting, 5 June 1990, Seoul, Republic of Korea

SC21 N 5337	EWOS Organizations and Activities, 9 October 1990, EWOS
SC21 N 5346	U.S. Contribution on the Upper Layer Security Model (ULSM), [SC21 N 5001], October 1990
SC21 N 5347	U.S. Contribution on the Security Frameworks Overview [SC21 N 5044, November 1990]
SC21 N 5348	U.S. Contribution on the Access Control Framework [SC21 N 5045, November 1990]
SC21 N 5349	U.S. Contribution on the Non-Repudiation Framework [SC21 N 5046, November 1990]
SC21 N 5351	Time Stamps, 24 September 1991
SC21 N 5394	Collections of Definitions of OSI Vocabulary, June 1991
SC21 N 5426	Directory Implementor's Guide - Editor, Version 3, ISO/IEC JTC1, 7 November 1990
SC21 N 5437	Proposal to Merge Working Set and Definition Working Set, 9 November 1990
SC21 N 5438	CD 10728 Clause 6, Proposed Revision 1, 9 November 1990
SC21 N 5439	Proposed Amendment to CD 10728 to Cover Error States, 9 November 1990
SC21 N 5448	Outline Working Draft for Part 1 of Generic Security Exchange ASE Definition, ISO/IEC, 30 October 1990
SC21 N 5502	Liaison Concerning Application Context Negotiation During Association Establishment, November 1990
SC21 N 5503	Response to Liaison Statement SC21 N 5453 on ULA Issues Arising on Security Work, November 1990
SC21 N 5504	Response to Liaison Statement to WG6 ULA and Upper Layer Security Groups (SC21/WG6 N 906), November 1990
SC21 N 5505	Liaison to CCITT Q23/VII and Q19/VII, ISO/IEC JTC WG6 ULA, November 1990
SC21 N 5543	Planning and Organization of SC21/WG4 Systems Management Activities, January 1991
SC21 N 5545	Working Draft Input on Scheduling for Management Functions, 12-23 November 1990
SC21 N 5546	Agreement on Planning Future Releases of CMIS/P, January 1991
SC21 N 5548	Issues Concerning the Management Information Model and GDMO, 12-23 November 1990
SC21 N 5549	Preliminary Consideration of New Work Items Relating to SMI, January 1991
SC21 N 5551	Work Plan for Managed Objects Standardization, 11 November 1990
SC21 N 5555	Liaison Statement to ISO/IEC JTC1/SC21 on Lower Layer Security, SC6, 3 January 1991
SC21 N 5557	Liaison Statement to ISO/IEC JTC1/SC21/WG1 on SC6 PICS Proforma Guidelines, SC6, 3 January 1991
SC21 N 5560	Liaison Statement to WG4 Concerning SMI-related Issues, SC6, 3 January 1991
SC21 N 5561	Liaison Statement to ISO/IEC JTC1/SC21 from ISO/IEC JTC1/SC18 on Problem with Filters in Distributed Office Applications, 3 January 1991
SC21 N 5564	Proposal for a New Work Item: ODP Trader - A Standard to Define the Role and Function of the Trader in Open Distributed Processing (ODP), 31 January 1991
SC21 N 5572	Report of the Ad Hoc CCIR/CCITT Experts Group Meeting on ISDN Satellite Matters 5-9 November 1990, Geneva, 7 January 1991
SC21 N 5575	Request for National Body Comment, SC21/WG1/CCITT, 7 January 1991
SC21 N 5576	Rapporteur's Report of the SC21/WG1/CCITT Collaborative Meeting on Security Frameworks, 7 January 1991
SC21 N 5580	New Area of Work for SC27/WG1 on IT Security Information Objects, 7 January 1991

SC21 N 5581	New Area of Work for SC27/WG1 on IT Security Terminology, 7 January 1991
SC21 N 5582	Corrections to the Joint Text of the Second Editions for CMIS and CMIP, 7 January 1991
SC21 N 5584	Information Technology - Open Systems Interconnection - Remote Procedure Call, Second Working Draft, SC21/WG6, 7 January 1991
SC21 N 5585	Call for Comment on RPC Bindings in the Computational Model, SC21/WG6, 7 January 1991
SC21 N 5586	Call for Comment on the Nature of the OSI RPC Service Boundary and Service Provider, SC21/WG6, 7 January 1991
SC21 N 5587	Call for Comment on RPC Exception Model, SC21/WG6, 7 January 1991
SC21 N 5588	Call for Comment on OSI RPC Interface Definition Notation (IDN), SC21/WG6, 7 January 1991
SC21 N 5590	Temporary Working Definitions for (RPC) Client and Server, SC21/WG6, 7 January 1991
SC21 N 5593	The Role of the Extended Application Layer Structure in the Standardization of RPC, ECMA, 7 January 1991
SC21 N 5596	Multiple Outstanding RPC Calls, ECMA, 7 January 1991
SC21 N 5597	RPC Context Handles, ECMA, 7 January 1991
SC21 N 5599	Notice of and Draft Agenda for the ISO/IEC JTC1/SC21 Meeting, 4 & 5 June 1991, Arles, France, SC21 Secretariat, 12 February 1991
SC21 N 5605	Subcommittee Report to the ISO/IEC JTC 1 Advisory Group Meeting, 19-21 February 1991, Washington, D.C., USA, 13 January 1991
SC21 N 5606	Working Draft for [Information Technology-Open Systems Interconnection-Structure of Management Information-Part X:] Generic Managed Objects [for CCITT Applications], 1 March 1991
SC21 N 5635	Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI), 23 January 1991
SC21 N 5657	Liaison Statements from CCITT SG VII to SC21/WG1 on Various Topics (conformance testing, OSI Reference Model regarding ISDN, OSI naming and addressing), 1 February 1991
SC21 N 5682	Contribution from WG11, Binding Techniques for Languages, 5 February 1991
SC21 N 5686	Managed Object Conformance Statement (MOCS) Proforma, 14 February 1991
SC21 N 5687	Management Information Registration Procedure, Working Draft, 14 February 1991
SC21 N 5707	Position Statement on PICS Notations, SGFS, 1 March 1991
SC21 N 5714	Resolutions of the ISO/IEC JTC1 Advisory Group Meeting, Washington, D.C., 19-21 February 1991, 8 March 1991
SC21 N 5731	Progression of the Upper Layers Security Standards, Canada, 4 April 1991
SC21 N 5732	Use of Presentation Layer in Providing Confidentiality/Integrity, Canada, 4 April 1991
SC21 N 5733	Proposed ASN.1 Useful Type to Support Presentation Layer Confidentiality/Integrity, Canada, 4 April 1991
SC21 N 5734	Proposed Working Draft for Part 2 of Generic Security Exchange ASE Definition, Canada, 4 April 1991
SC21 N 5737	Recommendation on Progression for CD 9075.2 Information Technology - Database Languages - SQL2, 10 April 1991
SC21 N 5738	Minutes of Editing Meeting for CD 9075.2, April 1991
SC21 N 5756	The Proliferation of Managed Objects, UK, March 1991
SC21 N 5757	Work on Security Within SC21, UK, March 1991
SC21 N 5758	Discussion Paper on Conformance and Registration, BSI, March 1991
SC21 N 5764	Information Retrieval, Transfer and Management for USA (ANSI), 23 April 1991

SC21 N 5803	Extended Relationship Management, USA, 28 March 1991
SC21 N 5815	A General Model for Managed Object Relationships, Canada, 28 March 1991
SC21 N 5816	Position on RPC Modelling, ECMA, 28 March 1991
SC21 N 5817	Binding Concepts Within RPC, ECMA, 28 March 1991
SC21 N 5818	Proposal for RPC Service Definition and Protocol Specification Parts, ECMA, 28 March 1991
SC21 N 5819	Modelling Rationale for OSI RPC, ECMA, 28 March 1991
SC21 N 5821	Contribution on the [RPC] Computation Model, ECMA, 28 March 1991
SC21 N 5822	Proposal for the Use of the XALS in the Standardization of RPC, ECMA, 28 March 1991
SC21 N 5823	Position on RPC Context Handles, 28 March 1991
SC21 N 5826	EWOS Working Document on Behavior of DSAs for Distributed Operations, EWOS/EGDIR/91/A/713, 3 April 1991
SC21 N 5830	SC21 Standards Maintenance, AFNOR, 3 April 1991
SC21 N 5833	TP/CCR Extensions - Proposed Restructure for Future Work, USA, 3 April 1991
SC21 N 5835	Discussion Paper on Association Pools as an Extension of ACSE, WG5, 4 April 1991
SC21 N 5836	USA Discussion Paper on Subtransactions, 4 April 1991
SC21 N 5840	Comments on the Relationship Between Concepts and Models for OSI and ODP, USA, 3 April 1991
SC21 N 5845	Questions and Issues Concerning Combined Use of CMISE and TP, USA, 4 April 1991
SC21 N 5848	Request for Documenting Requirements for More Performant Association Establishment, 4 April 1991
SC21 N 5849	USA Requirements to Reactivate the Multipeer Data Transmission Project (JTC 1.21.09.01), USA, 4 April 1991
SC21 N 5851	USA Contribution to SC21 on the Conceptual Schema Topic, USA, 4 April 1991
SC21 N 5853	Call for Contributions on SC21 N 5077 Clause 3.1, Formalization of User Defined Operation Definition, April 1991
SC21 N 5856	Discussion Paper on Multi-Protocol Testing, SC21/WG1 and CCITT SG VII Collaborative Meeting on Conformance, Phoenix, 7-14 February 1991, 5 April 1991
SC21 N 5857	Proposed liaison to SGFS on Proforma Conformance Issues, April 1991
SC21 N 5858	Call for Contributions on Multi-User Test Methods, April 1991
SC21 N 5864	Disposition of Comments on DIS 9646-1, April 1991
SC21 N 5866	Disposition of Comments on DIS 9646-2, April 1991
SC21 N 5868	Disposition of Comments on DIS 9646-4, April 1991
SC21 N 5870	Disposition of Comments on DIS 9646-5, April 1991
SC21 N 5886	Cooperation Between TP and CCR, 16 April 1991
SC21 N 5887	Liaison Statement to CCITT Q20/VII and SC21/WG4 Directories Regarding Use of case Exact String Syntax in Transaction Processing, 16 April 1991
SC21 N 5888	Liaison Statement to the Registration Authority for the Register of Object Identifier Components Allocated to Areas of Joint ISO-CCITT Work - Request for Updates to the Register, 16 April 1991
SC21 N 5889	Liaison Statement to SC21/WG6 CASE and ULCT Groups Regarding ACSE PICS Proforma, 16 April 1991
SC21 N 5890	Liaison Statement to SC21/WG6 CASE and ULA Groups Regarding ACSE Application Context Negotiation, 16 April 1991
SC21 N 5891	Contribution to the New Work Item: Management Information Register and Registration Procedures, Germany, 16 April 1991

SC21 N 5893	Liaison Statement to SC21/WG6 on Notation for Conditional ASN.1, 16 April 1991
SC21 N 5903	Presentation Connection-Oriented Abstract Test Suite (ATS), Common Partial ATS (CD expected in June 1992; DIS in June 1993; IS in June 1994)
SC21 N 5904	Liaison Statement to JTC 1/SC18, SC21 and SC27 - Tracking of Existing and New Security Related Work Items, ISO/TC 68/SC2, 23 April 1991
SC21 N 5928	Disposition of Comments on DIS 10729-1, April 1991
SC21 N 5933	Conventions for the Definition of OSI Services, CD June 1990; DIS March 1991; IS expected March 1992
SC21 N 5934	Collection of Definitions of OSI Vocabulary (April 1991 Version), Rapporteur on Q17: OSI Vocabulary, 12 June 1991
SC21 N 5978	Review of SC21 Operation and Structure, May 1991
SC21 N 5984	Report of the Interim Q25/VII and Q26/VII Rapporteur Group Meetings, 11-15 March 1991, 9 May 1991
SC21 N 5997	USA Position on Use of RTSE by SC21 Standards, 12 June 1991
SC21 N 6002	Liaison to SC21 on Directory's Use of ISO 9066 (ROSE), WG4, 12 June 1991
SC21 N 6006	Use of Systems Management for Administration of the Directory, WG4, JTC1 N 1440, 3 July 1991 (new work item)
SC21 N 6007	FTAM Document Type for Directory, WG4, May 1991 (new proposal) (WD status projected for June 1992; CD November 1992, IS June 1994)
SC21 N 6008	Proposed New Question Q4/4 on Directory Schema Migration, 29 July 1991
SC21 N 6017	Comments on Standardization of Application Programmatic (sic) Interfaces, WG4, May 1991
SC21 N 6018	Resolutions of the Eighth SC21/WG4 Meeting, Arles, 20-27 May 1991, 20 June 1991
SC21 N 6019	Minutes of the Eighth SC21/WG4 Meeting, Arles, 20-27 May 1991, May 1991
SC21 N 6020	SC21/WG4 Convenor's Report to the ISO/IEC JTC1/SC21 Plenary Meeting, Arles, June 1991, 20 June 1991
SC21 N 6021	[Information Technology - Open Systems Interconnection - Systems Management - Part s:] Scheduling Function, 29 July 1991
SC21 N 6023	Work Plan for SC21/WG4 Systems Management, 20 June 1991
SC21 N 6029	Proposal for the Establishment of a Managed Object Advisory Group, WG4, 20 June 1991
SC21 N 6035	Enhanced Event Management and Log Control, WG4, 1 July 1991 (new work item)
SC21 N 6036	Planning and Organization of SC21/WG4 Systems Management Activities, 20 June 1991
SC21 N 6037	Need for Security Services with OSI Management, SG4, July 1991
SC21 N 6039	Development of Enhanced Functionality for CMIS/P, WG4, 1 July 1991 [CD 1993, DIS 1994, IS 1995], JTC1 N 1438, 3 July 1991 (voting ends 21 October 1991) (new work item)
SC21 N 6040	OSI Software Management - Working Draft, WG4, 20 June 1991
SC21 N 6041	General Relationship Model--Working Draft, WG4, 20 June 1991
SC21 N 6046	Response to Systems Management Tutorial NWI Proposal Ballot (contains initial May 1991 draft of the Systems Management Tutorial), WG4, 20 June 1991
SC21 N 6047	First Working Draft on Management Domains, WG4, 20 June 1991 (part of the Extended Systems Management Architecture)
SC21 N 6048	Working Document on Management Knowledge Management, WG4, 20 June 1991 (part of the Extended Systems Management Architecture)
SC21 N 6049	Working Document on Synchronization, WG4, 20 June 1991 (part of the Extended Systems Management Architecture)
SC21 N 6057	Report of the Conceptual Schema Topic Meeting, Arles, 9 October 1991

SC21 N 6058	Minutes of the Conceptual Schema Topic Meeting, October 1991
SC21 N 6059	Initiative on Conceptual Schema and Common Data Modelling Facility, Conceptual Schema Topic Meeting, Arles, 25 May 1991
SC21 N 6060	Proposed Draft Answer to Question Q6/1--Versions and Extensibility, SG6, 30 May 1991
SC21 N 6061	Progression of Methodology and Guidelines for the Development of Application Layer Standards, WG6, June 1991
SC21 N 6063	Use of Object Identifiers to Access Directory Information, WG6, 12 June 1991
SC21 N 6066	Liaison to SC6/WG4, SC21/WG6, SC21/WG4, and SC21/WG1 on Managed Object Structures, 24 July 1991
SC21 N 6068	Modelling Recovery in the Application Layer, WG6, 12 June 1991
SC21 N 6069	Proposed New WG6 Question Q6/2 on the Relationship Between the OSI Upper Layer Architecture and ODP, 24 July 1991
SC21 N 6070	Working Draft Answer to the Proposed WG6 Question on the Architectural Relationship Between OSI and ODP, 25 June 1991
SC21 N 6071	Guidelines for Application Context Definition, WG6, 12 June 1991
SC21 N 6073	List of Open and Resolved Issues--June 1991 Version, June 1991
SC21 N 6076	Resolutions of the ISO/IEC JTC1/SC21/WG7 Meeting in Arles, France, 22-31 May 1991, 5 September 1991
SC21 N 6078	WG7 Convenor's Report to the SC21 Plenary Meeting in Arles in June 1991, 25 July 1991
SC21 N 6079	CD 10746-2, Reference Model of ODP - Part 2: Descriptive Model SC21/WG7, 30 May 1991
SC21 N 6080	Working Draft for Part 3 of the Reference Model for ODP, SC21/WG7, 30 May 1991
SC21 N 6081	Working Document on Topic 4.3 - Function and Interface Definitions, 31 May 1991
SC21 N 6082	Recommendation X.9zz: Basic Reference Model of Open Distributed Processing - Part 5: Architectural Semantics, Specification Techniques and Formalisms, 21 August 1991
SC21 N 6083	Working Document Partial Text for Part 1 and Part IV of the Reference Model for ODP, SC21/WG7, 30 May 1991
SC21 N 6084	Working Document on Topic 9.1 - ODP Trader, 31 May 1991
SC21 N 6085	Revised NP on ODP Trader, SC21/WG7, 30 May 1991
SC21 N 6086	Resolution of Ballot Comments on the NP on ODP Trader, SC21/WG7, 30 May 1991
SC21 N 6088	Proposal for a WG7 Question on the Suitability of the Formal Description Technique Z for Use in ODP, 31 May 1991
SC21 N 6096	Working Draft of Security Exchange ASE - Part 1: Security Exchange Model and Specification Framework, WG6, 3 June 1991 [Part 2: Security Exchange ASE Service Definition, Part 3: Security Exchange ASE Protocol Specification; and Part 4: Security Exchange ASE PICS Proforma]
SC21 N 6097	Working Draft of Security Exchange ASE - Part 2: Security Exchange ASE Service Definition, WG6, 3 June 1991
SC21 N 6098	Working Draft of Security Exchange ASE - Part 3: Security Exchange ASE Protocol Specification, WG6, 3 June 1991
SC21 N 6099	Authentication Services for Distributed Applications, WG6, 1 July 1991 [WD 5/91, CD 5/92, DIS 5/93, IS 5/94], JTC1 N 1437, 3 July 1991 (new work item)
SC21 N 6110	Session Layer Extension to Support Re-Use of Transport Connections, WG6, JTC1 N 1436, 3 July 1991 (voting ends 21 October 1991) (new work item)
SC21 N 6111	Information Technology - Open Systems Interconnection - Remote Procedure Call, Third Working Draft, WG6, 25 June 1991

SC21 N 6119	RO Extensions--Concepts, Model, and Notation, WG6, 12 June 1991
SC21 N 6120	RO Extensions--Service Definition, WG6, 12 June 1991
SC21 N 6121	RO Extensions--Protocol Specification, WG6, 12 June 1991
SC21 N 6126	LOTOS Description of CCR Service and Protocol, WG6, JTC1 N 1435, 3 July 1991 (voting ends 21 October 1991) [PDTR 5/92, DTR 6/93, TR 6/94] (new work item)
SC21 N 6130	Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression, WG6, June 1991
SC21 N 6131	Working Draft on Light-Weight Encoding Rules for ASN.1, WG6, 8 July 1991
SC21 N 6132	Call for National Body and Liaison Organization Comment on Symmetric Synchronization, 25 July 1991
SC21 N 6133	Abstract Syntax Model, WG6, June 1991
SC21 N 6136	Light Weight Encoding Rules (LWER) for ASN.1, WG6, JTC1 N 1434, 3 July 1991 (voting ends 21 October 1991) (draft is SC21 N 6131) (new work item)
SC21 N 6151	Enhancements to ROSE Service Definition, Protocol Specification, and Concepts, Model and Notation, WG6, 1 July 1991; JTC1 N 1433, 3 July 1991 (new work item)
SC21 N 6157	Answer to CCITT SG VII Q 23 on OSI Reference Model Regarding ISDN, May 1991
SC21 N 6158	Final Answer to Q1/62 (Quality of Service Architectural Issues), WG1, May 1991
SC21 N 6159	Framework on Quality of Service, WG1, May 1991 (new project proposal for a TR) (PDTR projected for May 1993, DTR May 1994, TR May 1995)
SC21 N 6160	Catalogue of PICS Proforma Notations, WG1, July 1991
SC21 N 6162	ISO/IEC JTC1/SC21/WG1 Programme of Work, 29 July 1991
SC21 N 6167	Revised Draft Guide to Open Systems Security, WG1, July 1991
SC21 N 6172	Security Enhancement to Directory (Extension to ISO/IEC 9594-8), WG1, July 1991 (new work item) (CD projected for 4th quarter 1992, DIS second quarter 1993, IS second quarter 1994)
SC21 N 6189	Liaison Statement to SC18 on [SGML] Conformance, WG1, 22 July 1991
SC21 N 6194	Final Answer to Q1/63.1--Meaning of Conformance to Objects in the Context of OSI Management, WG1, May 1991
SC21 N 6196	PICS Issues (Part 7 to ISO/IEC 9646), WG1, July 1991
SC21 N 6197	WG1 Position on the Reactivation of Project 1.21.9.1 (Multi-Peer Data Transmission), WG1, July 1991 (national body comments requested by 31 March 1992)
SC21 N 6198	Approved Commentaries on the OSI Basic Reference Model [SC21 SD-9], July 1991
SC21 N 6201	Working Draft on Formal Methods in Conformance Testing, WG1, July 1991
SC21 N 6204	List of Late Contributions and Output Documents of SC21/WG1 Arles Meeting, 22-30 May 1991, May 1991
SC21 N 6205	Report of the ISO/IEC JTC1/SC21/WG1 Meeting, Arles, France, 29 July 1991
SC21 N 6210	Recommendations Approved by the ISO/IEC JTC1/SC21/WG1 at its Arles Meeting, 22-30 May 1991, May 1991
SC21 N 6213	Motive for the Establishment of a SC21 Special Group on Conceptual Schema and Common Data Modelling Facilities Issues, 9 October 1991
SC21 N 6217	Recommendations of the ISO/IEC JTC1/SC21/WG5 Meeting, Arles, 23-31 May 1991, June 1991
SC21 N 6219	Liaison statement to ISO/IEC/JTC1/SC21 Lower Layer Security, 10 November 1990
SC21 N 6222	CD 10026-6, Information Technology - Open Systems Interconnection - Distributed Transaction Processing - Part 6: Unstructured Data Transfer, 23 August 1991
SC21 N 6224	Proposed EDIFACT/FTAM Document Type, WG5, July 1991

SC21 N 6225	Response to Liaison from JTC1/SC24/WG3 about CGM Document Types, 3 July 1991
SC21 N 6226 Rev	OSI Distributed Transaction Processing Statement of Results, 14 June 1991
SC21 N 6227	Virtual Terminal Support of ODA, WG5, July 1991
SC21 N 6231	Preliminary Model and Service Definition for Queued Data Transfer, WG5, July 1991
SC21 N 6232	Preliminary TP Security Model, WG5, June 1991
SC21 N 6233	Issues Relating to TP Association Management, 29 July 1991
SC21 N 6236	Requirements and Issues for Subtransactions, WG5, June 1991
SC21 N 6239	Working Document for TP Commit Optimization, WG5, June 1991
SC21 N 6240	Requirements and Issues on Separation of Data and Commitment Flows, WG5, June 1991
SC21 N 6243	TP Testing Methodology (Revised), WG5, June 1991
SC21 N 6244	Conformance Test Suite for the TP Protocol - Part 1: Test Suite Structure and Test Purposes, WG5, June 1991
SC21 N 6248	Resolutions of the ISO/IEC JTC1/SC21/WG6 Meeting, 22-31 May 1991, Arles, France, 10 June 1991
SC21 N 6249	Resolutions of the SC21/WG3 Meeting, Arles (May 1991), 23 July 1991
SC21 N 6251	Proposed New Question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM),, 23 July 1991
SC21 N 6252	Revision of the IRDS Framework, WG3, 1 July 1991 (new work item)
SC21 N 6253	Proposed New Question on the Approach to Remote IRDS Access, , 23 July 1991
SC21 N 6257	Recommendation on NWI for Stored DBL Procedures, 23 July 1991
SC21 N 6260	Report of WG1 Convenor, May 1991
SC21 N 6261	Standing Document 8: SC21 Schedule of Meetings, 20 June 1991
SC21 N 6262	Notes of Ad Hoc Meeting on SC21 Organization, Arles, June 1991
SC21 N 6263	SC21 Contribution to JTC1 SWG Meeting on Organization, 17-19 June 1991, ANSI, 10 June 1991
SC21 N 6264	WG6 Convenor's Report to the SC21 Plenary Meeting in Arles in June 1991, 25 July 1991
SC21 N 6265	ISO/IEC JTC1/SC21/WG5 Convenor's Report to the ISO/IEC JTC1/SC21 Plenary Meeting in Arles, 26 August 1991
SC21 N 6273	Resolutions of the Seventh Plenary Meeting of ISO/IEC JTC1/SC21, 4-5 June 1991, Arles, France, 20 June 1991
SC21 N 6275	Plan to Mechanize the ISO/IEC JTC1 Secretariat (SC21 Pilot Project), 26 June 1991
SC21 N 6277	JTC1 Advisory Group Resolution 8:1991 Regarding Long Range Planning Group (LRPG) Items of High Importance (JTC1 N 1192) and A Vision for the Future (extract contained in JTC1 N 1351), 26 June 1991
SC21 N 6306	[Information Technology - Open Systems Interconnection - Systems Management -] Performance Management Working Document - Seventh Draft, 29 July 1991
SC21 N 6307	[Information Technology - Open Systems Interconnection - Systems Management -] Confidence and Diagnostic Test Categories [for CCITT Applications], 29 July 1991
SC21 N 6314	Directory Implementor's Guide , Version 5, CCITT, July 1991
SC21 N 6317	Recommendations on IRDS Services Interface Progression (CD 10728), 1 August 1991
SC21 N 6346	Liaison Statement to JTC1/SC21 on Data Link Layer Security, 16 August 1991
SC21 N 6348	Liaison Statement to JTC1/SC21 Regarding a NP on "Framework for CIM Systems Integration", 16 August 1991
SC21 N 6370	Register of Object Identifier Components Allocated to Areas of Joint ISO/CCITT Work, 20 August 1991

SC21 N 6387	Minutes of the CD 10728 (IRDS Services Interface) Continuation Meeting, 20-24 May 1991, Arles, France, 5 September 1991
SC21 N 6398	Request for SGFS Member Comment on Standardization of Profile Test Specifications, 10 September 1991
SC21 N 6399	The Way Ahead, 10 September 1991
SC21 N 6403	Proposal for a New Work Item: Generic Operating System Interface, 10 September 1991
SC21 N 6404	Proposal for a New Work Item: API (Application Program Interface) for Windows Systems, 10 September 1991
SC21 N 6405	Proposal for a New Work Item: Model and Framework of Interfaces for Application Portability, 10 September 1991
SC21 N 6449	Calling Notice for SC21 Special Meeting on Conceptual Schema Facilities and Common Data Modelling Facilities, 9-13 March 1992, Renesse, The Netherlands, 9 October 1991
SC21 N 6455	Proposed ASN.1 Specification Framework for Part 1 of Generic Security Exchange ASE Definition (SC21 N 6096), 11 October 1991
SC21 N 6456	Contribution to Part 3 of Generic Security Exchange ASE Definition (SC21 N 6098), 11 October 1991
SC21 N 6457	Frameworks Overview, 15 October 1991
SC21 N 6458	Integrity Framework, 15 October 1991
SC21 N 6459	Confidentiality Framework, 15 October 1991
SC21 N 6460	Contribution on the Security Exchange ASE-Part 3, 15 October 1991
SC21 N 6461	Contribution on the Definition of ENCRYPTED and SIGNED in CD 8824-3 and CD 8824-4,15 October 1991
SC21 N 6462	Application Context for Systems Management with TP, 15 October 1991
SC21 N 6463	Response to SC21 N 5845, "Questions and Issues Concerning Combined Use of CMISE and TP", 15 October 1991
SC21 N 6464	Contribution for TP Testing Methodology, 15 October 1991
SC21 N 6465	Contribution on Test Purposes for TP, 15 October 1991
SC21 N 6469	Liaison Statement to SC21/WG4 - Generic Management Information, 22 October 1991
SC21 N 6470	Liaison Statement to CCITT SG XI/Q20 - Protocol Discriminator, 22 October 1991
SC21 N 6471	Liaison Statement to SC21/WG1 - PICS Proforma Guidelines for 22 October 1991
SC21 N 6475	USA Contribution on the Security Exchange ASE - Part 1, 22 October 1991
SC21 N 6476	CD 10026-4.2, Information Technology - OSI - Distributed Transaction Processing - Part 4: PICS Proforma CD 10026-4 Editing Meeting, Arles, May 1991, 23 October 1991
SC21 N 6478	Target Dates for Completion of SC22 Projects, 7 November 1991
SC21 N 6482	Progress Report on ISO/IEC JTC1 and CCITT Cooperation, 23 October 1991
SC21 N 6485	CD 10164-13.2, Information Technology - OSI - Systems Management - Part 13: Summarization Function CD 10164-13 Editing Meeting, 23 October 1991
SC21 N 6493	Revised SC21 Management Guidelines SC21 Strategic Planning Rapporteur, 24 October 1991
SC21 N 6494	Revised OSI Reference Model - Working Group Version Q56 Rapporteur, 24 October 1991
SC21 N 6530	Report of the JTC1 Plenary Ad Hoc Group on EDI, 31 October 1991
SC21 N 6538	Proposed New SC21 Working Group Structure, 4 November 1991
SC21 N 6553	Japanese Position on the SC21 Restructuring, 7 November 1991
SC21 N 7016	Presentation Connection-Oriented Abstract Test Suite (ATS), Specific Partial ATS

SC21 N 7018	Common Partial Embedded ATS (CD text expected June 1992)
SC21/WG6 N 965	An OSI RPC Example Based on Other USA Positions, 22 January 1991
SC21/WG6 N 1123	UK Position on Alignment of Upper and Lower Layer Security Protocols, 4 November 1991
SC21/WG6 N 1124	UK Comment on SC21 N 6130, Generic Transfer Syntax Providing Upper Layers Security, 4 November 1991
SC21/WG6 N 1125	UK Contribution on Lightweight Encoding Rules for ASN.1, 4 November 1991
SC22 N 190	Specification for a Set of Common Language-Independent Data Types, working draft 4, 6 September 1990
SC22 N 194R	Specification for a Model for Common Language-Independent Procedure Calling Mechanisms, Version 2, 2 December 1990

II. CCITT RECOMMENDATIONS[3]

A. F-SERIES TELEMATIC SERVICES

CCITT F.200♦[4]	Teletex Service
CCITT F.200♦	Teletex Service, Annex C: Mixed Mode of Operation
CCITT F.201♦	Internetworking Between the Teletex Service and the Telex Service
CCITT F.400	Message Handling System and Service Overview
CCITT F.401	Naming and Addressing for Public Message Handling Services
CCITT F.410	The Public Messaging Transfer Service
CCITT F.415	Intercommunication with Public Physical Delivery Services
CCITT F.420	The Public Interpersonal Messaging (IMP) Service
CCITT F.421	Intercommunication Between the IPM Service and the Telex Service
CCITT F.422	Intercommunication Between the IPM Service and the Teletex Service
CCITT F.500	International Public Directory Services

B. I- SERIES ISDN SERVICES

CCITT I.110	General Structure of the I-Series Recommendations
CCITT I.111	Relationship with Other Recommendations Relevant to ISDNs
CCITT I.112	Vocabulary of Terms for ISDNs
CCITT I.113	Vocabulary of Terms for Broadband Aspects of ISDNs
CCITT I.120	Integrated Service Digital Networks (ISDNs)
CCITT I.121	Broadband Aspects of ISDNs
CCITT I.122	Framework for Providing Additional Packet Mode Bearer Services
CCITT I.130	Attributes for the Characterization of Telecommunications Services Supported by an ISDN and Network Capabilities of an ISDN
CCITT I.140	Attribute Techniques for the Characterization of Telecommunication Services Supported by an ISDN and Network Capabilities of an ISDN
CCITT I.141	ISDN Network Charging Capabilities Attributes
CCITT I.144	Number Identification Supplementary Services
CCITT I.200	Guidance to the I.200 Series of Recommendations
CCITT I.210	Principles of Telecommunications Services Supported by an ISDN
CCITT I.211	Bearer Services Supported by an ISDN
CCITT I.212	Teleservices Supported by an ISDN
CCITT I.220	Common Dynamic Description of Basic Telecommunication Services

---

[3] CCITT Recommendations are final versions of 1988 documents (Blue Book) unless otherwise indicated.

[4] The symbol ♦ is used throughout this Section to identify those recommendations included in the November 1991 (Sixth Edition) *NTIS Transition Strategy*.

CCITT I.221	Common Specific Characteristics of Services
CCITT I.230	Definition of Bearer Service Categories
CCITT I.231	Circuit-Mode Bearer Service Categories
CCITT I.232	Packet Mode Bearer Service Categories
CCITT I.240	Definition of Teleservices
CCITT I.241	Teleservices Supported by an ISDN
CCITT I.250	Definition of Supplementary Services
CCITT I.251	Number Identification Supplementary Services
CCITT I.252	Call Offering Supplementary Services
CCITT I.253	Call Completion Supplementary Services
CCITT I.254	Multiparty Supplementary Services
CCITT I.255	Community of Interest Supplementary Services
CCITT I.256	Changing Supplementary Services
CCITT I.257	Additional Information Transfer Supplementary Services
CCITT I.310	ISDN - Network Functional Principles
CCITT I.320	ISDN Protocol Reference Model
CCITT I.324	ISDN Network Architecture
CCITT I.325	Reference Configurations for ISDN Connection Types
CCITT I.326	Reference Configurations for Relative Network Resource Requirements
CCITT I.330	ISDN Numbering and Addressing Principles
CCITT I.331	Numbering Plan for the ISDN Era
CCITT I.332	Numbering Principles for Interworking Between ISDNs and Dedicated Networks with Different Numbering Plans
CCITT I.333	Terminal Selection in ISDN
CCITT I.334	Principles Relating ISDN Numbers/Subaddresses to the OSI Reference Model Network Layer Addresses
CCITT I.335	ISDN Routing Principles
CCITT I.340	ISDN Connection Types
CCITT I.350	General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs
CCITT I.351	Recommendations in Other Services Including Network Performance Objectives that Apply at T Reference Point of an ISDN
CCITT I.352	Network Performance Objectives for Connection Processing Delays in an ISDN
CCITT I.410	General Aspects and Principles Relating to Recommendations on ISDN User-Network Interfaces
CCITT I.411	ISDN User-Network Interfaces - Reference Configurations
CCITT I.412	ISDN User-Network Interfaces - Interface Structures and Access Capabilities
CCITT I.420	Basic User-Network Interface (ISDN)
CCITT I.421	Primary Rate User-Network Interface (ISDN)
CCITT I.430♦	Basic User-Network Interface - Layer 1 Specification (ISDN)
CCITT I.431♦	Primary Rate User-Network Interface - Layer 1 Specification (ISDN)
CCITT I.440♦	ISDN User-Network Interface - Data Link Layer General Aspects
CCITT I.441♦	ISDN User-Network Interface - Data Link Layer Specification
CCITT I.450♦	ISDN User-Network Interface - Layer 3 General Aspects (Q.921)
CCITT I.451♦	ISDN User-Network Interface - Layer 3 Specification (Q.931)
CCITT I.452	ISDN User-Network Interface - Layer 3 Specification - Generic Procedures for the Control of the ISDN Supplementary Services

CCITT I 460♦	Multiplexing, Rate Adaptation and Support of Existing Interfaces (ISDN)
CCITT I.461♦	Support of X.21 and X.21 bis Based DTEs by an ISDN (X.30)
CCITT I.462♦	Support of Packet Mode Terminal Equipment by an ISDN (X.31)
CCITT I.463♦	Support of DTEs with V-Series Type Interfaces by an ISDN
CCITT I.464♦	Multiplexing Rate Adaptation and Support of Existing Interfaces for Restricted 64 kbit/s Transfer Capability
CCITT I.500	General Structure of the ISDN Interworking Recommendations
CCITT I.510	Definitions and General Principles for ISDN Interworking
CCITT I.511	ISDN to ISDN Layer 1 Internetwork Interface
CCITT I.515	Parameter Exchange for ISDN Interworking
CCITT I.520	General Arrangement for Network Interworking Between ISDNs
CCITT I.530	Network Interworking Between an ISDN and a Public Switched Telephone Network (PSTN)
CCITT I.540	General Arrangement for Network Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services
CCITT I.550	General Arrangement for Network Interworking Between Packet Switched Public Data Networks (PSPDNs) and ISDNs for the Provision of Data Transmission Services
CCITT I.560	Requirements to be Met in Providing the Telex Service Within the ISDN
CCITT I.601	General Maintenance Principles of ISDN Subscriber Access and Subscriber Installation
CCITT I.602	Application of Maintenance Principles to ISDN Subscriber Installation
CCITT I.603	Application of Maintenance Principles to ISDN Basic Accesses
CCITT I.604	Application of Maintenance Principles to ISDN Primary Rate Accesses
CCITT I.605	Application of Maintenance Principles to Static Multiplexed ISDN Basic Accesses

C. T-SERIES TELEMATIC SERVICES

CCITT T.0	Classification of Facsimile Apparatus for Document Transmission Over the Public Networks
CCITT T.5♦	General Aspects of Group 4 Facsimile Apparatus
CCITT T.6♦	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus
CCITT T.50	International Alphabet No. 5
CCITT T.51♦	Coded Character Sets for Telematic Services
CCITT T.60♦	Terminal Equipment for Use in the Teletex Service
CCITT T.61♦	Character Repertoire and Coded Character Sets for the International Teletex Service
CCITT T.62♦	Control Procedures for Teletex and Group 4 Facsimile Services
CCITT T.62 bis	Control Procedures for Teletex and Group 4 Facsimile Services Based on Recommendations X.215/X.225
CCITT T.63♦	Provision for Verification of Teletex Terminal Compliance
CCITT T.70♦	Network-Independent Basic Transport Service for the Telematic Services
CCITT T.71♦	LAPB Extended for Half-Duplex Physical Level Facility
CCITT T.72♦	Terminal Capabilities for Mixed Mode of Operation
CCITT T.73♦	Document Interchange Protocol for the Telematic Services
CCITT T.90♦	Teletex Requirements for Internetworking with the Telex Service
CCITT T.91♦	Teletex Requirements for Real-Time Internetworking with the Telex Service in a Packet-Switching Network Environment

CCITT T.330♦	Telematic Access to Interpersonal Messaging System
CCITT T.400	Introduction to Document Architecture, Transfer and Manipulation
CCITT T.411	Open Document Architecture (ODA) and Interchange Format - Introduction and General Principles (see ISO 8613-1)
CCITT T.412	Open Document Architecture (ODA) and Interchange Format - Document Structures (see ISO 8613-2)
CCITT T.414	Open Document Architecture (ODA) and Interchange Format - Document Profile (see ISO 8613-4)
CCITT T.415	Open Document Architecture (ODA) and Interchange Format - Open Document Interchange Format (ODIF) (see ISO 8613-5)
CCITT T.416	Open Document Architecture (ODA) and Interchange Format - Character Content Architectures (see ISO 8613-6)
CCITT T.417	Open Document Architecture (ODA) and Interchange Format - Raster Graphics Content Architectures (see ISO 8613-7)
CCITT T.418	Open Document Architecture (ODA) and Interchange Format - Geometric Graphics Content Architectures (see ISO 8613-8)
CCITT T.419	Document Transfer and Manipulation (DTAM) - Composite Graphics Content Architectures
CCITT T.431	Document Transfer and Manipulation (DTAM) - Services and Protocols, Introduction and General Principles
CCITT T.432	Document Transfer and Manipulation (DTAM) - Services and Protocols, Service Definition
CCITT T.433	Document Transfer and Manipulation (DTAM) - Services and Protocols, Protocol Specification
CCITT T.441	Document Transfer and Manipulation (DTAM) - Operational Structure
CCITT T.501	Document Application Profile MM for the Interchange of Formatted Mixed Mode Documents (Mixed Mode)
CCITT T.502	Document Application Profile PM1 for the Interchange of Processible Form Documents (Teletex Processible Mode)
CCITT T.503	A Document Application Profile for the Interchange of Group 4 Facsimile Documents
CCITT T.504	Document Application Profile for Videotex Interworking
CCITT T.521	Communication Application Profile BTO for Document Bulk Transfer Based on the Session Service (According to Rules Defined in T.62 bis)
CCITT T.522	Communication Application Profile BT1 for Document Bulk Transfer
CCITT T.523	Communication Application Profile DM-1 for Videotex Interworking
CCITT T.541	Operational Application Profile for Videotex Interworking
CCITT T.561	Terminal Characteristics for Mixed Mode of Operation MM
CCITT T.562	Terminal Characteristics for Teletex Processing Mode PM1
CCITT T.563	Terminal Characteristics for Group 4 Facsimile Apparatus
CCITT T.564	Gateway Characteristics for Videotex Interworking

D. V-SERIES

CCITT V.5	Standardization of Data Signalling Rates for Synchronous Data Transmission in the General Switched Telephone Network
CCITT V.6	Standardization of Data Signalling Rates for Synchronous Data Transmission on Leased Telephone-Type Circuits
CCITT V.10/X.26♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communication

CCITT V.11/X.27♦	Electrical Characteristics for Balanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communications
CCITT V.20♦	Telex and Gentex Signalling on Radio Channels (Synchronous 7-Unit Systems Affording Error Correction by Automatic Repetition)
CCITT V.24♦	List of Definitions for Interchange Circuits Between DTE and DCE
CCITT V.25♦	Automatic Answering Equipment and/or Parallel Automatic Calling Equipment on the General Switched Telephone Network Including Procedures for Disabling of Echo Control Devices for Both Manually and Automatically Established Calls
CCITT V.25 bis♦	Automatic Calling and/or Answering Equipment on the General Switched Telephone Network (GSTN) Using the 100-Series Interchange Circuits
CCITT V.28♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits
CCITT V.31♦	Electrical Characteristics for Single-Current Interchange Circuits Controlled by Contact Closure
CCITT V.31 bis♦	Electrical Characteristics for Single-Current Interchange Circuits Using Opto Couplers
CCITT V.35♦	Data Transmission at 48 Kilobits per Second Using 60-108 kHz Group Band Circuits
CCITT V.36♦	Modems for Synchronous Data Transmission Using 60-108 kHz Group Band Circuits
CCITT V.37♦	Synchronous Data Transmission at a Data Signalling Rate Higher than 72 kbit/s Using 60-108 kHz Group Band Circuits
CCITT V.54	Loop Test Devices for Modems

E. X-SERIES PUBLIC DATA NETWORKS

CCITT X.1	International User Classes of Service in Public Data Networks and Integrated Services Digital Networks (ISDNs)
CCITT X.3♦	Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN).
CCITT X.4	General Structure of Signals of International Alphabet No. 5 Code for Data Transmission Over Public Data Networks
CCITT X.10	Categories of Access for DTE to Public Data Transmission Services Provided by PDNs and/or ISDNs through Terminal Adaptors
CCITT X.20♦	Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks
CCITT X.20 bis	Use on Public Data Networks of DTE Which Is Designed for Interfacing to Asynchronous Duplex V-Series Modems
CCITT X.21♦	Interface Between DTE and DCE for Synchronous Operation on Public Data Networks
CCITT X.21 bis♦	Use on Public Data Networks of DTE Which Is Designed for Interfacing to Synchronous V-Series Modems
CCITT X.22♦	Multiplex DTE/DCE Interface for User Classes 3-6
CCITT X.24♦	List of Definitions for Interchange Circuits Between DTE and DCE on Public Data Networks
CCITT X.25-84♦	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit, 1984
CCITT X.25-88	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit, 1988
CCITT X.28♦	DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Directory (Country)
CCITT X.29♦	Procedures for the Exchange of Control Information and User Data Between a PAD and a Packet Mode DTE or Another PAD
CCITT X.31♦	Support of Packet Mode Terminal Equipment by an ISDN

CCITT X.32♦	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Accessing a Packet Switched PDN Through a Public Switched Telephone Network or a Circuit Switched PDN
CCITT X.75-84♦	Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits Between PSDNs
CCITT X.75-88	Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits Between PSDNs
CCITT X.110	International Routing Principles and Routing Plan for Public Data Networks
CCITT X.141	General Principles for the Detection and Correction of Errors in Public Data Networks
CCITT X.150	Principles of Maintenance Testing for Public Data Networks Using DTE and DCE Test Loops
CCITT X.200	Reference Model of OSI for CCITT Applications (see ISO 7498)
CCITT X.208	Specification of Abstract Syntax Notation One (ASN.1) (see ISO 8824, Revised Edition)
CCITT X.209	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (see ISO 8825, Revised Edition)
CCITT X.210	OSI Layer Service Definition Conventions (see ISO TR 8509)
CCITT X.211	Physical Service Definition for OSI for CCITT Applications (see DIS 10022)
CCITT X.212	Data Link Service Definition for OSI for CCITT Applications (see ISO 8886)
CCITT X.213	Network Service Definition for OSI for CCITT Applications (see ISO 8348, 8348/AD 2, and 8348/AD 3)
CCITT X.214	Transport Service Definition for OSI for CCITT Applications (see ISO 8072, 1986)
CCITT X.215	Session Service Definition for OSI for CCITT Applications (see ISO 8826 and 8326/AD 2)
CCITT X.216	Presentation Service Definition for OSI for CCITT Applications (see ISO 8822)
CCITT X.217	Association Control Service Definition for OSI for CCITT Applications (see ISO 8649)
CCITT X.218	Reliable Transfer: Model and Service Definition (see ISO 9066-1)
CCITT X.219	Remote Operations: Model, Notation and Service Definition (see ISO 9072-1)
CCITT X.220	Use of X.200 Series Protocols in CCITT Modifications
CCITT X.223	Use of X.25 to Provide the OSI Connection-Mode Network Service for CCITT Applications (see ISO 8878, 1987)
CCITT X.224	Transport Protocol Specification for OSI for CCITT Applications (see ISO 8073)
CCITT X.225	Session Protocol Specification for OSI for CCITT Application (see ISO 8327 and 8327/AD 2)
CCITT X.226	Presentation Protocol Specification for OSI for CCITT Application (see ISO 8823)
CCITT X.227	Association Control Protocol Specification for OSI for CCITT Applications (see ISO 8650)
CCITT X.228	Reliable Transfer: Protocol Specification (see ISO 9066-2)
CCITT X.229	Remote Operations: Protocol Specification (see ISO 9072-2)
CCITT X.244	Procedure for the Exchange of Protocol Identification During Virtual Call Establishment on Packet Switched Public Data Networks
CCITT X.250	Formal Description Techniques for Data Communications Protocols and Services
CCITT X.290	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications (see DIS 9646-1 and DIS 9646-2)
CCITT X.300	General Principles and Arrangements for Interworking Between Public Data Networks, and Between PDNs and Other Public Networks
CCITT X.301	Description of the General Arrangement for Call Control Within a Subnetwork and Between Subnetworks for the Provision of Data Transmission

CCITT X.302	Description of the General Arrangement for Internal Network Utilities Within a Subnetwork and Immediate Utilities Between Subnetworks for the Provision of Data Transmission Services
CCITT X.305	Functionalities of Subnetworks Relating to the Support of the OSI Connection-Mode Network Service
CCITT X.310	Procedures and Arrangements for DTE Accessing Circuit Switched Digital Data Services Through Analogue Telephone Networks
CCITT X.320	General Arrangements for Interworking Between ISDNs for the Provision of Data Transmission Services
CCITT X.321	General Arrangements for Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services
CCITT X.322	General Arrangements for Interworking Between Packet Switched Public Data Networks (PSPDNs) and CSPDNs for the Provision of Data Transmission Services
CCITT X.323	General Arrangements for Interworking Between PSPDNs
CCITT X.324	General Arrangements for Interworking Between PSPDNs and Public Mobile Systems for the Provision of Data Transmission Services
CCITT X.325	General Arrangements for Interworking Between PSPDNs and ISDNs for the Provision of Data Transmission Services
CCITT X.326	General Arrangements for Interworking Between PSPDNs and Common Channel Signalling Network (CCSN)
CCITT X.327	General Arrangements for Interworking Between PSPDNs and Private Data Networks for the Provision of Data Transmission Services
CCITT X.353	Routing Principles for Interconnecting the Maritime Satellite Data Transmission System with Public Data Networks
CCITT X.400♦	Message Handling Systems (MHSs): System Model - Service Elements (see ISO 10021-1, MOTIS)
CCITT X.401♦	MHSs - Basic Service Elements and Optional User Facilities
CCITT X.402♦	MHSs - Overall Architecture (ISO 10021-2, MOTIS)
CCITT X.403♦	MHSs - Conformance Testing
CCITT X.407♦	MHSs - Abstract Service Definition Conventions (ISO 10021-3, MOTIS)
CCITT X.408♦	MHSs - Encoded Information-Type Conversion Rules
CCITT X.409♦	MHSs - Presentation Transfer Syntax and Notation [replaced by X.208 (ISO 8824 with DAD 1) and X.208 (ISO 8825 with DAD 1)]
CCITT X.410♦	MHSs - Remote Operations and Reliable Transfer Server [replaced by X.218 (ISO 9066-1), X.219 (ISO 9072-1), X.228 (ISO 9066-2), and X.229 (ISO 9072-2)]
CCITT X.411♦	MHSs - Message Transfer Layer (see ISO 10021-4, MOTIS)
CCITT X.413♦	MHSs - Message Store: Abstract Service Definition (ISO 10021-5, MOTIS)
CCITT X.419♦	MHSs - Protocol Specifications (ISO 10021-6, MOTIS)
CCITT X.420♦	MHSs - Interpersonal Messaging User Agent Layer (ISO 10021-7, MOTIS)
CCITT X.430♦	MHSs - Access Protocol for Teletex Terminals
CCITT X.500	The Directory - Overview of Concepts, Models, and Service (see ISO 9594-1)
CCITT X.501	The Directory - Models (see ISO 9594-2)
CCITT X.509	The Directory - Authentication Framework (see ISO 9594-8)
CCITT X.511	The Directory - Abstract Service Definition (see ISO 9594-3)
CCITT X.518	The Directory - Procedures for Distributed Operation (see ISO 9594-4)
CCITT X.519	The Directory - Protocol Specifications (see ISO 9594-5)
CCITT X.520	The Directory - Selected Attribute Types (see ISO 9594-6)
CCITT X.521	The Directory - Selected Object Classes (see ISO 9594-7)

F. Z-SERIES

CCITT Z.100	Specification and Description Language (SDL)
CCITT Z.110	Criteria for the Use and Applicability of Formal Description Techniques
CCITT Z.200	CCITT High Level Language (CHILL) [see DIS 9496.2]
CCITT Z.301	Introduction to the CCITT Man-Machine Language (MML)
CCITT Z.302	The Meta-Language for Describing MML Syntax and Dialogue Procedures
CCITT Z.311	Introduction to Syntax and Dialogue Procedures (MML)
CCITT Z.312	Basic Format Layout (MML)
CCITT Z.314	The Character Set and Basic Elements (MML)
CCITT Z.315	Input (Command) Language Syntax Specification (MML)
CCITT Z.316	Output Language Syntax Specification (MML)
CCITT Z.317	Man-Machine Dialogue Procedures (MML)
CCITT Z.321	Introduction to the Extended MML for Visual Display Terminals
CCITT Z.322	Capabilities of Visual Display Terminals (VDTs)
CCITT Z.323	Man-Machine Interaction
CCITT Z.331	Introduction to the Specification of the Man-Machine Interface
CCITT Z.332	Methodology for the Specification of the Man-Machine Interface - General Working Procedures
CCITT Z.333	Methodology for the Specification of the Man-Machine Interface - Tools and Methods
CCITT Z.341	Glossary of Terms (MML)

(This page intentionally left blank.)

APPENDIX F

ORGANIZATIONS FOR STANDARDIZATION

ORGANIZATIONS FOR STANDARDIZATION[1]

1. INTRODUCTION

This appendix provides an overview of NATO organizations and other bodies with responsibility for standardization in the fields of communications and information systems. Eventually, this appendix is intended to be expanded to show specific responsibilities of each of the standards bodies. Where appropriate, the charts show the class of STANAGs or other standards maintained by each organization. The emphasis in this appendix is on technical standards for data communications.

2. NATO STANDARDS BODIES

Figure F-1 (foldout) identifies the NATO bodies with responsibility for standardization in communications and information systems. The chart only shows the NATO bodies for which staff support is provided by the NATO Headquarters' staffs, with the exception of those associated with the NATO Communications and Information Systems Organization (NACISO). Operational requirements are the responsibility of the Military Committee, primarily through the Military Agency for Standardization (MAS). Procedural standards are the responsibility of the Allied Data Systems Interoperability Agency (ADSIA), which reports to the Military Committee through the NACISO. Technical standards are the responsibility of the Tri-Service Group on Communications and Electronics (TSGCE).

Many groups in NATO produce standards. A substantial part of the work takes place within the sturcture of the Conference of National Armaments Directors (CNAD), and is mainly concerned with material standardization. The Military Agency for Standardization (MAS) is exclusively concerned with standardization, primarily in the operational field. Specific topics are also dealt with by other groups under the Military Committee.

In 1983 the North Atlantic Council decided to establish a NATO Standardization Group (NSG) composed of national representatives from both the operational and materiel-oriented sides of defence departments, and representatives from the Major NATO Commands (MNCs), the International Staff (IS), the International Military Staff (IMS) and the MAS. The purpose of the Group is to provide a multi-national forum for the harmonisation of national views and the pursuit of NATO standardization activities. The Group is responsible to the Council for obtaining national and staff inputs with a view to the preparation of a composite NATO Standardization Programme (NSP) to be submitted to the NATO Standardization Tasking Authorities, after approval by the Council, for subsequent implementation.[2]

2.1 NATO Technical Standards Bodies

TSGCE has created a number of subgroups (SGs) and Project Groups (PGs) to develop and maintain technical standards for NATO. The subgroups and selected working groups (WGs) are:[3]

- SG4 on Navigation and Position Finding
- SG5 on Identification; seeks to enhance the interoperability of current identification equipment and to ensure the standardization, where necessary, to the NATO Identification System (NIS)
  - WG4 on Question and Answer (Q&A) System Interoperability; dedicated to Mark X/Mark XII issues, but will consider issues affecting the optimum implementation of the NATO Q&A
  - WG5 on Transition to the NIS Q&A

---

1 Appendix revised December 1991.

2 The North Atlantic Treaty Organization--Facts and Figures [NATO 1989].

3 *NATO Bodies in the Fields of Communications and Information Systems*, AC/317-D/23, NACISC, April 1988, NATO UNCLASSIFIED; and USMCEB *Directory--U.S. Participants in the International C3 Fora*, Military Communications Electronics Board, Joint Staff, March 1989, UNCLASSIFIED.

- WG6 on Data Processing

- SG9 on Data Distribution; focuses on the development of data communications protocols, specifically for the NATO OSI Reference Model
  - WG1 on OSI Layers 1-4--standards and functional profiles (to be phased out in 1992 or 1993)
  - WG2 on OSI Layer 5-7--standards and functional profiles (to be phased out in 1992 or 1993)
  - WG3 on Communications System/Network Interoperability (CSNI) (to be disbanded in 1992)
  - WG4 on Data Links
  - WG5 on Profiles
  - WG6 on Pan-Layer Issues
  - Ad Hoc Working Group (AHWG) on Security
  - AHWG on Integrated Services Digital Network (ISDN)
  - AHWG on OSI Management (to be phased out in 1992 or 1993)
  - PG3 on Multinational Information Distribution System (MIDS)
- SG11 on Tactical Communications
  - WG1 on Tactical Area Communications; seeks cooperation among the NATO nations in the development and procurement of tactical area communications for national forces
  - WG8 on Satellite Communications (SATCOM) Systems; seeks SATCOM interoperability between NATO and national military SATCOM systems
  - PG6 on Tactical Communications Systems for the Land Combat Zone--Post 2000; seeks, through a coordinated program, tactical communications systems designed to common standards
- SG12 on Information Systems
  - WG2 on Data Processing and Management
  - AHWG on Army Tactical Command and Control Information System (ATCCIS) (convened in conjunction with the meetings of the Technical Subgroup of the ATCCIS Permanent Working Group.

There are still two Project Groups reporting directly to the TSGCE:

- PG7 on Battlefield Information and Exploitation Systems (BICES)
- Special Working Group (SWG) on Ada Programming Support Environment (APSE), formed by 10 nations in 1987 to provide an environment in which tools can work together effectively to support information systems projects for the total development life cycle.

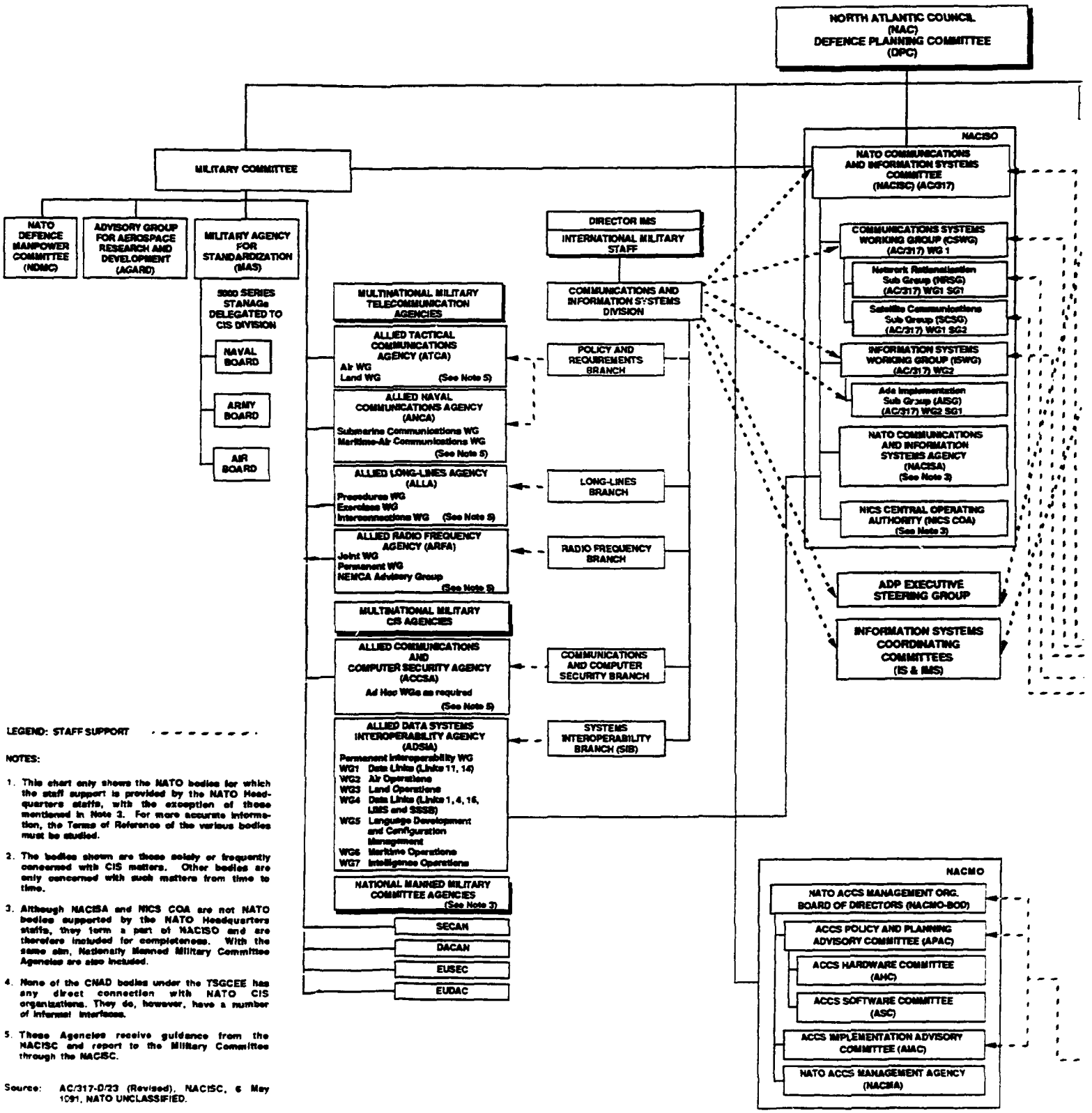
Liaison among these bodies (e.g., PG6 and SG9) is normally at the Secretary level. Plans are coordinated in annual meetings of the Secretaries and Action Officers of the Allied Tactical Communications Agency (ATCA), the Allied Naval Communications Agency (ANCA), the Allied Communications and Computer Security Agency (ACCSA), and the communications subordinate groups of TSGCE.[4]

To a limited degree, technical standards are also being addressed in the NATO Industrial Advisory Group (NIAG), specifically in SG6 on Compatibility of Naval Data Handling Equipment. NIAG SG6 is making recommendations on standards to be used in shipboard combat systems for data distribution, such as the Network Independent Interface (NIIF).

Table F-1 and Figure F-2 highlight the relationships among the NATO standards bodies whose responsibilities be discussed in a chart that follows. To clarify the relationships among the organizations and to emphasize those bodies concerned with technical standards, some of the NATO bodies have been left out and most of the names have been replaced with acronyms. Table F-1 provides the definitions of the acronyms for Figure F-2.

---

4 "Working Relationships," Note by the Secretary, AC/317-N/185, NACISC, 24 February 1989, NATO UNCLASSIFIED.



LEGEND: STAFF SUPPORT - - - - - - - - -

NOTES:

1. This chart only shows the NATO bodies for which the staff support is provided by the NATO Headquarters staffs, with the exception of those mentioned in Note 3. For more accurate information, the Terms of Reference of the various bodies must be studied.
2. The bodies shown are those solely or frequently concerned with CIS matters. Other bodies are only concerned with such matters from time to time.
3. Although NACISA and NICS COA are not NATO bodies supported by the NATO Headquarters staffs, they form a part of NACISO and are therefore included for completeness. With the same aim, Nationally Manned Military Committee Agencies are also included.
4. None of the CNAD bodies under the TSGCEE has any direct connection with NATO CIS organizations. They do, however, have a number of informal interfaces.
5. These Agencies receive guidance from the NACISC and report to the Military Committee through the NACISC.

Source: AC/317-D/23 (Revised), NACISC, 6 May 1991, NATO UNCLASSIFIED.

A

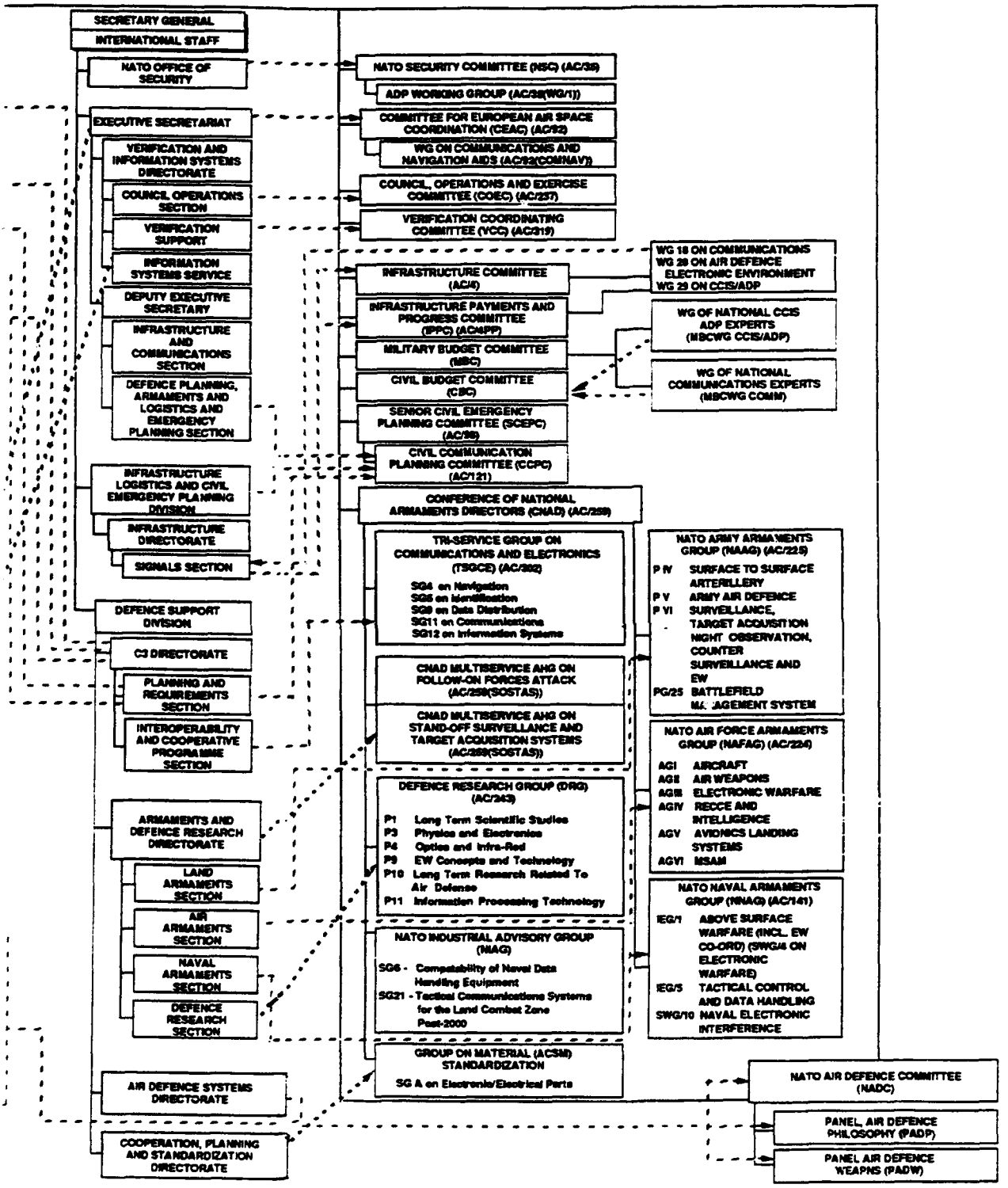


Figure F-1. NATO Bodies in the Fields of Communications and Information Systems

2.2 NATO OSI Standards Bodies

TSGCE SG9 has responsibility for the NATO OSI Reference Model and developing OSI STANAGs. SG9 also maintains the *NTIS Transition Strategy* [Purton 1987] that contains intercept recommendations.

TSGCE SG9 meets biannually, usually in March and October. Beginning in 1990, SG9 will meet approximately 6 to 8 weeks after the fall meetings of WG1 and WG2, to allow time for the nations to coordinate positions on issues developed by the working groups. Thus, the next meeting of SG9 is December 1990, while WG1 and WG2 will meet in October 1990. AHWGs meet approximately quarterly.

2.3 Standards Responsibilities of Selected NATO Bodies

Table F-2 is an incomplete first draft of an effort to identify the specific responsibilities of NATO organizations for technical standards. Eventually, this and similar tables for other groups of standards bodies will be analysed to identify overlaps as well as possible gaps in the standards coverage.

Table F-1. Acronyms and Titles of Key NATO Bodies in the Fields of Communications and Information Systems Standardization

Acronym	Name
NAC	North Atlantic Council
NSG	NATO Standardization Group
DPC	Defence Planning Committee
MC	Military Committee
AGARD	Advisory Group for Aerospace Research and Development
MAS	Military Agency for Standardization
MNCs	Major NATO Commands
ACE	Allied Command Europe
CHAN	Allied Channel Command
LANT	Allied Command Atlantic
ATCA	Allied Tactical Communications Agency
ANCA	Allied Naval Communications Agency
ALLA	Allied Long Lines Agency
ARFA	Allied Radio Frequency Agency
ACCSA	Allied Communications and Computer Security Agency
ADSIA	Allied Data Systems Interoperability Agency
SECAN	Communications Security and Evaluation Agency
DACAN	Distribution and Accounting Agency
EUSEC	European Security and Evaluation Committee European Distribution and Accounting Agency
IMS	International Military Staff
CIS DIV	Communications and Information Systems Division
NACISO	NATO Communications and Information Systems Organization
NACISC	NATO Communications and Information Systems Committee
CSWG	Communications Systems Working Group
NRSG	NATO Rationalization Subgroup
SCSG	Satellite Communications Subgroup
ISWG	Information Systems Working Group
AISG	Ada Implementation Subgroup
NACISA	NATO Communications and Information Systems Agency
NICS-COA	Central Operating Authority
CNAD	Conference of NATO Armaments Directors
TSGCEE	Tri-Service Group on Communications and Electronic Equipment
NAAG	NATO Army Armaments Group
NAFAG	NATO Air Force Armaments Group
NNAG	NATO Navy Armaments Group
DRG	Defence Research Group
NIAG	NATO Industrial Advisory Group
CEAC	Committee for European Airspace Coordination
NADC	NATO Air Defence Committee

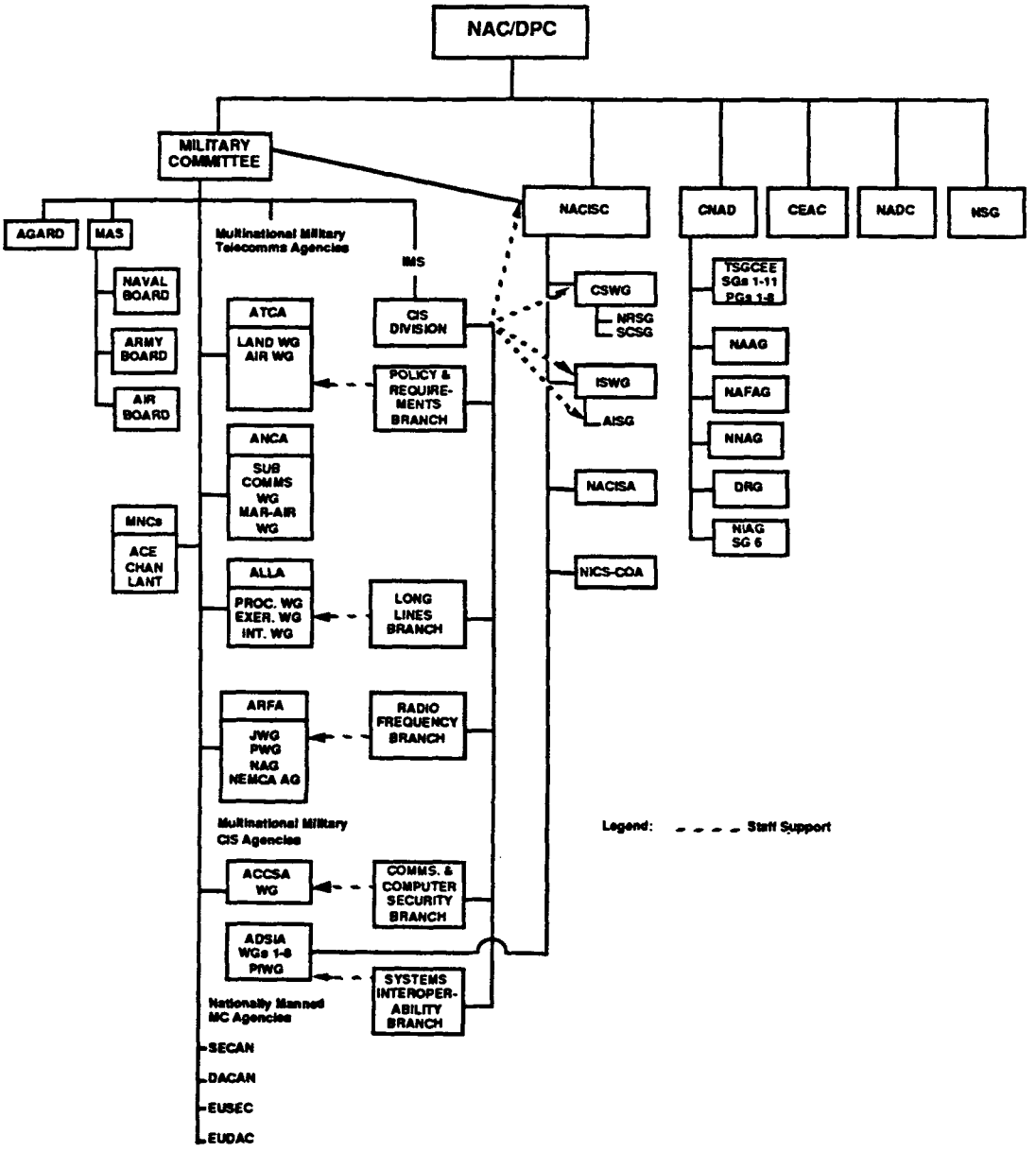


Figure F-2. NATO Standards Bodies for Communications and Information Systems

Table F-2. Responsibility for Standards in NATO Bodies

NATO Organization	Title	Standards Responsibility
CNAD	Conf of Nat'l Armaments Directors	
TSGCEE	Tri-Serv Group Comm-Electron Equipment	Technical Standards
SG1	Tactical Area Communications	STANAGs 4206-4214,4249,4290,4295,5000-5018
SG2	Tactical Radio Equipment	STANAGs 4197-4205,4245-46,4285-92,4335-39,5020
SG3	Multi-Functional Info Distribution	
SG4	Navigation and Position Finding	
SG5	Identification	
SG7	Channel Eval Tech in HF Communications	
SG8	Tactical SATCOM Terminal	STANAGs 4231-33, 4271
SG9	Data Processing and Distribution	NATO OSI Standards; STANAG 4250
AHWG-Security	OSI Security	NATO OSI Standards (Annex B)
AHWG-OM	OSI Network Management	NATO OSI Standards (e.g., Net Mgmt)
AHWG-ISDN	Integrated Services Digital Network	ISDN Standards for Open Systems
WG1	Lower 4 Layers of Reference Model	STANAGs 4251-54, 4261-64
WG2	Upper 3 Layers of Reference Model	STANAGs 4255-56, 4258-59, 4265-66
AHWG-MMHS	Military Msg Handling System	STANAG 4257
WG3	Comm System/Network Interoperability	MOU for Multinational Programme
SG10	Geographic Information	
PG2	NATO Identification System	
PG3	MIDS	
PG4	Low Cost INS for Ships	
PG5	Multi-Functional Inertial Sensor Assembly	
PG6	Tac Comm Post 2000-Land Combat	
PG7	BICES	
PG8	Tactical Spectrum Mgmt System	
OGN	Conformance Testing	
NIAG	NATO Industrial Advisory Group	
SG6	Naval Data Handling Equipment	Functional Profiles
NACISC	NATO Comm and Info Sys Committee	Oversight for Procedural Standards
CSWG	Comm Systems Working Group	
ISWG	Information Systems Working Group	
AISG	Ada Implementation Subgroup	
NACISA	NATO Comm and Info Sys Agency	
NICS-COA	Central Operating Authority	
MC	Military Committee	
IMS	International Military Staff	
CCCS Div	Command, Control and Comm System	STANAGs 5000-6999
CISD	Comm and Info Systems Divison	
SIB	Systems Interoperability Branch	
MAS	Military Agency for Standardization	Operational Standards (STANAGs 1000-3999)
Air Board	Air Board	STANAGs 8000-8999
ACCSA	Allied Comm and Comp Sec Agency	
PSN WG	Packet Switched Network	
ADSIA	Allied Data Systems Interop Agency	Procedural Standards
PIWG	Permanent Interoperability WG	
WG1	Maritime TDS Interoperability Standards	Data Links 10, 11, and 14
WG2	Air Operations	
WG3	Land Forces TDSs	
WG4	Inter-Service Data Systems	Data Links 1,16; IJMS,SSSB; STANAG 5516
WG5	Character-Oriented	Language Development and Configuration Mgmt
WG6	Maritime Operations	
WG7	Intelligence Operations	Intelligence Messages
WG8	Common Operational Vocabulary	
SECAN	Comm Security and Eval Agency	
NSG	NATO Standardization Group	Prepare Composite NATO Standardization Programme

3. INTERNATIONAL STANDARDS BODIES

Table F-3 identifies standards bodies from CCITT, ISO, and ECMA that recommend, develop, and maintain technical standards for communications and information processing. The primary international bodies are described below.[5] National standards bodies are identified in Chapter 4 of this appendix.

3.1 ISO/IEC

The International Organization for Standardization (ISO) has 89 members representing national standards bodies (e.g., AFNOR in France, JISC in Japan, ANSI in the United States, BSI in the United Kingdom). The International Electrotechnical Commission (IEC)[6] is a federation of more than 200 national committees working in the area of electronics and electrical standards with specific interest in information processing. ISO and IEC have formed a joint committee, Joint Technical Committee One (JTC1), to develop standards for information processing systems.

3.2 CCITT/CCIR

The Comite Consultatif International pour le Telephone et le Telegraph (CCITT) is the permanent organ of the Union Internationale des Telecommunications (UIT), which groups all the Postal Telephone Telegraph (PTT) administrations of the world's countries. CCITT develops standards in 4-year cycles and works closely with ISO to harmonize results. The Comite Consultatif International pour les Radiocommunications (CCIR) and the International Frequency Registration Board (IFRB) are the other two standards organs of the UIT; together with the CCITT, they are all based in Geneva.

3.3 CEN/CENELEC

The Comite Europeen de Normalisation (CEN) is a grouping of the national organizations of 16 countries of the European Community (EC) and the European Free Trading Association (EFTA).[7] CEN works in cooperation with the Comite Europeen de Normalisation Electrotechnique (CENELEC) to develop and publish European standards [normes europeennes (ENs)]. CENELEC deals exclusively with electrotechnical standards and CEN works with standards in all other areas. Based in Brussels, CEN/CENELEC works to harmonize standards that are established by its members and to create European standards where no other appropriate standards exist. CEN/CENELEC members include AFNOR (France), UNI (Italy), DIN (Germany), BSI (United Kingdom), IBN (Belgium), DCQ (Portugal), and SIS (Sweden).

CEN/CENELEC standards are initially distributed for comment by member bodies in the form of an experimental standard (ENV[8]) or a European prestandard (prENV). Future technical work in developing proposals for ENVs has now been taken over by the European Workshop for Open Systems

---

5 "La Galaxie de la Normalisation," Telecoms Magazine, 1989; *The OMNICON Index of Standards for Distributed Information and Telecommunication Systems*, OMNICON, 1987; and "The Value and Use of IT Standards in Public Procurement," PPSC-IT N268.1, Commission of the European Communities, August 1988, UNCLASSIFIED.

6 The IEC is also known as the Commission Electrotechnique Internationale (CEI).

7 The EFTA is also known as the Association Europeenne de Libre Exchange (AELE).

8 The "V" in ENV is for "Vornorm," and indicates a standard based on DIS or other draft standards that are not completely stable; modifications to ENV standards may eventually be required to bring them in line with international standards. ENVs are valid for 3 years--they are reviewed after 2 years and may then become an EN, be prolonged for another 2 years, be replaced by another ENV, or be withdrawn.

Table F-3. Responsibilities for Communications and Information Processing in International Civil Standards Bodies

International Organization	Title	Standards Responsibility
CCITT	International Consult Comm Telephone Telegrams	
SG I	Definitions, Operation & Quality of Service	
SG II	Operation of Telecommunication Network & ISDN	
SG III	General Tariff Principles	
SG IV	Transmission Maintenance	
SG VII	Data Communication Networks	OSI standards; facilities, I/Fs
WG1	Network Services, Facilities, Prototypes	
WG2	Network Access Interfaces	
WG3	Internetworking, Switching, Signal	
WG4	Transmission & Message Handling	
WG5	Routing, Numbering, Layered Model	
SR ISDN	ISDN-Related Issues	
SR DEFs	Terms and Definitions	
SG VIII	Telematic Services	OSI standards; FAX, teletex, videotex
WG1	Terminal Characteristics	
WG2	Common Protocols & Internetworking	
SG IX	Telegraph Networks & Terminal Equipment	
SG X	Languages & Methodology for Telcomm Applications	
SG XI	ISDN & Telephone Network Switching	
SG XII	Transmission Performance of Telephone Network	
SG XV	Transmission Systems	
SG XVII	Data Transmission over Telephone Network	
SG XVIII	Digital Networks including ISDN	OSI standards for ISDN
CCIR	International Radio Consultant Committee	
CEN	European Communications for Standardization	
CENELEC	European Communications for Telecom Standardization	
CEPT	European Conf of Postal & Telecom Administration	
CCH	Harmonization Coordination Committee	
CAC	Commercial Action Committee	
CLTA	Liaison Committee for Transatlantic Telecommunications	
ECMA	European Computer Manufacturing Association	
TC29	Text Preparation & Interchange	Telematic services; text/office systems
TC32	Communications, Networks & Systems Interconnection	OSI standards
TG1	Public Data Networks	
TG3	Local Area Networks	
TG6	Interfaces to Private Switching Networks	
TG7	Transport & Network Layers	Layer 3 and Layer 4 OSI standards
COS	Corporation for Open Systems	
COSINE	Corporation for Open Systems in Europe	
EMUG	European MAP User Group	
ETSI	European Telecommunication Standards Institute	
EWOS	European Workshop on Open Systems	

Table F-3. (Continued)

International Organization	Title	Standards Responsibility
ISO	International Organization for Standardization	
JTC1 (TC97)	Technology Committee on Information Processing Systems	Promote standards worldwide
TSG-1	Tech Study Group on IAP	Interfaces for Application Portability
SC1	Vocabulary	
SC2	Character Sets & Information Coding	
SC6	Telecommunications and Info Exchange Between Systems	OSI standards
WG1	Data Link Layer	Layer 2 OSI standards
WG2	Network Layer	Layer 3 OSI standards
WG3	Physical Layer	Layer 1 OSI standards
WG4	Transport Layer	Layer 4 OSI standards
WG5	Architecture, Layers 1-4	OSI Architecture
SC7	Software Development & Systems Documentation	
WG2	Documentation	
WG3	Software Quality Characteristics	
SC11	Flexible Magnetic Media	
SC13	Interconnection of Equipment	
SC14	Representation of Data Elements	
SC15	Labelling and File Structure	
SC17	Identification and Credit Cards	
SC18	Text and Office Systems	Message handling protocols
WG4	Text Interchange	MOTIS
WG9	User System Interfaces & Symbols	
SC20	Data Cyrptographic Techniques	
SC21	Information Retrieval, Transfer, & Management	OSI and other standards
WG1	OSI Architecture	OSI architecture, concep schema
WG3	Database (not part of OSI)	
WG4	OSI Management	
WG5	Specific Application Services	Layer 7 (TM, FTAM, JTM, VT)
WG6	Session & Presentation Layers; ASCEs	Layer 5 and layer 6 OSI standards
WG7	Open Distribution Procedures (not part of OSI)	
SC22	Languages	
WG15	POSIX	
SC23	Optical Digital Data Disks	
SC24	Computer Graphics	(Work formerly done by SC21/WG2)
SC47B	Microprocessor Systems	
SC83	Information Technology Equipment	
IEC	International Electrotechnical Commission	
IFIP	International Federation for Information Processing	
ITSTC	Information Technology Steering Technology Committee	
OSITOP	OSI for Technical & Office Protocol	
OSF	Open Software Foundation	
POSI	Promotion Conference for OSI	Asia-Oceania workshop/standards forum
SOGITS	Senior Official Group for Info Tech Standardization	Commission of European Communities
SOGT	Senior Official Group on Telecommunications	Commission of European Communities
SPAG	Standards Application & Promotion Groups	
UER	European Union on Radiobroadcasting	
X/OPEN	X/OPEN	

(EWOS). When proposed international standards are harmonized with national standards, harmonized documents (HDs) are produced. When adopted, an HD must be used and national deviations can only exist temporarily. European norms (ENs) must be adopted as national standards, and any conflicting national standards must be withdrawn. An example standard is ENV 41201, Private Message Handling System. A second class of standards promulgated by CEN/CENELEC are the Telecommunications European Norms (NETs), which are common technical specifications covering access to networks and equipment. Examples are NET2 (X.25 Access) and NET3 (ISDN Basic Access).

CEN/CENELEC standards originate as draft documents, standards proposals, and implementors guides developed by various standards promoting organizations. When stable, these documents are reviewed and coordinated by the European Telecommunications Standards Institute (ETSI) and EWOS and are issued for comment as functional specifications, recommendations, and technical specifications. When the review is complete, they are forwarded to CEN/CENELEC, or to the Conference Europeenne des Postes et Telecommunications (CEPT), for final standards development.[9]

3.4 ECMA

The European Computer Manufacturer Association (ECMA) represents a group of about 30 manufacturers in Europe. ECMA, based in Geneva, acts as observer at ISO and as a consultant at CCITT. ECMA takes an active role in the definition of functional profiles with EWOS.

3.5 SPAG

The Standards Application and Promotion Group (SPAG), based in Brussels, was created by 12 major European manufacturers (e.g., Bull, ICL, Siemens). SPAG seeks to accelerate standardization by selecting, among all OSI standards, a limited number for implementation. The stacks of standards are called profiles and are developed toward supporting complete applications, such as FTAM. SPAG has made a major contribution to the rapid progress of European experimental standards (ENVs) and standards (ENs).

3.6 OSITOP

Open Systems Interconnection for Technical and Office Protocol (OSITOP) is an association of users (such as BNP, EDF/GDF) for the promotion of ISO functional profiles and the concept of TOP.

3.7 EMUG

The European Manufacturing Automation Program (MAP) User Group (EMUG) was created in 1985 by a large group of manufacturers. It aims to promote the MAP standards in Europe. Specific groups in the nations, such as the Club Informatique des Grandes Enterprises Francaises (CIGREF) in France, are appointed to be EMUG's representatives. A key element of MAP, the Manufacturing Message Specification (MMS) has reached DIS status (DIS 9506).

3.8 EWOS

The European Workshop on Open Systems (EWOS) promulgates harmonized technical proposals for functional profiles of OSI standards and corresponding conformance test specifications. EWOS has been given the responsibility for technical work in developing proposals for ENVs, with increased involvement of users. When complete, the proposals are submitted to CEN/CENELEC. The founding members of EWOS include CEN, CENELEC, ECMA, EMUG, OSITOP, Reseaux Associes pour le Recherche Europeenne (RARE, Association of European Research Networks), and the Corporation for Open Systems Interconnection Networking in Europe (COSINE). The member bodies of EWOS have agreed not to undertake on their own any new work on the development of functional standards.

3.9 Support to the Commission of the European Community (CEC)

The Senior Official Group for Information Technology Standardization (SOGITS) and the Senior Official Group on Telecommunications (SOGT) assist the CEC in the implementing legislation for

---

9 Briefing on EUROPE 92--The European Community's Approach to Integration in the Information Technology Area, Fred Griefenstein, Softsiel Corporation, San Diego, 15 May 1989.

information technology standards. The Public Procurement Subcommittee in the Information Technology Sector (PPSC-IT) enforces the role of standards in public procurement for the CEC.

3.10 ITSTC

The Information Technology Steering Technical Committee (ITSTC) provides recommendations for European members in three areas: standards (the Information Technology Ad-hoc Expert Group for Standards), manufacturing/automation (the Information Technology Ad-hoc Expert Group for Manufacturing), and certification (the Information Technology Ad-hoc Expert Group for Certification). While the ITSTC does not produce standards, it does define programmes for European standards and organizes and coordinates the work.

3.11 CEPT/ETSI/UER

Three consortia represent the interests of public telecommunication administrations of European countries, including France, the United Kingdom, and Germany. The Conference Europeenne des Postes et Telecommunications (CEPT) coordinates political aspects and prepares technical specifications for member administrations (but does not produce any standards). The CEPT has 20 member countries and works closely with CEN/CENELEC. The European Telecommunications Standards Institute (ETSI) is an organization created within CEPT to prepare specifications concerning public telecommunications networks. The Union Europeenne de Radiodiffusion (UER) is a technical committee with the aim of harmonizing radio broadcasting system standards; its proposals are transmitted to the CCIR and the IEC. The UER has 32 countries actively participating and 45 associated member bodies.

3.12 COS/COSINE

The Corporation for Open Systems (COS) and the Corporation for Open Systems Interconnection Networking in Europe (COSINE) participate in the development of functional profiles for OSI and plays an active role in setting standards for testing OSI products for conformance to the international standards and profiles. COS is based in Vienna, Virginia, in the United States, and COSINE is based in Paris. COS has over 60 member organizations, both vendors and users.

COSINE is a project established by the CEC to promote internetworking facilities between industrial and academic research and development communities throughout Europe. Participating countries are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and Yugoslavia.

The COSINE project is set to achieve its objective of establishing a pan-European OSI data networking infrastructure for European researchers by the end of 1992. COSINE is intended as an enabling or catalytic project, not a long-term operational activity. The Reseaux Associes pour Recherche Europeene (RARE), which exists to coordinate and promote networking activities for the European research community, could add an operational or service role to its present representative, promotional, and coordinating functions and take over any activities from COSINE that remain necessary after the end of the project.[10]

3.13 X/OPEN

X/OPEN is a non-profit consortium developing extensions to UNIX SVID operating system standards to support a distributed transaction processing environment that meets OSI standards. X/OPEN is developing a Common Applications Environment to promote software portability. Alignment of both activities with the emerging POSIX standards is planned.

3.14 OSF

Created in 1988, the Open Software Foundation (OSF) is a group of over 90 information systems companies (including International Business Machines) for the promotion of standards, such as the POSIX standard for operating system interfaces.

---

10 "COSINE on Target for 1992," in *OSN: The Open Systems Newsletter*, volume 5, issue 5/6, May/June 1991, pp. 14-17.

3.15 IFIP

The International Federation for Information Processing (IFIP) is a group of international experts drawn principally from universities and also from some industries (e g., Xerox, Bell). IFIP has contributed to the work of ISO on the OSI model and, more recently, to the work on X.400-type message handling systems.

3.16 POSI

Created by six major vendors in Japan and the Nippon Telephone and Telegraph (NTT), the Promotion Conference for Open Systems Interconnection (POSI) is the equivalent to SPAG in Europe and to COS in the United States. POSI is an Asia-Oceania regional forum for the international workshops on OSI, and as such, seeks agreements among vendors to ensure interoperability and compatibility of products. The POSI regional workshop is known as the Asia-Oceania Workshop (AOW).

3.17 ODAC

Six major international computer companies formed the Open Document Architecture Consortium (ODAC) in early 1991 to develop a toolkit of software that conforms to the ISO ODA standard. The toolkit will be openly licensed to allow other computer companies and systems developers to build software applications using ODAC's published specifications. It is expected to be available in 1993. The consortium members are currently: Digital, ICL, Siemens Nixdorf Informationsysteme, Groupe Bull, IBM, and Unisys. The Consortium has been established as a European Economic Interest Group in Brussels. [OSN 1991b, 24]

3.18 OSINET

OSINET was formed in 1984 under the auspices of NIST. Governed by its membership it works in three specific areas: (1) the research and development of test scripts which are used in OSI interoperability testing, (2) the interoperability testing and registration of announced OSI products, and (3) the demonstration and promotion of ISO technology. The U.S.-based organization comprises 55 members and recently voted to reorganize under the auspices of COS [OSN 1991b, 23].

4. NATIONAL STANDARDS BODIES

This section identifies national standards bodies and their responsibilities for standards development or use.[11] Additional contributions to this section would be welcomed.

4.1 Belgium

The Institut Belge de Normalisation (IBN) is the primary standards body for Belgium.

4.2 Canada

The Canadian Standards Association (CSA) is responsible for the development of OSI standards in Canada. The Standards Council of Canada (SCC) is a Canadian national non-governmental agency that develops standards policy. The SCC provides coordination and support for the National Standards System (NSS) and supports Canada's participation in international standards work.

4.3 Denmark

Danish Standards Association (Dansk Standardiseringsrad) is the ISO member body from Denmark. It is also the member body for CEN.

4.4 France

The Association Francaise de Normalisation (AFNOR) is the French official organization for normalization/standardization and the French member body for ISO. It works with manufacturers, users, and administration. It promulgates international standards in France, chooses working groups in which

---

[11] *The OMNICON Index of Standards for Distributed Information and Telecommunication Systems*, OMNICON, 1987, UNCLASSIFIED.

France is to take an active part, manages French technical experts, and defines/coordinates the proposals they must put forward in discussions. The AFNOR role also includes giving information--it sends out literature on national and international standards and answers questions from manufacturers and users. AFNOR standards are classified according to the activity to which they relate. For example, Class Z corresponds to data processing. The Union Technique de l'Electricite (UTE) is the member of CENELEC from France and an active participant in AFNOR for the development and exploitation of standards for electricity and electronics.

4.5 Germany

The Deutsches Institut fur Normung (DIN) is the official organization for standardization for the Federal Republic of Germany and Berlin (West) and is the member body of ISO and CEN.

4.6 Netherlands

The Nederlands Normalisatie-Instituut (NNI) is the ISO member body for the Netherlands. When ISO or CCITT standards are translated or modified, they are issued by NNI as NENs. For example, NEN-ISO 3309 is a translation of an ISO HDLC standard.

4.7 United Kingdom

The British Standards Institute (BSI) is the UK member of ISO and the recognized body for the preparation and promulgation of British national standards.

4.8 United States

The American National Standards Institute (ANSI) is the U.S. member of ISO and a U.S. clearinghouse for voluntary standards.

Table F-4 identifies ANSI and other standards bodies[12] in the United States, both civil and military, that recommend, develop, manage, and maintain technical standards for communications and information processing.

Table F-5 identifies all the current Technical Committees (TCs) currently active in ANSI for Infomation Processing Systems (X3).

In the United States, the process of defining standards is voluntary and is coordinated by ANSI. ANSI accredits organizations such as professional and technical societies, trade associations, or consumer and labor groups to develop or adopt standards in various areas. Three types of organizations can create a standard: (1) Accredited Sponsor (AS), (2) Accredited Organization (AO), and (3) Accredited Standards Committee (ASC) [Cargill 1989, 103].

Under the AS method, an organization sponsors a drive for standardization and begins the canvass method by inviting comments on the proposed standard from anyone who cares or may be materially affected by it. This method is appropriate only when substantial agreement on the document to be standardized already exists, as was the case with the Ada programming language standard [Cargill 1989, 104].

---

12 Similar tables need to be developed for standards bodies in other nations. Additional contributions will be included in future editions of this working paper.

Table F-4. Responsibilities for Communications and Information Processing in U.S. Standards Bodies [13]

U.S. Organization	Title	Standards Responsibility
ANSI X3	Information Processing	
X3S3	Technology Committee (TC) on Data Communications	Devel of US OSI standards; input to ISO JTC1/SC21
X3S3.1	Task Group on Data Communications Planning	General standardization efforts
X3S3.2	Task Group on Communications Vocabulary	Data transmission vocabulary
X3S3.3	Task Group on Network Layer	Directory, management, routing, ISDN
X3S3.4	Task Group on Control Procedures	Protocols, procedures, & management; X.25
X3S3.5	Task Group on Communications Systems Performance	Nomenclature, presentation & performance measurement
X3S3.7	Task Group on Public Data Network Access	ISDNs, gateways (X3.100, X.25, X.75, X.32)
X3T2	Technology Committee on Data Interchange	
X3T3	Technology Committee on ODP	
X3T4	Technology Committee on Security Techniques	
X3T5	Technology Committee on OSI	Development of US OSI standards; input to ISO JTC1/SC21
X3T5.1	OSI Architecture; Reference Model	FDTs; Conf Testing; Sec. Open Distributed Proc
X3T5.4	Task Group on OSI Management Protocols	Management, MIS, directory service
X3T5.5	Presentation and Application Layers	CL mode, VT, ANS.1
X3T5.7	Task Group on OSI Security Techniques	
X3T6	Task Group on Non-Contact Information Systems Interface	
X3T9	Technology Committee on I/O Interface	
X3T9.2	Task Group on Lower Level Interface	
X3T9.3	Task Group on Device Level Interface	
X3T9.5	Task Group on Local Distribution Data Interface	
X3V1	Office and Publishing Systems	
X3V1.1	Task Group on User Requirements M.S T.	
X3V1.3	Task Group on Document Architecture	
X3V1.4	Task Group on Text Interchange	
X3V1.5	Task Group on Content Architecture	
X3V1.8	Task Group on Text Description and Process Language	
X3V1.9	Task Group on User Systems Interface/Symbols	
X3V1.10	Task Group on Font Resources	
USCCITT	US Organization for CCITT	
NC	National Committee	
GS-A	Telecommunication policies & services	
SG-B	WATTC-1988	
SG-C	Worldwide telephone network	
SG-D	Data and ISDN	
JWP	Joint Working Party on ISDN	
IEEE	Institute for Electrical and Electronic Engineering	
802	Committee on Local Area Networks	
Ad-hoc	Study Group on Functional Requirements	
802.1 .	Overall architecture of LANs/internetwork	
802.1A	Glossary	
802.1B	Network Management	
802.1D	Mac Sublayer Interconnection	
802.1E	System Load Protocol	
802.1F	Recommended Practices for Development of IEEE 802	
802.1G	Mac Sublayer Interconnection	
802.1I	Standard Mac Bridges - FDDI Supplement	
802.2	Logical link control	
802.3 .	CSMA/CD	
802.4 .	Token-passing bus access methodology	
802.5 .	Token ring access methodology	
802.6 .	Metropolitan area networks	
802.7 .	Broadband tech adv group	
802.8 .	Fiber-optics tech adv group	
802.9 .	Integrated Voice and Data (IVD) LAN Interface Standard	
802.10 .	Secure local area networks	
P1003	POSIX	
P1201	Window Interface	

13 Updated from Accredited Standards Committee X3, Information Processing Systems, *Membership and Officers* X3/SD-6, April 1991.

Table F-4. (Continued)

U.S. Organization	Title	Standards Responsibility
COS	Corporation for Open Systems	Promote OSI; conformance testing
X/OPEN	X/OPEN	Promote portability and use of OSI
NIST	National Institute for Standards & Techology	Standards development and coordination; conformance
Workshops	Implementation Workshops	Develop design-to functional profiles
ASD(C3I)	Asst Sec Def C3I	
DASD C3	Deputy Assistant Secretary of Defense C3	
T&TC3	Theater and Tactical C3	Interoperability of C3 systems
IS	Information Systems	DoD transition to GOSIP
CIM	Corporate Information Management	Requirements and priorities for standards development
ASD(P&L)	Production and Logistics	
S&DS	Standardization & Data Management	Distribution of standards
DIA	Defense Intelligence Agency	
DISA (formerly DCA)	Defense Information Systems Agency	DoD Executive Agent for data comm protocol standards
DCS Organ	Defense Communications System Organization	
DCEC	Defense Communications Engineering Center	Lead on standards for long haul communications
JTC3A	Joint Tactical C3 Agency	Lead for tactical communication technical standards
JINTACCS	Joint Interoperability Tactical C2 Systems Program	Joint message standards
JMSWG	JTIDS Message System WG	TADIL J; J-Series messages and protocols
FSSG	Fire Support Subgroup	K-Series messages (and protocols)
JITF	Joint Interface Test Force	Testing Joint interfaces
JITC	Joint Interoperability Test Center	Testing Joint interfaces
CIM	Corporate Information Management	Developing Standards
JDSSC	Joint Data Systems Support Center	
WIS	WWMCCS Information System	
JSC	Joint Steering Committee	Develop common interoperability standards
PSSG	Protocol Standards Steering Group	Primary advisory body for standards policy issues
DTMP	DCPS Technical Management Panel	
DLA	Defense Logistics Agency	
DMSSO	Defense Materiel Specifcations & Standards Office	
NSA	National Security Agency	
JCS J-6J	Joint Tactical C3 Systems Division	Ensure Interoperability of TDSs
MCEB	Military Communications-Electronics Board	Coordinate representation to international standards bodies
USA DISC4	Director, Information Systems for C4	Technical requirements, interoperability
SAIS-ADO	RSI-Rationalization, Standards, & Interoperability	Interoperability and standards
DCSOPS	International RSI	Operational requirements, interoperability
PEO CCS	PEO Command & Control Systems	Interoperability of Army Tactical C2 Systems
PEO Comm	PEO Communications	Interoperability of Communications Systems
AMC	Army Materiel Command	Materiel standards
ICP-M	Office of International Cooperative Programs	
CECOM	Communications & Electronics Command	
C3D	C3 Directorate	Technical support and POC for standards
TRADOC	Training and Doctrine Command	
CAC	Combined Arms Command	Operational and procedural standards
SIGCEN	Signal Center	Communications standards
USAISC	Information Systems Command	
ISEC	Information Systems Engineering Command	
USN Info MGT	Information Management	
ASN RE&S/C3I&Space	C3I and Space	
CNO/SPAWAR	Space & Naval Warfare Systems Command	
CNO/Space,C2	Space & C2	
OP-945	Information Management Support	
NAVDAC	Naval Data Automation Command	
USMC MCRDAC SI	Systems Integration	Standards
MCCDC-WFC	Warfighting Center	Requirements
HQMC (C412) D4 Div P&I	Planning and Interoperability	Standards coordination
USAF AQ/DAS C4	Acquisitions-C4	
ACS C4 Sys	C4 Systems	
AF Comm Cmd	Communications Command	
AFSC	Air Force Systems Command	
ESD	Electronic Systems Division	
RADC	Rome Air Development Center	
TAC DRI	Tactical Air Command	

Table F-5. ANSI X3 Technical Committees[14]

X3A1	Optical Character Recognition	X3J11	C
X3B5	Digital Magnetic Tape	X3J12	DIBOL
X3B6	Instrumentation Tape	X3J13	LISP
X3B7	Magnetic Disks	X3J14	FORTH
X3B8	Flexible Disk Cartridges	X3J15	DATABUS
X3B9	Paper/Forms Layout	X3J16	C++
X3B10	Credit/Identificaton Cards	X3J17	Prolog
X3B11	Optical Digital Data Disks	X3J18	REXX
X3H2	Database	X3K5	Vocabulary
X3H3	Computer Graphics		
X3H4	Information Resource Dictionary System	X3L2	Codes & Character Sets
X3H5	Parallel Processing Constructs for High Level Programming Languages	X3L3	Picture Coding
		X3L8	Data Representation
X3J1	PL/1	X3S3	Data Communications
X3J2	BASIC		
X3J3	FORTRAN	X3T2	Data Interchange
X3J4	COBOL	X3T3	Open Distributed Processing
X3J7	APT	X3T4	Security Techniques
X3J9	PASCAL	X3T5	Open Systems Interconnection
X3J10	APL	X3T6	Non-Contact Information Systems Interface
		X3T9	I/O Interface
		X3V1	Text: Office & Publishing Systems
		X3W1	Office Machines

In the AO method, an existing group completes a standard in an area in which it has direct and material interest and a perceived expertise. Usually an industry trade group or association of industry experts or participants, the AO often has extant standards that are based on the methodologies of its profession or discipline [Cargill 1989, 105]. The IEEE Computer Society is an example of an AO.

The ASC takes groups and factions with diverse, even antagonistic viewpoints and melds them into a semicohesive whole, with the aim of engineering a solution that encompasses all of the diversity while maintaining the benefits of individuality. The key to the ASC is the Secretariat, held by a sponsoring organization, which provides legal, administrative, and financial backing [Cargill 1989, 107]. The Computer and Business Equipment Manufacturers Association (CBEMA) is the Secretariat for ASC X3 on Information Processing Systems standards. In addition to developing, reviewing, and approving proposed American National Standards, the ASCs coordinate standardization activities on the international level by participating in the ISO.

An ASC project is assigned an arbitrary project number followed by an alphabetic suffix describing its type:

- S. Study project to determine the feasibility and need for a development project that has been proposed to the ASC.

---

[14] Updated from Accredited Standards Committee X3, Information Processing Systems, *Membership and Officers*, X3/SD-6, April 1991.

- D. Development project formally recommended and approved to produce an American National Standard.
- DT. Development project to produce a Technical Report.
- R. Revision project to revise an existing approved American National Standard.
- RF. Reaffirmation project, as a result of the ANSI-required five year review when the Technical Committee recommends that an existing American National Standard be reaffirmed without change.
- M. Maintenance project, the status into which a Development project is automatically placed upon approval of an American National Standard by ANSI.
- L. Liaison project, formal recognition of relations with another standards body on a project for which X3 has no existing standard or work in process.
- I. International Development project, which is intended to result in an International Standard [CBEMA 1989, iv].

The National Computer Systems Laboratory (NCSL) at the NIST contributes to the development of industry-wide standards by leading and participating in the work of organizations such as ANSI, IEEE, and ISO. In addition it develops tests and test methods for new standards. NIST prepares and the Department of Commerce issues Federal Information Processing Standards Publications (FIPS PUBS). Wherever possible, the FIPS are aligned with or identical to ANSI or ISO standards. However, when the government needs a standard, and the industry and its standards groups do not respond to this need, the NCSL has the ability to develop its own FIPS [Cargill 1989, 213].

The Department of Defense (DoD) also issues standards, called MIL-STDs or DoD-STDs, through its Quality Standardization Program. Where there is no substantial or demonstrable advantage to DoD in the development of a new standard, non-Government specifications and standards are to be adopted [DoD 1976, 2]. The DISA is responsible for developing military standards in communications and information technology.

The Center for Information Management (CIM) Infrastructure office within DISA has the responsibility for defining requirements and priorities for standards development. The Protocol Standards Steering Group (PSSG) recommends DoD standards policies to the director of DISA. The Chief of the DISA Office of Interoperability and Standards chairs the PSSG. Other representatives are nominated from the Military Departments, Defense Agencies, Joint Staff, Office of the Secretary of Defense (OSD), Defense Research Advanced Projects Agency (DARPA), National Communications System (NCS), JTC^{3}A, and NIST. The Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) [formerly the Protocol Standards Technical Panel (PSTP)] was formed under the direction of the PSSG to investigate technical matters and develop recommendations for standardization. The focus of the PSTP's work in 1989 and 1990 was developing a military supplement to GOSIP. The report of the PSTP [PSTP 1991] was published on January 8, 1991.

Now a part of DISA, the JTC^{3}A is the lead agency for tactical communications standards. A new organization within the JTC^{3}A is the Center for Standards, which centralizes the standards activity of DISA. Two major standards bodies within the Center for Standards are the Joint Message Standards Working Group (JMSWG) and the Fire Support Subgroup (FSSG). The JMSWG is responsible for Joint Interoperability Tactical Command and Control System (JINTACCS) message text formats (MTFs) and tactical data links. The FSSG has developed a Variable Message Format (VMF) standard for bit-oriented messages expected to be used in fire support. A subordinate group to the JMSWG, the FSSG has recently been given responsibility for joint data communication standards for digital entry devices, such as the Digital Communications Terminal.

The Joint Technical Standards Steering Group (JTSSG) sets policy for and approves the products of the MIL-STD-187 and MIL-STD-188 series standards activities.

4.9 Standards Bodies in Non-NATO Nations

Finland is represented in ISO and IEC by the Suomen Standardisoimisliitto (SFS).

Sweden is represented in ISO by the Standardiseringskommisionen i Sverige (SIS). SIS coordinates with the Swedish Electrical Commission (SEK) and the Swedish Mechanical Standardization (SMS).

The Irish member of ISO and CEN is the National Standards Authority of Ireland (NSAI), an autonomous unit of the Institute for Industrial Research and Standards (IIRS).

The Japanese Industrial Standards Committee (JISC) oversees the Japanese Industrial Standards (JISs). The JISC is attached to the Agency of Industrial Science and Technology, Ministry of International Trade and Industry (MITI). JISC members include representatives from manufacturers, consumers, and knowledgeable individuals. Texts of standards approved by the relevant Minister and announced in the Government Gazette are published by the Japanese Standards Association (JSA). An Information Technology Standardization Technology Committee (INSTAC) within the Japanese Standards Association, the Telecommunications Technology Committee (TTC), the Interoperability Database System Development Project, and the Interoperability Association for Information Processing (INTAP) were established in 1985 to promote interoperability technology. INTAP has the responsibility to develop functional standards and conformance tests for OSI in Japan.

The Saudi Arabian Standards Organization (SASO) represents Saudi Arabia in ISO and IEC.

APPENDIX G

STATUS OF OPEN SYSTEMS STANDARDS DEVELOPMENT IN ISO/IEC

STATUS OF OPEN SYSTEMS STANDARDS DEVELOPMENT IN ISO/IEC [1]

1. INTRODUCTION

This appendix provides an overview of the work plans of selected technical committees and working groups in ISO/IEC. The purpose is to illustrate how rapidly international civil standards are being progressed in those areas applicable to ATCCIS. A compilation of ISO/IEC and CCITT standards relevant to ATCCIS is provided in Appendix D (by layer of the OSI Reference Model) and Appendix E (numerical listing). An overview of international standards bodies and their responsibilities for standards development is provided in Appendix F. The information in this Appendix is as of July 1990.

2. INFORMATION PROCESSING STANDARDS (JTC1)

Table G-1 provides[2] an overview of the work plans for the major working groups of ISO/IEC JTC1 SC21, whose responsibility is Information Retrieval, Transfer, and Management for OSI. The standards bodies included in this table are:

- WG1 on OSI Architecture
- WG3 on Database
- WG4 on OSI Management
- WG5 on Specific Application Services
- WG6 on Session and Presentation Layers
- WG7 on Open Distributed Processing.[3]

The symbols used in Table G-1 show the progress of a standard from its submission as a working draft (circulated to SC21), through the intermediate stages of committee draft (CD) or draft proposal (DP) and draft international standard (DIS), in becoming an international standard. In many areas, balloting as an international standard is planned for 1992 or earlier.

---

1 Effective date of this Appendix is December 1991.

2 These tables are based on a format developed by Technology Appraisals, Limited. The original versions of the tables were taken from Standard Status--SC21 Information Retrieval, Transfer, and Management for OSI," Alan Payton, OSN: The Open System Newsletter, Volume 2, Issue 5, Technology Appraisals, Limited, London, July 1988 (used with permission). The authors wish to acknowledge additional contributions from Alan Payton and Technology Appraisals, Limited, during the years 1989-1992.

3 The table for WG7 is short and is placed after the table for WG3.

Table G-1. Status of Standards Development In ISO/IEC JTC1 SC21/WG1

WG1 OSI ARCHITECTURE	CURRENT STANDARD	1992	1993	1994
OSI Reference Model	-			
Basic Reference Model	ISO 7498-1: 1984			
Revision	SC21 N 6152	▨	■	
Connectionless data transmission	ISO 7498 AD1			
Multipeer data transmission (MPDT)	ISO 7498 PDAD 2	PROJECT SUSPENDED		
Security architecture	ISO 7498-2: 1989			
Naming and addressing	ISO 7498-3: 1989			
OSI Service Conventions	TR 8509: 1987			
Conventions for service definition	DIS 10731	■		
Tutorial on Naming and Addressing	DTR 10730	■		
Concepts and Terminology for Conceptual	-			
Schema and information base	TR 9007: 1987			
Security Frameworks in Open Systems	DIS 10181			
Overview	WD 10181-1	▣	▨	■
Authentication	DIS 10182-2.2	■		
Access Control	CD 10181-3	▨ ■		
Non-Repudiation	WD 10181-4	▣	▨	■
Confidentiality	WD 10181-5	▣	▨	■
Integrity	WD 10181-6	▣	▨	■
Security audit framework	CD 10181-7	▨ ■		
Formal Methods in Conformance Testing	SC21 N 5112			▣
Conformance Testing Methodology and Framework	ISO 9646			
General aspects	ISO 9646-1: 1991			
Abstract tes. suite specifications	ISO 9646-2: 1991			
TTCN	ISO 9646-3: 1991			
TTCN extensions	PDAM 1	▨	■	
Test realisation	ISO 9646-4: 1991			
Requirements on test labs. and clients	ISO 9646-5: 1991			
Protocol profile tet specification	CD 9646-6	▨ ■		
Formal Description Techniques				
Estelle	ISO 9074: 1989			
Estelle tutorial	ISO 9074 DAM 1	■		
LOTOS	ISO 8807: 1989			
G-LOTOS	ISO 8807 DAM 1	■		
Guidelines for Application of Estelle, LOTOS and SDL	TR 10167: 1991			

Key: ☐ WD ▣ DP/CD ▨ DIS ■ ISO

Table G-1. (Continued)

WG1 OSI ARCHITECTURE (CONT'D)	CURRENT STANDARD	1992	1993	1994
Application Layer Structure (ALS)	ISO 9545: 1989			
Extended ALS (XALS)	DAM 1	■		
Modelling recovery in application layer	SC21 N 4901			
Modelling communication aspects of distr. applications	?			
Association Control Service Element (ACSE)	-			
Service definition	ISO 8649: 1988			
Protocol specification	ISO 8650: 1988			
Authentication	AM 1			
A-context specification	WDAM 2	▭	⊡	▨
PICS proforma	CD 8650-2	▨	■	
Committment, Concurrency, and Recovery (CCR)	-			
Service definition	ISO 9804: 1990			
Protocol specification	ISO 9805: 1990			
Enhancements	WDAM 1	⊡	▨	■
Session mapping changes	PDAM 2	■		
Restart	WDAM 3	⊡	▨	■
PICS proforma	CD 9805-2.2	▨	■	
Security Exchange Application Service Element (ASE)	-			
Model and specification framework	SC21 N 6096	⊡	▨	■
Service definition	SC21 N 6097	⊡	▨	■
Protocol specification	SC21 N 6098	⊡	▨	■
Practical Conditions for ACSE Authentication	?			
Representation of Numerical Values in Character Strings	ISO 6093: 1985	INACTIVE		
Remote Procedure Call (RPC)	-			
Model	SC21 N 6111	⊡ ▨	■	
Interface definition notation (IDN)	SC21 N 6111	⊡ ▨	■	
Service	SC21 N 6111	⊡ ▨	■	
Protocol	SC21 N 6111	⊡ ▨	■	
Procedures for Specific OSI Registration Authorities	ISO 9834			
General procedures	DIS 9834-1	■		
Joint JTC1/CCITT object identifiers	ISO 9834-3: 1990			
Application titles	DIS 9834-6	■		
Abstract syntaxes	ISO 8822/PDAM 3	■		
Transfer syntaxes	ISO 8823/PDAM 3	■		
Application contexts	WD 9834-ac	WORK SUSPENDED		
System titles	WD 9834-st	INACTIVE		
Authentication mechanisms	WD 9834-am	PROJECT TERMINATED		

Key: ▭ WD ⊡ DP/CD ▨ DIS ■ ISO

Table G-2. Status of Standards Development in ISO/IEC JTC1 SC21/WG3

WG3 DATABASE	CURRENT STANDARD	1992	1993	1994
Database Languages	-			
NDL	ISO 8907: 1987			
SQL (with integrity enhancement)	ISO 9075: 1989			
SQL 2	DIS 9075.2	■		
SQL 3	WD 9075.3	□	⊡	▨
Export/import for SQL	-		⊡	▨
Design Support for SQL Applications	SC21 N 5152	⊡	▨	■
Information Resource Dictionary System (IRDS)	-			
Framework	ISO 10027: 1990			
Services interface	DIS 10728	■		
Extensions	SC21 N 6259	□	⊡	▨
Export/import for IRDS	SC21 N 5137		⊡	▨
Command language	DP 8800-1			
Panel interface	DP 8800-2			
Reference Model of Data Management	DIS 10032	■		
Technical report on RM of data magement	SC21 N 4119		⊡	▨
Data Management Export/Import for SQL and IRDS	-			
Remote Database Access (RDA)	DIS 9579			
Generic model, service, and protocol	DIS 9579-1	■		
SQL specialization	DIS 9579-2	■		
Tutorial (future technical report)	SC21 N 3343	⊡	▨	■
Support for stored DBL statements	-			

Key: □ WD ⊡ DP/CD ▨ DIS ■ ISO

Table G-3. Status of Standards Development in ISO/IEC JTC1 SC21/WG7

WG7 DATABASE	CURRENT STANDARD	1992	1993	1994
Open Distributed Processing (ODP)	-			
Introduction	WD 10746-1	□	⊡	▨
Descriptive model	CD 10746-2	▨	■	
Framework for ODP standards	WD 10746-3	⊡	▨	■
User guide	WD 10746-4	□	⊡	▨
Architectural semantics, formalisms	WD 10746-5		⊡	▨

Key: □ WD ⊡ DP/CD ▨ DIS ■ ISO

Table G-4. Status of Standards Development in ISO/IEC JTC1 SC21/WG4

WG4 OSI MANAGEMENT	CURRENT STANDARD	1992	1993	1994
OSI Reference Model--Management Framework	ISO 7498-4: 1989			
Systems Management	-			
Overview	ISO 10040: 1991			
Tutorial	SC21 N 4942			
Extended systems management architecture	SC21 N 4943			
Relationship model	SC21 N 6041			
Object management function	ISO 10164-1: 1991			
State management function	ISO 10164-2: 1991			
Relationship management function	ISO 10164-3: 1991			
Alarm reporting function	ISO 10164-4: 1991			
Event report management function	ISO 10164-5: 1991			
Log control function	ISO 10164-6: 1991			
Security alarm reporting function	ISO 10164-7: 1991			
Security audit trail function	DIS 10164-8: 1991	■		
Objects and attributes for access control	CD 10164-9.2	▨ ■		
Accounting meter function	CD 10164-10.2	▨ ■	■	
Workload monitoring function	CD 10164-11.2	▨		
Test management function	CD 10164-12	▨ ■		
Summarization function	CD 10164-13	▨ ■		
Confidence and diagnostic testing	WD 10164-cdt	▣ ▨	■	
Time management function	WD 10164-A		▣	▨
Software management	WD 10164-sm		▣	▨
Response time monitoring	WD 10164-rtm		▣	▨
Scheduling function	WD 10164-s	▣	▨	■
Structure of Management Information	ISO 10165			
Management information model	ISO 10165-1: 1991			
Definition of management information	ISO 10165-2: 1991			
Guidelines for definition of managed objects	ISO 10165-4: 1991			
Generic management information	CD 10165-5	▨ ■		
Guidelines for conformance mgmt. statement	CD 10165-6	▨ ■		
Mgmt. information register and reg. procedure	WD 10165-7	▣ ▨	■	

Key: ▭ WD ▣ DP/CD ▨ DIS ■ ISO

Table G-4. (Continued)

WG4 OSI MANAGEMENT (CONT'D)	CURRENT STANDARD	1992	1993	1994
Common Management Information	-			
Service definition (CMIS)	ISO 9595: 1991			
Protocol specification (CMIP)	ISO 9596-1			
Support for allomorphism	PDAM 3		⊡	▨
Access control	DAM 4	■		
PICS proforma	DIS 9596-2	■		
The Directory	-			
Overview	ISO 9594-1: 1990			
Information framework	ISO 9594-2: 1990			
Abstract service definition	ISO 9594-3: 1990			
Distributed operations	ISO 9594-4: 1990			
Protocol specification	ISO 9594-5: 1990			
Selected attribute types	ISO 9594-6: 1990			
Selected object classes	ISO 9594-7: 1990			
Authentication framework	ISO 9594-8: 1990			
Replication and knowledge management	CD 9594-9.2	▨ ■		
Amendments on replication	PDAMs	▨ ■		
Amendments on schema	PDAMs	▨ ■		
Amendments on access control	PDAMs	▨ ■		
Amendments on enhanced search	PDAMs	▨ ■		
PICS proforma	WD 9594-10	⊡	▨	■

Key: □ WD ⊡ DP/CD ▨ DIS ■ ISO

Table G-5. Status of Standards Development in ISO/IEC JTC1 SC21/WG5

WG5 SPECIFIC APPLICATION SERVICES	CURRENT STANDARD	1992	1993	1994
Operating System Command and Response Language		INACTIVE		
Virtual Terminal (VT)				
Basic class VT service	ISO 9040: 1990			
Basic class VT protocol	ISO 9041-1: 1990			
Additional functional units	AM 2			
PICS proforma	DIS 9041-2	■		
File Transfer, Access and Management (FTAM)	-			
General description	ISO 8571-1: 1988			
Virtual filestore	ISO 8571-2: 1988			
File service definition	ISO 8571-3: 1988			
File protocol specification	ISO 8571-4: 1988			
PICS proforma	AM 2			
Filestore management	DAM 1	■		
Overlapped access	ISO 8571-5: 1990			
Service enhancements	PDAM 3	▨	■	
Security enhancements	WDAM 4	□ ▣	▨	■
Job Transfer and Manipulation (JTM)	-			
Concepts and services	ISO 8831: 1989			
Basic class protocol	ISO 8832: 1989			
Full protocol specification	AM 1			
Distributed Transaction Processing (TP)	-			
Model	DIS 10026-1	■		
Service	DIS 10026-2	■		
Protocol	DIS 10026-3	■		
Security (amendments)	SC21 N 6232	□	▣	▨
Association management (amendments)	SC21 N 6233	□ ▣	▨	■
Committment optimization (amendments)	SC21 N 6239	□ ▣	▨	■
Dialogue recovery and user suspension of dialogue	SC21 N 6235	▣	▨	■
Subtransactions	SC21 N 6236	□	▣	▨
Separation of TP data and committment flaws	SC21 N 6240	□	▣	▨
PICS proforma	CD 10026-4	▨	■	
Application context proforma	CD 10026-5	▨ ■		
Distributed Transaction Processing (TP)	-			
Unstructured data transfer	CD 10026-6	▨ ■		
Other data transfer modes	WD 10026-7	□ ▣	▨	■
Heuristic decisions (amendments)	SC21 N 4167	INACTIVE		
Terminal Management (TM)	-			
Model	CD 10184-1.2	▨	■	
Service	WD 10184-2	▣	■	
Protocol	WD 10184-3	▣	■	
Conformance Test Suites for FTAM	-			
Test suite structure and purposes	ISO 10170-1:1988			
Abstract test suite (ATS)	WD 10170-2	▣	▨	■
ACSE ATS embedded under FTAM	WD 10170-3	□	▣	▨
Presentation ATS embedded under FTAM	WD 10170-4	□	▣	▨
Session ATS embedded under FTAM	WD 10170-5	□	▣	▨
Conformance Test Suites for Basic Class VT Protocol	-			
Test suite structure and test purposes	CD 10739-1	▨ ■		
Conformance Test Suite for TP Protocol	SC21 N 6244	▣	▨	■

Key: □ WD ▣ DP/CD ▨ DIS ■ ISO

Table G-6. Status of Standards Development In ISO/IEC JTC1 SC21/WG6

WG6 OSI SESSION, PRESENTATION, AND APPLICATION SERVICE ELEMENTS	CURRENT STANDARD	1992	1993	1994
Data Descriptive File for Information Exchange	ISO 8211: 1985			
Revision	WD 8211.2			
Methodology Guidelines for Developing AL Stds.	SC21 N 4903	▨	■	
Upper Layer Architecture (ULA)	ISO 7498-1 PDAD3			
Upper Layer Security Model	CD 10745	▨	■	
Management information for OSI upper layers	-			
Session Layer Services and Protocols	-			
Basic session service definition	ISO 8326: 1990			
Basic session protocol specification	ISO 8327: 1990			
LOTOS description of session service	TR 9571: 1989			
LOTOS description of session protocol	TR 9572: 1989			
PICS proforma	CD 8327-2.2	▨	■	
Additional resynchronization functionality	PDAMs	▨ ■		
Presentation Layer Services and Protocols	-			
Basic CO presentation service definition	ISO 8822: 1988			
Connectionless mode presentative service	AM 1			
Basic CO presentation protocol specification	ISO 8823: 1988			
Symmetric synchronization	PDAM 2	▨	■	
Syntax registration	DAM 3	■		
Unlimited user data	PDAM 4	▨ ■		
Additional resynchronization functionality	DAM 5	■		
Confidentiality and integrity	WDAM 6	▫ ▨	■	
PICS proforma	DIS 8823-2	■		
Specification of ASN.1	ISO 8824: 1990			
Basic ASN.1	CD 8824-1	▨ ■		
Information object classes	CD 8824-2	▨ ■		
Constraint specification	CD 8824-3	▨ ■		
Parametenzation	CD 8824-4	▨ ■		
Specification of Basic Encoding Rules for ASN.1	ISO 8825: 1990			
Packed encoding rules	CD 8825-2	▨ ■		
Distinguished encoding rules	CD 8825-3	▨ ■		
Presentation layer cryptographic techniques	?			
Connectionless Services and Protocols	-			
Session CL protocol to provide CL mode	ISO 9548: 1990			
PICS proforma for CL session protocol	CD 9548-2	▨ ■		
CL presentation protocol to provide CL mode	ISO 9576: 1991			
PICS proforma for CL presentation protocol	DIS 9576-2	■		
CL ACSE service	ISO 8649 AD2: 1990			
CL ACSE protocol to provide CL mode	ISO 10035: 1991			
PICS proforma for A-unit-data protocol	?			
CL-mode operation for ALS	?			
Conformance Test Suite for Session Protocol	-			
Test suite structure and test purposes	DIS 10168-1	■		
Generic test suite	WD 10168-2		▫	▨
Abstract test suite for CS method	WD 10168-3	▫ ▨	■	
Test management protocol specification	DIS 10168-4	■		
Conformance Test Suite for Presentation Layer	-			
Test suite structure and test purposes	DIS 10729-1	■		
Test suite for ASN.1 encodings	WD 10729-2	▫ ▨	■	
Common presentation abstract test suite	WD 10729-3	▫	▨	■
Conformance Test Suite for ACSE Protocol	-			
Test suite structure and test purposes	DIS 10169-1	■		
Common ACSE abstract test suite	WD 10169-2	▫	▨	■
Conformance Test Suite for CCR Protocol	?		□	▫

Key: □ WD ▫ DP/CD ▨ DIS ■ ISO

APPENDIX H

INTERNATIONAL MILITARY AND OTHER STANDARDS BASED ON OSI STANDARDS OR USED IN OPEN SYSTEMS PROFILES

INTERNATIONAL MILITARY AND OTHER STANDARDS BASED ON OSI STANDARDS OR USED IN OPEN SYSTEMS PROFILES

I. NATO STANDARDS

A. OSI STANAGs

STANAG 4250♦	NATO Reference Model for OSI, NATO UNCLASSIFIED
STANAG 4250-1♦	Part 1--General Description, Revised Draft, May 1990, NATO UNCLASSIFIED
STANAG 4250-2♦	Part 2--Security, Draft (SANISI Document), NATO SECRET
STANAG 4250-3♦	Part 3--Naming and Addressing, Draft (Working Paper), NATO UNCLASSIFIED
STANAG 4250-4♦	Part 4--Management, Draft (Working Document), NATO UNCLASSIFIED
STANAG 4250-5♦	Part 5--Military Features, Draft (Working Document), NATO UNCLASSIFIED
STANAG 4251♦	NATO Reference Model for OSI - Layer 1 (Physical Layer) Service Definition, Draft, 13 July 1990, NATO UNCLASSIFIED
STANAG 4252♦	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Service Definition, Draft, 6 July 1990, NATO UNCLASSIFIED
STANAG 4253♦	NATO Reference Model for OSI - Layer 3 (Network Layer) Service Definition, Draft, July 1990, NATO UNCLASSIFIED (Appendix B is NATO CONFIDENTIAL)
STANAG 4254♦	NATO Reference Model for OSI - Layer 4 (Transport Layer) Service Definition, Draft, July 1990, NATO UNCLASSIFIED
STANAG 4255♦	NATO Reference Model for OSI - Layer 5 (Session Layer) Service Definition, Draft, 12 April 1990, NATO UNCLASSIFIED
STANAG 4256♦	NATO Reference Model for OSI - Layer 6 (Presentation Layer) Service Definition, Draft, 19 January 1990, NATO UNCLASSIFIED
STANAG 4257♦	NATO Standard Profile on Military Message Handling System (MMHS), Draft, 16 February 1990, NATO UNCLASSIFIED
STANAG 4258♦	Specification of ASN.1, Draft, 15 January 1990, NATO UNCLASSIFIED
STANAG 4259♦	Specification of Basic Encoding Rules for ASN.1, Draft, 15 January 1990, NATO UNCLASSIFIED
STANAG 4261♦	NATO Reference Model for OSI - Layer 1 (Physical Layer) Protocol Specification, Draft, 13 July 1990, NATO UNCLASSIFIED
STANAG 4262♦	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Protocol Specification, Draft, 6 July 1990, NATO UNCLASSIFIED
STANAG 4263♦	NATO Reference Model for OSI - Layer 3 (Network Layer) Protocol Specification Draft, July 1990, NATO UNCLASSIFIED
STANAG 4264♦	NATO Reference Model for OSI - Layer 4 (Transport Layer) Protocol Specification, Draft, July 1990, NATO UNCLASSIFIED
STANAG 4265♦	NATO Reference Model for OSI - Layer 5 (Session Layer) Protocol Specification, Draft, 12 April 1990, NATO UNCLASSIFIED
STANAG 4266♦	NATO Reference Model for OSI - Layer 6 (Presentation Layer) Protocol Specification, Draft, 19 January 1990, NATO UNCLASSIFIED
STANAG xxxx♦	NATO Standard Profile on R.131(M), Draft, 1989, NATO UNCLASSIFIED

STANAG xxxx♦	NATO Standard Profile on TC 111(M) - Connection-Mode Transport Service Over Connection-Mode Network Service - Permanent Access to a Packet Switched Data Network (Military), Draft, Version 1.3, 13 July 1990, NATO UNCLASSIFIED
STANAG xxxx♦	NATO Standard Profile on TA 51(M) - Interface Between a Reference End System That Provides the Connection-Mode Transport Service (CO-TS) Over the Connectionless-Mode Network Service (CL-NS) and a CSMA/CD LAN of Types 10Base2 and 10Base5, Draft, Version 2.0, 23 July 1990, NATO UNCLASSIFIED

B. OTHER STANAGs

STANAG 4146	Interim Specifications for Input/Output Interfaces in NATO Naval Data Handling Equipment
STANAG 4153	Standard Specification for an Asynchronous Serial Data Interface for Point to Point Connections and for Connection to Data Networks in NATO Naval Systems
STANAG 4156	Standard Specification for a Serial Data Interface for Synchronous Connections to a Data Network
STANAG 4175	Multi-Functional Information Distribution System
STANAG 4197	Modulation and Coding Characteristics that must be Common to Assure Interoperability of 2400 BPS Linear Predictive Encoded Digital Speech Transmitted Over HF Radio Facilities
STANAG 4198	Parameters and Coding Characteristics That Must Be Common to Assure Interoperability of 2400 BPS Linear Predictive Encoded Digital Speech
STANAG 4199	Uniform System of Exchange of Materiel Management Data
STANAG 4202	Transmission Envelope Characteristics for High Reliability Data Exchange between Land Tactical Data Processing Equipment Over Single Channel Radio Links
STANAG 4203	Technical Standards for Single Channel HF Radio Equipment
STANAG 4204	Technical Standards for Single Channel VHF Radio Equipment
STANAG 4205	Technical Standards for Single Channel UHF Radio Equipment
STANAG 4206	The NATO Multichannel Tactical Digital Gateway-System Standards
STANAG 4207	The NATO Multi-Channel Tactical Digital Gateway - Multiplex Group Framing Standards
STANAG 4208	The NATO Multi-Channel Tactical Digital Gateway - Signalling Standards
STANAG 4209	The NATO Multi-Channel Tactical Digital Gateway - Standards for Analogue to Digital Conversion of Speech Signals
STANAG 4210	The NATO Multi-Channel Tactical Digital Gateway - Cable Link Standards
STANAG 4211	The NATO Multi-Channel Tactical Digital Gateway - System Control Standards
STANAG 4212	The NATO Multi-Channel Tactical Digital Gateway - Radio Relay Link Standards
STANAG 4213	The NATO Multi-Channel Tactical Digital Gateway - Data Transmission Standards
STANAG 4214	International Routing and Directory for Tactical Communication Systems
STANAG 4231	Digital Interoperability Between UHF Tactical Satellite Communications Terminals
STANAG 4232	Digital Interoperability Between SHF Tactical Satellite Communications Terminals
STANAG 4233	Digital Interoperability Between EHF Tactical Satellite Communications Terminals
STANAG 4234	Radio Frequency Environmental Conditions Affecting the Design of Materiel for Use by NATO Forces

STANAG 4245	Secure and ECM Resistant HF Low Speed Digital Data Communications System
STANAG 4246	Have Quick and UHF Secure Jam Resistant Communications Equipment
STANAG 4249	NATO Multi-Channel Tactical Digital Gateway - Data Transmission Standards (Packet Switching Service)
STANAG 4250	The NATO Reference Model for Open Systems Interconnection - Overview
STANAG 4261	The NATO Reference Model for Open Systems Interconnection- Layer 1 (Physical Layer) Protocol Specification
STANAG 4262	The NATO Reference Model for Open Systems Interconnection - Layer 2 (Data Link Layer) Protocol Specification
STANAG 4263	The NATO Reference Model for Open Systems Interconnection - Layer 3 (Network Layer) Protocol Specification
STANAG 4271	ECM Resistant Digital Traffic Exchange Between Tactical Satellite Communications Terminals
STANAG 4285	Characteristics of a 1200/2400 Bits Per Second Single Tome Modulator/Demodulator for HF Radio Links
STANAG 4290	NATO Multi-Channel Tactical Digital Gateway - Cable Link (Optical) Standards
STANAG 4291	Modulation and Coding Characteristics that must be Common To Assure Interoperability of 2400 BPS Wireline Modems for Use in Narrow-Band Secure Voice Systems
STANAG 4292	Standards to Achieve Communications Between Tactical Combat Net Radio Equipment Designed to STANAG 4202 and Frequency Hopping Radios Operating in the Same VHF Band
STANAG 4295	Significant Data and Telegraph Signalling Conditions
STANAG 5000	Interoperability of Tactical Digital Facsimile Equipment
STANAG 5004	Military Characteristics for Field Telephone Sets (Minimum Standard)
STANAG 5009	(Exact Title Unknown - Relates to Naval Gunfire Support Using HF Radio)
STANAG 5018	NATO Manual Interface Between the Manual Switched Telecommunications Systems of the Combat Zone
STANAG 5020	Interoperability of Aircraft UHF Multi-Frequency Transceiver Installation and Compatible Ground Transmitters and Receivers
STANAG 5026	Military Characteristics for Facsimile Equipment To Meet Meteorological Requirements
STANAG 5028	Significant Telegraph Signalling Conditions in Automatic Telegraphy [Morse and International Alphabet (IA) No. 2]
STANAG 5030	Single and Multichannel VLF and LF On-Line Broadcast and Off-Line OOK Systems
STANAG 5031	Introduction of Modern Audio Equipment for Naval HF-MF and LF Shore-to-Ship Broadcasts
STANAG 5032	HF Single Sideband Single Channel Voice Communications (exact title unknown)
STANAG 5035	Introduction of an Improved System for Maritime Air Communications on HF, LF and UHF
STANAG 5036	Parameters and Practices for the Use of the NATO 7-Bit Code
STANAG 5038	Interoperability of Ship UHF Transmitting and Receiving Systems
STANAG 5040	NATO Automatic and Semi-Automatic Interfaces Between the National Switched Telecommunications Systems of the Combat Zone and Between These Systems and the NICS from 1979 to the 1990's
STANAG 5501	Point-to-Point Digital Data Link - Link 1
STANAG 5504	Tactical Data Link for the Control of Aircraft - Link 4

STANAG 5505	NATO Standard Bit Fields, Bit Field Fillers and Codes
STANAG 5506	Link 6 SAM/NADGE Link
STANAG 5507	Link 7 Airspace/Air Traffic
STANAG 5510	Maritime Tactical Data Exchange - Link 10
STANAG 5511	Tactical Data Exchange - Link 11
STANAG 5514	Tactical Data Broadcasting - Link 14
STANAG 5516	Tactical Data Exchange - Link 16
STANAG 5550	NATO Standard Data Elements, Data Items and Codes
STANAG 5601	Standards for Interface of NATO Data - Links 1, 11, 14, and TADIL B Through A Ship/Shore/Ship Buffer
STANAG 5620	Standards for the Interoperability of ADP Fire Support Systems
STANAG 5621	Standards for the Interoperability of NATO Land Combat and Combined Operations Systems
STANAG 5622	Air Operations System
STANAG 5623	Standards for Interoperability of Maritime Operations Systems

C. OTHER NATO DOCUMENTS

ACP 127	Message Relay Procedures
ACP 167(F)	Glossary of Communications-Electronics Terms, NATO, August 1981, UNCLASSIFIED
ADatP-2(D)	NATO Glossary of Automatic Data Processing (ADP) Terms and Definitions, December 1985, NATO UNCLASSIFIED
ADatP-3 (STANAG 5500)	NATO Message Text Formatting Systems, Part IV, Catalog of Standard Field Formats, December 1986, NATO UNCLASSIFIED
AM 96-1-4	Data Management, SHAPE, 30 October 1988, NATO UNCLASSIFIED
Classification Guide	NATO Network Security Information Classification Guide (NU), Version 1.0, TSGCEE SG9, February 1989, NATO RESTRICTED
MC[1] 203/2	The Operational Requirements for the Interoperability of the Communications Between Different National Component Land Forces in the Combat Zone and the Communication Used in Provision of Air and Naval Support to These Forces
MC 277	The Operational Requirements for the Interoperability of Tactical Communication Systems for Use by the NATO Nations in the Land Combat Zone - Post 1985
MC 283	The Military Police for ECCM Applied to Tactical Communications in the Combat Zone
MC 284	The NATO Military Requirement for ECM Resistant and Secure Communications (NR)
NIMP	NATO Interoperability Management Plan (NIMP), Third Endorsement Edition, ADSIA-RCU-D/1 (Revised), Allied Data Systems Interoperability Agency, 1 July 1988, NATO UNCLASSIFIED
NIPD Vol. 1	NATO Interoperability Planning Document (NIPD), Volume 1, Introduction to Information Systems Interoperability Including the Allied Data Systems Interoperability Agency and the Organization of and Coordination Among NATO Bodies Involved in NATO Common Interoperability Standards Development and Configuration Management, Second Draft, ADSIA-RCA-WP/76, 20 April 1990, NATO UNCLASSIFIED

1 MC: Military Characteristic

NIPD Vol. 2	NATO Interoperability Planning Document (NIPD), Volume 2, Formal Specification of Information Exchange Requirements, Draft, ADSIA-RCA-WP/72, February 1990, NATO UNCLASSIFIED
NIPD Vol. 3	NATO Interoperability Planning Document (NIPD), Volume 3, Plan for Development of NATO Common Interoperability Standards (NCIS), Revised Draft, ADSIA-RCA-WP/73 (First Revise), February 1990, NATO UNCLASSIFIED
NIPD Vol. 4	NATO Interoperability Planning Document (NIPD), Volume 4, NATO Common Interoperability Standards Configuration Management Plan (NCISCMP), Revised Draft, ADSIA-RCA-WP/32 (5th Revise), August 1989, NATO UNCLASSIFIED
NIPD Vol. 5	NATO Interoperability Planning Document (NIPD), Volume 5, NATO Common Interoperability Standards Testing Concept, First Draft, ADSIA-RCA-WP/75, February 1990, NATO UNCLASSIFIED
NIPD Vol. 6	NATO Interoperability Planning Document (NIPD), Volume 6, Documentation Plan for NATO Common Interoperability Standards, First Draft, ADSIA-RCA-D-15-90, 13 June 1990, NATO UNCLASSIFIED
NOSA	NATO OSI Security Architecture (NOSA), Ad Hoc Working Group on Security, TSGCEE SG9, Draft Version 2.1, March 1988, NATO UNCLASSIFIED
NTIS Transition Strategy	NATO Technical Interface Standards (NTIS) Transition Strategy, Fifth Edition, AC/259-D/1218(Revised), Conference of National Armaments Directors (CNAD), Tri-Service Group on Communications and Electronic Equipment (TSGCEE), NATO, Brussels, 30 November 1989, NATO UNCLASSIFIED
SANISI	Security Architecture for NATO Information Systems Interconnection (SANISI) (NU), Version 2.0, Ad Hoc Working Group on Security, TSGCEE SG9, AC/302(SG/9)D/53, 14 April 1989, NATO CONFIDENTIAL
STAMINA 4.0	Standard Automated Message Interface for NATO ACCIS (STAMINA), Version 4.0, NACISA, April 1990, NATO UNCLASSIFIED
TM-776	Data Management Standardization for ACE ACCIS, TM-776, SHAPE Technical Centre, July 1985, NATO UNCLASSIFIED.

(This page intentionally left blank.)

II. U.S. MILITARY STANDARDS

DoD-STD-1467	Software Support Environment, 18 January 1985
DoD-STD-1700	Data Management Program, 28 September 1987
DoD-STD-1703	Software Product Standards, 12 February 1987
DoD-STD-1838A	Common Ada Programming Support Environment (APSE) Interface Set (CAIS-A), 6 April 1989
DoD-STD-2167A	Defense System Software Development
MIL-A-89007	Presentation Manager
MIL-C-28748A	Connectors, Electrical, Rectangular, Rack and Panel, Solder-Type and Crimp-Type Contacts, February 1985
MIL-D-28000	Digital Representation for Communication of Product Data: IGES Application Subsets, 22 December 1987 with Amendment 1 of 20 December 1988 (used in CALS for computer-aided design and vector graphics (e.g., in technical manual illustrations, engineering diagrams) [Currently undergoing revision]
MIL-D-28003	Digital Representation for Communication of Illustration Data: CGM Application Profile, 20 December 1988 (based on CGM; used in CALS for vector graphics in technical manual illustrations) [Currently undergoing revision]
MIL-D-89000	Digital Terrain Elevation Data
MIL-HDBK-59	CALS Program Implementation Guide, 20 December 1988
MIL-HDBK-782	Software Support Environment Acquisition Implementation Guide for DoD-STD-2167, 29 February 1988
MIL-M-28001A	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text and Amendment 1, 1991 (based on ISO 8879, SGML)
MIL-R-28002A	Requirements for Raster Graphics Representation in Binary Format, 30 November 1990 (based on GRP 4 Raster de facto industrial standards; used in CALS for raster-scanned images in engineering drawings and technical manual illustrations)
MIL-STD-188-114A	Electrical Characteristics of Digital Interface Circuits, July 1984
MIL-STD-188C	Military Communication System Technical Standards, November 1969
MIL-STD-188-100	Common Long-Haul and Tactical Communication System Technical Standards, November 1972
MIL-STD-188-148(S)	Interoperability Standards for Anti-Jam Communications in the HF Band (U)
MIL-STD-1379D	Military Training Programs
MIL-STD-1388-2B	DoD Requirements for a Logistic Support Analysis Record
MIL-STD-1777	Internet Protocol (IP), August 1983
MIL-STD-1778	Transmission Control Protocol (TCP), August 1983
MIL-STD-1779	Interfaces for High Capacity C3 Local Area Networks, November 1983
MIL-STD-1780	File Transfer Protocol (FTP), May 1984
MIL-STD-1781	Simple Mail Transfer Protocol (SMTP), May 1984
MIL-STD-1782	TELENET Protocol, May 1984
MIL-STD-1815A	Ada Programming Language (ISO 8652), 1983
MIL-STD-1840B	Automated Interchange of Technical Information, March 1991

MIL-T-31000	General Specifications for Technical Data Packages (supersedes DoD-D-1000, Engineering Drawings and Associated Lists)
RFC[2] 742	Finger Protocol (Elective, Proposed Standard)
RFC 768	User Datagram Protocol (UDP) (Recommended)
RFC 783	Trivial File Transfer Protocol (TFTP) (Elective, Draft Standard)
RFC 791	Internet Protocol (IP) (Required)
RFC 792	Internet Control Message Protocol (ICMP) (Required)
RFC 793	Transmission Control Protocol (TCP) (Recommended)
RFC 821	Simple Mail Transfer Protocol (SMTP) (Recommended)
RFC 822	Format of Electronic Mail Messages (MAIL) (Recommended)
RFC 826	Address Resolution Protocol (ARP) (Elective)
RFC 854	TELNET Protocol (Recommended)
RFC 862	Echo Protocol (ECHO) (Recommended)
RFC 863	Discard Protocol (DISCARD) (Elective)
RFC 864	Character Generator Protocol (CHARGEN) (Elective)
RFC 865	Quote of the Day Protocol (QUOTE) (Elective)
RFC 866	Active Users Protocol (USERS) (Elective)
RFC 867	Daytime Protocol (DAYTIME) (Elective)
RFC 868	Time Server Protocol (TIME) (Elective)
RFC 877	Internet Protocol on X.25 Networks (IP-X25) (Elective)
RFC 891	Internet Protocol on DC Networks (IP-DC) (Elective)
RFC 894	Internet Protocol on Ethernet Networks (IP-E) (Elective)
RFC 895	Internet Protocol on Experimental Ethernet Networks (IP-EE) (Elective)
RFC 903	A Reverse Address Resolution Protocol (RARP) (Elective)
RFC 904	Exterior Gateway Protocol (EGP) (Recommended)
RFC 907	Internet Protocol on Wideband Networks (IP-WB) (Elective)
RFC 919	Internet Protocol Broadcast Datagrams (Required)
RFC 922	Internet Protocol Broadcast Datagrams With Subnets (Required)
RFC 950	Internet Protocol Subnet Extension (Required)
RFC 951	Bootstrap Protocol (BOOTP)
RFC 954	Who Is Protocol NICNAME) (Elective, Draft Standard)
RFC 959	File Transfer Protocol (FTP) (Recommended)
RFC 1001-1002	Net BIOS Service Protocol (Elective)
RFC 1006	ISO Transport Service on Top of TCP (TP-TCP) (Elective, Draft Standard)
RFC 1009	Gateway Requirements (Required)
RFC 1034-1035	Domain Name System (Recommended)
RFC 1042	Internet Protocol on IEEE 802 (IP-IEEE) (Elective)
RFC 1044	Internet Protocol on Hyperchannel Networks (IP-HC) (Elective)
RFC 1048	Bootstrap Protocol (BOOTP) (Recommended, Draft Standard)
RFC 1049	Content of Header Type (CONTENT) (Recommended)
RFC 1051	Internet Protocol on ARCNET (IP-ARC) (Elective)

---

2 The list of Internet Requests for Comment (RFCs) was updated from Appendix C of *Internetworking with TCP/IP*, Volume I, *Principles, Protocols, and Architecture*, Dourglas Comer, Prentice Hall, 1991.

RFC 1054	Internet Group Multicast Protocol (IGMP)
RFC 1055	Transmission of IP Over Serial Lines (IP-SLIP) (Elective)
RFC 1058	Routing Information Protocol (RIP) (Elective, Draft Standard)
RFC 1059	Network Time Protocol
RFC 1060	Assigned Numbers (Required)
RFC 1084	Bootstrap Protocol (BOOTP) (Recommended, Draft Standard)
RFC 1088	Transmission of IP Over NetBIOS (IP-NETBIOS) (Elective)
RFC 1095	Common Management Information Services and Protocol Over TCP/IP (CMOT) (Recommended, Draft Standard)
RFC 1103	Transmission of IP Over FDDI (IP-FDDI) (Elective)
RFC 1112	Internet Group Multicast Protocol (IGMP) (Recommended)
RFC 1113-15	Mail Privacy (Procedures, Key Management, and Algorithms) (Elective, Draft Standard)
RFC 1122	Host Requirements--Communications (Required)
RFC 1123	Host Requirements--Appications (Required)
RFC 1132	Transmission of 802.2 over IPX Nets (IP-IPX (Elective)
RFC 1155	Structure of Management Information (SMI) (Recommended)
RFC 1156	Management Information Base (MIB) (Recommended)
RFC 1157	Simple Network Management Protocol (SNMP) (Recommended)
RFC B1822	Internet Protocol on ARPANET IIP-ARPA) (Elective)

(This page intentionally left blank.)

III. AGREEMENTS FROM REGIONAL WORKSHOPS

EDxxx	Application Function A/4113, Basic Class VT, A-mode X3 Functional Standard, European Workshop for Open Systems, [EWOS EG VT/90/112], Final Draft, November 1990
EWOS xxxx	EWOS Technical Guide on Lower Layer Relays, Final Draft, EWOS, 1990
EWOS/ETG003	EWOS/EG FT, File Transfer Access and Management - FTAM Remote Actions (RA) Service and Protocol, 24 January 1990
EWOS/EG VT/89	Application Function A/4121, Basic Class VT S-Mode Forms Functional Standard, Part 1: Virtual Terminal Service, EWOS/EG VT/89/53, Part 2: VT Protocol Check List, EWOS/EG VT/89/59, and Part 3: Underlying Layers Check List, EWOS/EG VT/89/60, Final Text, prENV 41 208
Profile RC p,q	X.25 Protocol Relaying, Draft, EWOS/EGLL/2990/81, EWOS, 9 May 1990
ECMA TR/46	Security in Open Systems--A Security Framework, ECMA TR/46, European Computer Manufacturers Association, July 1988
ECMA TR/55	Reference Model for Frameworks on Computer Assisted Software Engineering Environments, developed by ECMA TC33 Technical Group on Reference Models (TGRM), December 1990.
ECMA 149	Portable Common Tools Environment (PCTE) Abstract Specification, European Computer Manufacturers Association, December 1990
ECMA 158	Portable Common Tools Environment (PCTE) C Programming Language Binding, European Computer Manufacturers Association, June 1991
NIST SP 500-177	Stable Implementation Agreements for Open Systems Interconnection Protocol, Version 3, Edition 1, Proceedings of the December 1989 NIST OSI Implementor's Workshop (NOIW), March 1990
NISTIR 88-4017	Standards for the Interchange of Large Format Tiled Raster Documents, U.S. NIST, December 1988
ENV[3] 41 101♦	LANs: Provision of the OSI Connection-Mode Transport Service (COTS) Service Using the Connectionless-Mode Network Service (CLNS) on a CSMA/CD Single LAN, June 1986
ENV 41 102♦	LANs: Provision of the OSI COTS and the CLNS on a CSMA/CD Single or Multiple LAN Configuration, June 1986
ENV 41 103	LANs: Provision of the OSI COTS and the Connection-Mode Network Service (CONS) in an End System on a CSMA/CD LAN, August 1990
ENV 41 104	Packet Switched Data Networks: Permanent Access, August 1987
ENV 41 105♦	Packet Switched Data Networks: Switched Access, June 1988
ENV 41 106♦	Digital Data Circuit (CSDN) - Provision of the OSI COTS in the T.70 Case for Telematic End Systems, June 1988
ENV 41 107♦	Digital Data Circuit (CSDN) - Provision of the OSI COTS and the OSI CONS, June 1988
ENV 41 108	LANs: Provision of the OSI COTS and CONS in an End System on a Token Ring LAN, August 1990
ENV 41 109♦	LANs: Provision of the OSI COTS Using CLNS on a Token Ring Single LAN, February 1988

[3] ENV indicates a standard approved by the Join European Standards Institution (CEN/CENELEC) and the European Workshop for Open Systems (EWOS).

ENV 41 110♦	LANs: Provision of the OSI COTS Using CLNS in an End System on a Token Ring LAN in a Single or Multiple LAN Configuration, February 1988
ENV 41 111	ISDN: X.25 DTE to DTE Operation (B-channel)
ENV 41 112	ISDN: X.25 DTE to DTE Operation (Circuit-mode service)
ENV 41 201	Private Message Handling System - User Agent and Message Transfer Agent; Private Management Domain to Private Management Domain, June 1986
ENV 41 202	Message Handling Systems; User Agent and Message Transfer Agent: Access to an Administration Management Domain (ADMD), August 1987
ENV 41 203	Exchange of Telex Documents Between Two End Systems, Which May Be Teletex Terminals, June 1988
ENV 41 204	FTAM: Simple File Transfer, September 1989
ENV 41 205♦	FTAM: File Management, June 1989
ENV 41 206	FTAM: Positional File Transfer, September 1989
ENV 41 207	FTAM: Positional File Access Service, September 1989
ENV 41 208-1	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 1: Virtual Terminal Service, European Prestandard, December 1990
ENV 41 208-2	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 2: Check List, European Prestandard, December 1990
ENV 41 208-3	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 3: Underlying Layers Checklist, European Prestandard, December 1990
ENV 41 209	Information System Interconnection - Basic Class Virtual Terminal - Common Control Objects, European Prestandard, December 1990
prENV 41 210	Directory: Directory Access Protocol, April 1990
prENV 41 211-1	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode X.3 (A/VT15) - Part 1: Virtual Terminal Service, May 1991
prENV 41 211-2	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode X.3 (A/VT15) - Part 2: Virtual Terminal Protocol Checklist, May 1991
prENV 41 211-3	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode X.3 (A/VT15) - Part 3: Underlying Layers Checklist, May 1991
prENV 41 212	Information Systems Interconnection - Directory System Protocol (A/DI2), May 1991
prENV 41 213-1	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode Telnet' (A/VT13) - Part 1: Virtual Terminal Service, May 1991
prENV 41 213-2	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode Telnet' (A/VT13) - Part 2: Virtual Terminal Protocol Checklist, May 1991
prENV 41 213-3	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode Telnet' (A/VT13) - Part 3: Underlying Layers Checklist, May 1991
ENV 41 504	Data Stream Formats, Character-coded Text, Telex-compatible
ENV 41 506	Data Stream Formats, Character-coded Text, Teletex-compatible
ENV 41 507	Data Stream Formats, Character-coded Text, Videotex-compatible
ENV 41 509	ODF: Simple Document Structure, Character Content Architecture Only, January 1989
ENV 41 510	ODF: Enhanced Document Structure, Character, Raster, Geometric Graphics Content Architecture, January 1989
ENV 41 511	ODF: Processable and Layout Independent Documents, Simple Messaging Profile, January 1989
prENV 41 512	Directory Data Definitions, Common Directory Use, April 1990
prENV 41 513	Information Systems Interconnection - Virtual Terminal Basic Class - VT Font Assignment Type 1 (F/441), July 1991

ENV 41 901	X.29-Mode Procedures Between a Packet Mode DTE or a PAD and a PAD via a Public or Private X.25 Packet Switched Network or ISO 8208 Packet Level Entity and ISO 7776 Link Level Entity, June 1987
M-IT-02	Directory of Functional Standards (For Interworking in an OSI Environment) Adopted by the CEN/CENELEC/CEPT/ITSTC, March 1987
M-IT-02	A Framework for Testing and Certification in Europe (being implemented by ECITC)

Proposed NIST OIW ISP on Directory [SGFS N 216, 11 June 1990]:

Part 1: [Title to be taken from FTAM ISP, adding ROSE]

Part 2: ADI 11, Directory User Agent (DUA) Basic Operation

Part 3: ADI 12, DUA Secure Operation

Part 4: ADI 13, DUA Operation in Distributed Environment

Part 5: ADI 211, Directory Service Agent (DSA) - DUA Basic Operation Interaction

Part 6: ADI 212, DSA - DUA Secure Operation Interaction

Part 7: ADI 221, DSA - DSA Basic Operation Interaction

Part 8: ADI 222, DSA - DSA Secure Operation Interaction

Part 9: ADI 131, Common Use Directory Information

Part 10: ADI 132, Strong Authentication Directory Information

(This page intentionally left blank.)

IV. U.K. BSI STANDARDS AND PAPERS

IST/21: 1914	Delegates Report of the ISO/IEC JTC1 SC21/WG4 Plenary, OSI Management and Directory Services, Florence, 31 October to 9 November 1989
IST/21:2160	Report on SC21 Plenary, Held in Seoul, BSI IST/21, 5-6 June 1990, 13 July 1990
IST/21:2161	Report of SC21/WG1 Meeting, Seoul, Korea, 23-31 May 1990, BSI, IST 21, 27 July 1990
IST/21:2162	Report of SC21/WG3 Database Meeting, Seoul, Korea, 21 May to 1 June 1990, BSI, IST 21, 27 July 1990
IST/21:2164	OSI Specific Applications Services, ISO/IEC JTC1/SC21 WG5 Meeting, Seoul, Korea, 24 May to 1 June 1990, BSI, IST 21, 10 July 1990
IST/21:2165	Report of Seventh Meeting of SC21/WG6, Seoul, Korea, 23 May to 1 June 1990, BSI, IST 21, 3 August 1990
IST/21:2170	JTC1 Workshop on Security, London, 5-7 November 1990, BSI IST21, 29 June 1990
IST/21:2187	IST/21 Activities 1989-1990, 27 July 1990
IST/21:2236	Report of SC21/WG1/FDT Meeting, Seoul, Korea, 23 May to 31 May 1990, BSI, IST 21, 30 July 1990
IST/21:2237	Security Liaison Requirements, 27 July 1990
IST/21:2249	Current and Recent Ballots, 10 August 1990
IST18 N 2694	Final Report on the Framework for Open Systems, July 1990
IST21 N 2361	UK Comment Accompanying Vote of Disapproval on CD 10728, Information Resource Dictionary System Services Interface, UK, 24 October 1990
IST21 N 2393	Proposals for Corrigenda to OSI Standards - Reprint from BSI News, November 1990
IST21 N 2478	Catalogue of Security Related Projects for consideration at the JTC 1 Workshop on Security 5-7 November 1990, 30 May 1990
IST21 N 2491	Change in Work Schedule, SC21 Secretariat, 7 January 1991
IST21 N 2499	Report on the Anaheim IRDS Services Interface Meetings, David JL Gradwell, 18 January 1991
IST21 N 2508	PICS Proforma Notations, 17 January 1991
IST21 N 2514	Information Technology - International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the use by FTAM, Project Editor, 17 January 1991
IST21 N 2512	Resolutions of the 4th RWS-CC meeting, October 18-19, 1990, Tokyo, EWOS, 17 January 1991
IST21 N 2531	Discussion Paper on the Nature of Protocol Profiles, BSI, 6 February 1991
IST21 N 2551	UK Response to SC21/N5110 on the Technical Structure of Quality-of-Service (QOS) Architecture, February 1991
IST21 N 2552	Proposed UK Contribution on QOS, Joint Meeting on QOS, 29 January 1991
IST/21 N 2589	Minutes of the 20th meeting of EWOS EGLL from October 8 to October 11, 1990, in Brussels, 1 February 1991
IST21 N 2594	Register of IST/21 Documents, September 1990 - February 1991, 26 February 1991
IST21 N 2605	Connection-mode Transport Service over Connectionless-mode Network Service, 26 February 1991

IST21 N 2659	Press Release, EWOS Releases More IT Functional Standard Proposals for Open Systems, Addendum 1 to SC N148, Rev 2, 26 March 1991
IST21 N 2670	Prospective vs Traditional Standardization, 21 March 1991
IST21 N 2742	Information Technology - International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 2: Definition of document types, constraint sets and syntaxes, Project Editor, 17 January 1991
IST21 N 2743	Information Technology - International Standardized Profiles AFT nn-File Transfer, Access and Management - Part 3: AFT 11 - Simple File Transfer Service (unstructured), Project Editor, 17 January 1991
U.K. GOSIP Vol. 1	U.K. Government OSI Profile, Volume I, Introduction, Version 3.1, Central Computer and Telecommunications Agency, London, 1990
U.K. GOSIP Vol. 2	U.K. Government OSI Profile, Volume II, Specification, Version 3.1, Central Computer and Telecommunications Agency, London, 1990
U.K. GOSIP Vol. 3	U.K. Government OSI Profile, Volume III, Procurement Handbook, Version 3.1, Central Computer and Telecommunications Agency, London, 1990
Users Handbook	Users' Open Systems Handbook, Level-7 Limited, United Kingdom, 1989

V. US STANDARDS AND PAPERS[4]

ANSI/SMPTE RP 125	Digital Interface Standard, Draft
ANSI X3.1	Information Systems - Data Transmission - Synchronous Signalling Rates, 1987 (FIPS 22-1)
ANSI X3.4	Coded Character Sets - 7-Bit American National Standard Code for Information Exchange (7-Bit ASCII), 1986 [ISO 646]
ANSI X3.9	Programming Language FORTRAN, 1978 (revised 1989) (ISO 1539)
ANSI X3.15	Bit Sequencing of the American National Standard Code for Information Exchange in Serial-By-Bit Data Transmission, 1976 (FIPS 16-1; ISO 1177], Revision in process
ANSI X3.23	Programming Language COBOL, 1985 (ISO 1989)
ANSI X3.23A	Addendum to ANSI X3.23-1985, Programming Language COBOL, 1989
ANSI X3.32	Graphic Representation of the Control Characters of American Standard Code for Information Exchange, [ISO 2047-75], 1973, Revised 1990
ANSI X3.41	Code Extension Techniques for Use with the 7-Bit Coded Character Set of American National Standard Code for Information Exchange, 1974, Revised 1990 (FIPS 35, WITHDRAWN; ISO 2022-82])
ANSI X3.42	Representation of Numeric Values in Character Strings for Information Interchange, [ISO 6093.2], 1975, Revised 1989
ANSI X3.53	Programming Language PL/1, 1976 (ISO 6160)
ANSI X3.57	Structure for Formatting Message Headings for Information Interchange Using the American National Standard for Information Interchange for Data communication, 1977, Revised 1986, currently undergoing public review for reaffirmation.
ANSI X3.60	Programming Language Minimal BASIC, Draft (DP 6373]
ANSI X3.66	Advanced Data Communication Control Procedures (ADCCP), (FIPS 71), 1979, Revised 1990
ANSI X3.74	Programming Language PL/1 General Purpose Subset, 1987 (DP 6522)
ANSI X3.83	Sponsorship Procedures for ISO Registration According to ISO 2375, November 1988 [ISO 2375]
ANSI X3.91M	Interfaces, Storage Module, 1987
ANSI X3.92	Data Encryption Algorithm, 1981
ANSI X3.97	Programming Language Pascal, 1983 (DIS 7185)
ANSI X3.98	Text Information Interchange in Page Image Format (PIF), 1983
ANSI X3.102	Data Communication Systems and Services User Oriented Performance Parameters, 1983, Revised 1990
ANSI X3.105	Information Systems - Data Link Encryption, 1983, Revised 1990
ANSI X3.106	Information Systems - Data Encryption Algorithm - Modes of Operation, 1983, Revised 1990
ANSI X3.107	Data Link Layer Protocol for Local Distributed Data Interfaces (LDDI), August 1982 (DP)
ANSI X3.108	Information Systems - Local Distributed Data Interfaces (LDDI) - Physical Layer Interface to Nonbranching Coaxial Cable Bus, 1988

[4] Updated March 1991 from *Accredited Standards Committee X3 - Information Processing Systems Projects Manual*, X3/SD-4, CBEMA, August 1990 and periodically, from ASC X3 New Releases.

ANSI X3.109	Physical Layer Protocol for Local Distributed Data Interfaces (LDDI), 1982 (DP)
ANSI X3.110	Videotex/Teletext Presentation Level Protocol (North American PLPS), (FIPS 121) 1983 [ISO 6937/1-2]
ANSI X3.113	Full BASIC, 1987 (FIPS 68-2) [DP 10279]
ANSI X3.113A	Addendum to Programming Language Full BASIC, Modules and Individual Character Input, 1989
ANSI X3.122	Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information, 1986 (REPLACED by ISO 8632)
ANSI X3.122.5	LISP Binding of GKS, Draft, 1989
ANSI X3.123	Programming Language APL, Draft, 1989 (DP 8485)
ANSI X3.124	Computer Graphics - Graphical Kernel System (GKS) Functional Description, 1985 (ISO 7942) [undergoing reaffirmation]
ANSI X3.124.1	Computer Graphics - Graphical Kernel System (GKS) FORTRAN Language Binding, 1985 (ISO 8651-1) [undergoing reaffirmation]
ANSI X3.124.2	Computer Graphics - Graphical Kernel System (GKS) Pascal Language Binding, 1988 (ISO 8651-2)
ANSI X3.124.3	Computer Graphics - Graphical Kernel System (GKS) Ada Language Binding, 1989 (ISO 8651-3)
ANSI X3.124.4	Computer Graphics - Graphical Kernel System (GKS) C Binding, Draft, 1989 (DP 8651-4)
ANSI X3.129	Intelligent Peripheral Interface, Physical Level, 1986 [ISO 9318-1]
ANSI X3.130	Intelligent Peripheral Interface - Device-Specific Command Set for Magnetic Disks, 1986 [ISO 9318-2]
ANSI X3.131	Small Computer System Interface (SCSI), 1986 [ISO 9316]
ANSI X3.132	Intelligent Peripheral Interface - Device Generic Command Set for Magnetic and Optical Disks, 1986 [ISO 8907]
ANSI X3.133	Database Language NDL, 1986 (FIPS 126)
ANSI X3.134.1	8-Bit ASCII Structure and Rules, Draft
ANSI X3.134.2	7-Bit and 8-Bit ASCII Supplemental Multilingual Graphic Character Set (ASCII Multilingual Set), Draft
ANSI X3.135	Database Language SQL, 1989 (FIPS 127) [relational database application program interface] (ISO 9075)
ANSI X3.135.1	Database Language SQL - Addendum 1: Integrity Enhancement Feature, 1988 (ISO 9075 DAD1)
ANSI X3.138	Information Resource Dictionary System (IRDS), 1988 (DIS 10027) (FIPS 156)
ANSI X3.138A	Supplement to X3.138-1988, Information Resource Dictionary System (IRDS), 1991
ANSI X3.139	Fibre Distributed Data Interface (FDDI) Token Ring Media Access Control (MAC), 1987 [DP 9314-2]
ANSI X3.140	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Layer Protocol Specification, 1986 (ISO 8072 and 8073)
ANSI X3.141	Data Communication Systems and Services - Measurement Methods for User-Oriented Performance Evaluation, 1986
ANSI X3.143	Information Processing Systems - Text and Office Systems - Standard Generalized Markup Language (SGML), Draft [ISO 8879]
ANSI X3.144	Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Functional Description, September 1988 (ISO 9592, 9593)
ANSI X3.144.1	ANS for the FORTRAN Language Binding of the Programmer's Hierarchical Interactive Graphics System (PHIGS) Binding to FORTRAN, 1989 (ISO 9593-1)

ANSI X3.144.2	Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Binding to Pascal, Draft, 1987 (DP 9593-2)
ANSI X3.144.3	Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Binding to Ada, 1989 [DIS 9593-3]
ANSI X3.144.4	Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) C Language Binding, Draft, September 1988 (DP 9593-4)
ANSI X3.146	Streaming Cartridge and Cassette Tape Drives - Device-Level Interface, 1986
ANSI X3.147	Intelligent Peripheral Interface - Device Generic Command Set for Magnetic Tape, 1987 [ISO 9318-4]
ANSI X3.148	Fibre Distributed Data Interface (FDDI) - Physical Layer Protocol (PHY), 1988 (ISO 9314-1)
ANSI X3.153	Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification, 1987 (ISO 8327)
ANSI X3.159	Information Systems - Languages - Programming Language C, 1989 (ISO 9899: 1990; FIPS-160)
ANSI X3.160	Programming Language Extended Pascal, 1989 (DP) [ANSI/IEEE 770 X3.160-1989]
ANSI X3.161	Computer Graphics Interface (CGI), 1990 [REPLACED BY ISO 9636)
ANSI X3.165	Programming Language DIBOL (revision of ANSI X3.165-1988), 1991
ANSI X3.166	Fibre Distributed Data Interface (FDDI) - Physical Layer Medium Dependent (PMD), 1990 [ISO 9314-3]
ANSI X3.167	Local Distributed Data Interface (LDDI) Star-Wired Physical Interface Sublayer, 1987 (DP)
ANSI X3.168	Information Systems - Language - Embedding of SQL Statements into Programming Languages, 1989
ANSI X3.170	Information Systems - Data Communication - Enhanced Small Device Interface (ESDI), 1990 [DIS 10222]
ANSI X3.172	American National Standard Dictionary for Information Systems, 1990
ANSI X3.172A	Computer Security Glossary, 1991
ANSI X3.176	Intelligent Peripheral Interface - Logical Device-Specific Command Set for Magnetic Tapes, 1989, [ISO 9318-5]
ANSI X3.177	Intelligent Peripheral Interface - Device Generic Command Set for Communications, 1990, [ISO 9318-7]
ANSI X3.184	Fibre Distributed Data Interface (FDDI) Physical Layer Medium Dependent (SMF-PMD) (CD 9314-4)
ANSI X3.185	IRDS Software Interface, Draft
ANSI X3.190	Conformance Testing for SGML Systems, Draft, April 1991
ANSI X3.194	Database Language SQL2, Draft
ANSI X3.196	Computer Graphics - X Window System Data Stream Definition, Draft
ANSI X3.198	Programming Language FORTRAN Extended (FORTRAN 9X), Draft [DIS 1539] estimated completion 1991
ANSI X3.208	Transfer Syntax Description Notation (TSDN) ,Draft Proposed American National Standard, April 4, 1991
ANSI X3.209	Optical Character Recognition (OCR) - Matrix Character Sets for OCR-MB, 1991
ANSI X3H4.6	Technical Report on Model Unification for Data Repositories
ANSI X3S3.7	X.25 Data Transfer Phase Procedures for Operating the Packet Layer Transfer Phase of X.25
ANSI X3T9.5	FDDI Follow-On Local Area Network - Physical Medium Dependent (FFOL-PMD), new project, May 10, 1991

ANSI X3T9.5	FDDI Follow-On Local Area Network - Physical Layer Protocol (FFOL-PHY), new project, May 10, 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Service Multiplexer (FFOL-SMUX), new project, May 10, 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Asynchronous Media Access Control (FFOL-AMAC), new project, May 10, 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Isochronous Media Access Control (FFOL-IMAC), new project, May 10, 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Station Management (FFOL-SMT), new project, May 10, 1991
ANSI X3V1.4	Voice Messaging over MOTIS ISO/DIS 10021
ANSI X3V1.9	Standard User Interface to Voice Messaging
ANSI X3 682-D	Domestic Public/Private X.25 Network Interworking, Draft
ANSI X12	Electronic Data Interchange (ISO 9735)
AIAA/ANSI G-009-1991	Guide for Implementing Software Development Files Conforming to DoD-STD-2167A, 1991
HFS/ANSI 100-1988	Human Factors Engineering of Video Display Terminal Workstation Standard, 1988
IEEE 610.12	IEEE Standard Glossary of Software Engineering Terminology , 1990.
ANSI/IEEE 730	IEEE Standard for Software Quality Assurance Plans, 1984 (Revision underway)
IEEE 770	Programming Language Pascal, 1990
IEEE 802.1D	IEEE Standards for Local and Metropolitan Area Networks: Media Access Control, 1990
IEEE 802.1E	IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Layer Management (Section 5). 1990
IEEE 802.3h	IEEE Standards for Local and Metropolitan Area Networks: System Load Protocol, 1990
IEEE P802.10A	Interoperable LAN Security (SILS) - The Model [PAR approved 5/90]
IEEE P802.10B	SILS - Secure Data Exchange [PAR approved 5/90]
IEEE P802.10C	SILS - Key Management [PAR approved 5/90]
IEEE P802.10D	SILS - Security Management [PAR approved 5/90]
IEEE P802.11	Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications [PAR approved March 21, 1991]
IEEE P828	Standard for Software Configuration Management Plans, 1983 (PAR revised 28 September 1990[5]) [PAR WITHDRAWN 6 December 1990[6]]
ANSI/IEEE 829	IEEE Standard for Software Test Documentation, 1983 (Standard reaffirmed March 21, 1991])
ANSI/IEEE 830	IEEE Guide to Software Requirements Specifications, 1984 (Revision underway)
IEEE 928.1	IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988
IEEE 928.2	IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988

5 Updated from *The IEEE Standards Bearer*, vol. 4, no. 3, October 1990, pp. 8-9.

6 Updated from *The IEEE Standards Bearer*, vol. 4, no. 4, December 1990, pp. 8-9.

ANSI/IEEE 983	IEEE Guide for Software Quality Assurance Planning, 1986
ANSI/IEEE 990	IEEE Recommended Practice for Ada as a Program Design Language, 1986
ANSI/IEEE 1002	IEEE Standard Taxonomy for Software Engineering Standards, 1987
IEEE P1003.0	POSIX Guide, Draft 13, September 1991, Draft 15 to be balloted in July 1992
IEEE 1003.1	POSIX - System Interface, approved by ANSI in November 1989 and revised September 1990; approved by ISO as ISO 9945-1, December 1990. IEEE 1003.1-1988 approved as FIPS 151-1, March 1990. FIPS 151-2 to be proposed November 13, 1991.
IEEE P1003.1a	Language Independent Specifications, Draft 6, July 1991, Ballot spring 1992; target completion late 1992
IEEE P1003.1b	System Interface Extensions, Draft 5, December 1990, IEEE balloting planned for late 1991.
IEEE P1003.2	Shell and Utilities, Draft 11.2 balloted October 1991, IEEE standard expected 2Q 1992) (Draft 10 was submitted to ISO and balloted as DP 9945-2, but failed. A new draft was requested for registration , but is on hold
IEEE P1003.2a	User Portability Extensions, Draft 8 balloted October 1991, IEEE standard expected 2Q of 1992
IEEE 1003.3	Test Methods, IEEE 1003.3-1991 approved March 21, 1991. ISO standard proposed; international ballot initiation pending
IEEE P1003.3.1	Test Methods, Draft 13 balloted December 1991; approval of final text expected in 1Q 1992.
IEEE P1003.3.2	Test Methods, Draft 6, July 1991; ballot planned for mid-1992; approval of final text expected early 1993.
IEEE P1003.4	Real-Time Extensions, Draft 11 ballot closes November 1991; approval expected late 1992
IEEE P1003.4a	Threads, Draft 6 balloted December 1991.
IEEE P1003.4b	Language-Independent Specifications, Draft 3, June 1990
IEEE P1003.4c	Extensions to P1003.4, Draft 10, January 1991; balloting was planned for 2Q 1991.
IEEE P1003.5	Ada Language Binding, Draft 8, November 1991; approval expected in 2Q 1992
IEEE P1003.6	Security Interface for POSIX, Draft 12 balloted October 1991; approval expected 3Q 1992
IEEE P1003.7	Administered Systems (name changed from System Administration Interface), Work is being "sliced" into ballotable partitions which will be balloted separately in October 1992.
IEEE P1003.7a	Printing, Draft 1, May 1991.
IEEE P1003.7b	Software, Draft 1, July 1991
IEEE P1003.8	Transparent File Access (TFA), Draft 5, October 1991; mock balloting 4Q 1991.
IEEE 1003.9	FORTRAN Language Binding, Draft 11 approved October 1991
IEEE P1003.10	Supercomputing Application Environment Profile (AEP), Draft 5, March 1991; Draft 9 to be balloted July 1992
IEEE P1003.11	Transaction Processing, Draft 2, March 1991; mock ballot of Draft 5 planned for January 1992; ballot expected mid-1992
IEEE P1003.12	Protocol Independent Interfaces, Working pre-draft July 1991; balloting planned for 1992.
IEEE P1003.13	Real-Time AEP, Draft 2, March 1991
IEEE P1003.14	Multiprocessing Application Support AEP, Draft 5, October 1991; mock balloting October 1991.
IEEE P1003.15	Batch Environment Amendments, Draft 6, July 1991, balloting of Draft 10 planned for July 1992.

IEEE P1003.16	C Language Binding, Draft 1, May 1991; balloting expected 2Q 1992
IEEE P1003.17	Directory Services API-, Draft 2, September 1991; balloting planned for 2Q 1992
IEEE P1003.18	POSIX Platform Profile, Draft 4, January 1991; ballot planned for Spring 1992
IEEE P1003.19	POSIX Ada Language Interfaces, Part 1: Binding for Realtime Extensions, PAR approved, September 1991
ANSI/IEEE 1008	IEEE Standard for Software Unit Testing, 1987
ANSI/IEEE 1012	IEEE Standard for Software Verification and Validation Plans, 1987
ANSI/IEEE 1016	IEEE Recommended Practice for Software Design Descriptions, 1987
IEEE 1028	IEEE Standard for Software Reviews and Audits, 1988
ANSI/IEEE 1042	IEEE Guide to Software Configuration Management, 1988
IEEE P1044	Classification of Software Errors/Faults/Failures
IEEE P1045	Software Productivity Metrics
ANSI/IEEE 1058.1	IEEE Standard for Software Project Management Plans, 1987
IEEE P1058.2	Guide for Software Project Management Plans [PAR WITHDRAWN March 21, 1991]
IEEE P1059	Software Verification and Validation
IEEE P1061	Software Quality Metrics Methodology
IEEE P1062	Software Acquisition
ANSI/IEEE 1063	IEEE Standard for Software User Documentation, 1989
IEEE 1074	Standard for Developing Software Life Cycle Processes, (approved September 1991)
IEEE 1154	Standard for Programmed Inquiry Learning, or Tracking, 1991
IEEE P1172	Object Oriented Programming Language and Environment, Draft
IEEE P1178	SCHEME Language Standard, [Standard approved 6 December 1990]
IEEE P1201.1	Window Interface for User Application and Portability, Draft (Ballot planned for 2Q 1993)
IEEE P1201.2	Recommended Practice on Driveability (balloting expected 2Q 1992)
IEEE P1209	Recommended Practice for Evaluation of CASE Tools, Draft
IEEE P1219	Software Maintenance Standard
IEEE P1224	Common ASN.1 Object Management API for X.400 and Directory Services API, Draft 3, 1991. (Ballot expected 1Q 1992)
IEEE P1224.1	X.400 Based Electronic Messaging API [ballot planned for mid-1991]
IEEE P1228	Software Safety Plans
ANSI/IEEE 729	IEEE Standard Glossary of Software Engineering Terminology, 1983
IEEE P1237	Remote Call Procedure Interface Language, PAR approved May 1990
IEEE P1238	OSI Application Program Interfaces (Group formed January 1990; PAR approved May 1990; Draft 4 to be balloted January 1992)
IEEE P1238.1	OSI Application Program Interfaces, File Transfer, Access and Management (FTAM), (Group formed January 1990; PAR approved May 1990; ballot planned for 1993)
IEEE P1252	Standard for an Open Architecture for Knowledge Presentation (PAR approved 6 December 1990)
IEEE P1256	Standard for an Open Basic Input/output System Software (OBIOS), [PAR approved March 21, 1991]
FIPS 121	Videotext/Teletext Presentation Level Protocol Syntax (PLPS), (ANSI X3.110)
FIPS 127	Database Language SQL, 10m March 1987, [ANSI X3.135-1986]

FIPS 128	Computer Graphics Metafile, 16 March 1987, [ANSI X3.122-1986]
FIPS 146-1	Government Open Systems Interconnection Profile (GOSIP), FIPS 146-1, Version 2.0, U.S. National Institute of Standards and Technology, 3 April 1991
FIPS 151	POSIX, 12 September 1988 [IEEE 1003.1]
FIPS 152	SGML, 26 September 1988 [ISO 8879-1986]
FIPS 156	Information Resource Directory System (IRDS), 05 April 1989 [ANSI X3.138-1988]
FIPS 160	Information Systems - Languages - Programming Language C, 1989 (ISO 9899: 1990; ANSI X3.159)
Stable Agreements	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 2, Edition 1, NIST Special Publication 500-16, National Institute of Standards and Technology, December 1988 (basis for U.S. GOSIP 1.0)
Stable Agreements	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 3, Edition 1, NIST Special Publication 500-177, National Institute of Standards and Technology, March 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop; basis for U.S. GOSIP 2.0)
Working Agreements	Working Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements, Volume 2, Number 2, NISTIR 90-4247, National Institute of Standards and Technology, February 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop)
Yellow Book	Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Yellow Book), CSC-STD-003-85, DoD Computer Security Center, June 1985
Yellow Book Rationale	Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85, DoD Computer Security Center, June 1985
Orange Book	Department of Defense Trusted Computer System Evaluation Criteria (Orange Book), DoD 5200.28-STD, DoD Computer Security Center, December 1985
Red Book	Trusted Network Interpretation (Red Book), NCSG-TG-005, Version 1, National Computer Security Center, July 1987
SDN.301	Secure Data Network System (SDNS) Security Protocol 3 (SP3), Revision 1.5, SDNS Protocol and Signalling Working Group, 15 May 1989, National Security Agency, UNCLASSIFIED
SDN.401	Secure Data Network System (SDNS) Security Protocol 4 (SP4), Revision 1.3, SDNS Protocol and Signalling Working Group, 2 May 1989, National Security Agency, UNCLASSIFIED
SDN.601	Secure Data Network System (SDNS) Key Management Profile, Communication Protocol Requirements for Support of the SDNS Key Management Protocol, Revision 1.5, SDNS Protocol and Signalling Working Group, 11 August 1989, National Security Agency, UNCLASSIFIED
SDN 701	Secure Data Network System (SDNS) Message Security Protocol (MSP), Revision 1.5, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN.702	Secure Data Network System (SDNS) Directory Specifications for Utilization with the SDNS Message Security Protocol (MSP), Revision 1.4, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN.801	Secure Data Network System (SDNS) Access Control Concept Document, Revision 1.3, SDNS Protocol and Signalling Working Group, 26 July 1989, National Security Agency, UNCLASSIFIED

SDN.802	Secure Data Network System (SDNS) Access Control Specification, Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency, UNCLASSIFIED
SDN.802/1	Secure Data Network System (SDNS) Access Control Specification, Addendum 1, Access Control Information Specification (ACIS), Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency, UNCLASSIFIED
SDN 902	Secure Data Network System (SDNS) Key Management Protocol, Definition of Services Provided by the Key Management Application Service Element (KMASE), Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN 903	Secure Data Network System (SDNS) Key Management Protocol, Specification of the Protocol for Services Provided by the Key Management Application Service Element (KMASE), Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN 906	Secure Data Network System (SDNS) Key Management Protocol, SDNS Traffic Key Attribute Negotiation, Revision 1.3b, SDNS Protocol and Signalling Working Group, 18 September 1989, National Security Agency, UNCLASSIFIED

APPENDIX I

BACKGROUND, OBJECTIVE, AND STATEMENT OF WORK

APPENDIX I

BACKGROUND, OBJECTIVE, AND STATEMENT OF WORK

(U) This IDA Paper was written in response to Task Order T-J1-246 and Amendment No. 11. Those portions of the task order that pertain to the background and objectives of the task, and the additional guidance provided therein by the sponsoring office, are reprinted here.

2. BACKGROUND:

The tactical automated data processing (ADP) portion of the NATO Long Term Defense Program (LTDP) proposed that command and control systems be built to common specifications. The Deputy SACEUR initiated a study to determine the feasibility of the nations in the Central Region commonly developing an automated Army Tactical Command and Control Information System (ATCCIS) for deployment in the post-1995 timeframe. Commitments for supporting this effort were obtained from the United States, United Kingdom, France, and Federal Republic of Germany Army Chiefs of Staff. These nations provided information on their operational doctrine, procedures, functions, and information exchange requirements for their maneuver forces, as well as their operational requirements for an automated CCIS and information on the ADP systems that they are currently developing to support their maneuver forces. This information was used in the initial phase of the study to determine the extent to which similarities and differences in national requirements for automated CCISs would indicate that a commonly developed system is potentially feasible.

ATCCIS Phase II was successfully completed in 1990. In view of the significant force structure changes resulting from the Conventional Forces Europe (CFE) Agreement, e.g., the planned deployment of corps and division level multinational forces, SHAPE has now requested that the Nations initiate a Phase III effort to implement the operational and technical concepts developed during Phase II. This work will be progressed by the existing ATCCIS Permanent Working Group (PWG) consisting of military officers and technical experts from the four Nations, personnel from SHAPE and other NATO commands as well as technical support from the SHAPE Technical Centre. This

international effort is scheduled to last several years and its deliverables will provide the basis through which SHAPE, the NATO Military Agency for Standardization (MAS), and the Nations can develop and agree to the operational, procedural, and technical STANAGs required for the next generation of land force tactical command and control systems. IDA provides U.S. technical analytical support to the international PWG.

3. OBJECTIVE:

The objective of the Phase III effort is to assist SHAPE and the Nations in developing interoperability specifications from agreed standards appropriate to the ATCCIS operational and technical concepts, and validating the ATCCIS interoperability principles in a demonstration.

4. STATEMENT OF WORK:

The FY 1992 task includes:

b. Furnish a draft of ATCCIS Working Paper 25, *Technical Standards for CCISs*, Edition 3.0, by 31 March 1992

APPENDIX J

DISTRIBUTION LIST

DISTRIBUTION LIST

	No. of Copies
Office of the Secretary of Defense	
Director, Defense Information The Pentagon, 3E240 Washington, DC 20301	1
Office of the Assistant Secretary of Defense (C^3I) ATTN: Director, T&TC3 The Pentagon, Room 3D174 Washington, DC 20301-3040	10
Office of the Assistant Secretary of Defense (C^3I) ATTN: Telecommunications The Pentagon, Room 3E187 Washington, DC 20301-3040	1
Office of the Secretary of Defense (C3CM) ATTN: Mr. Jim Dyer The Pentagon, Room 3D200 Washington, DC 20301	1
Assistant Secretary of Defense for Production and Logistics ATTN: DQSO (Mr. Samuel Miller) 2 Skyline Place, Room 1406 5203 Leesburg Pike Falls Church, VA 22041-3466	1
Director, Defense Materiel Specifications and Standards Office ATTN: DQSO (Mr. Robert Gagnon) Two Skyline Place, Room 1403 5203 Leesburg Pike Falls Church, VA 22041-3466	1
Joint Chiefs of Staff	
Joint Staff ATTN: J6 The Pentagon, Room 2D866 Washington, DC 20301-5000	1
Joint Staff ATTN: J6C (Mr. Paul C. Fang) The Pentagon, Room 1E833 Washington, DC 20318-6000	1
Joint Staff ATTN: J6I (COL James D. Bryan) The Pentagon, Room 1E833 Washington, DC 20301-5000	1
Joint Staff ATTN: J6J (LTC L.P. Filipkowsky) The Pentagon, Room 1C826 Washington, DC 20318-6000	1
Joint Staff ATTN: J6U (Mal Billings) The Pentagon, Room 1D770 Washington, DC 20301-5000	1
Joint Staff Military Communications-Electronics Board (DP and ES Panels) ATTN: CDR W.B. (Bill) Zell The Pentagon, Room 1B707 Washington, DC 20301-5000	20
Defense Agencies and NSA	
Director, Defense Information Systems Agency Joint Interoperability and Engineering Organization ATTN: JIEO/TVCF (James Robinette) Virginia Square Plaza 3701 N. Fairfax Drive Arlington, VA 22203	2
Director, Defense Information Systems Agency ATTN: TDH, NATO Liaison Office (Steve Goya, LTC Candace Velez) Virginia Square Plaza 3701 N. Fairfax Drive Arlington, VA 22203	1
Director, Defense Information Systems Agency Center for Information Management ATTN: CIM/XT (Mr. John Keane) 701 South Court House Road Arlington, Virginia 22204-2199	1
Director, Defense Information Systems Agency Center for Information Management ATTN: CIM/XT (Mr. Mike Griefner) 701 South Court House Road Arlington, Virginia 22204-2199	1
Director, Defense Information Systems Agency Center for Information Management ATTN: Terry Hagle 1225 Jefferson Davis Highway Crystal Gateway #2, Suite 910 Arlington, Virginia 22202	1

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Switched Networks Engineering
ATTN: DRF (Mr. M. Hanz, Deputy Director)
1860 Wiehle Avenue
Reston, VA 22090-5500

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
DDN Systems Engineering
ATTN: DRFD (Mr. George Bradshaw)
1860 Wiehle Avenue, Room 2B01
Reston, VA 22090-5500

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Data Networks Engineering
ATTN: DRFE (Mr. Edward Cain)
1860 Wiehle Avenue
Reston, VA 22090-5500

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: DRFE (Mr. Robert Cleary)
1860 Wiehle Avenue
Reston, VA 22090-5500

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: DRFE (Mr. James Showalter)
1860 Wiehle Avenue
Reston, VA 22090-5500

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: DRFEE (Mr. Sherrill Adkins)
1860 Wiehle Avenue
Reston, VA 22090-5500

Director, Defense Information Systems Agency 1
Center for C3 Systems
ATTN: TV (Ms. Marilyn Kraus)
Virginia Square Plaza, Room 540
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
ATTN: JIEO/TVCE (Mr. Eli Williams)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
ATTN: Mr. Bob Leary
Virginia Square Plaza, Room 617
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Defense Systems Support Organization (DSSO)
ATTN: JD (Col Phil Daley, Principal Deputy Director)
Building 12, Room 2260
Washington, DC 20350

Director, Defense Information Systems Agency 1
Defense Systems Support Organization (DSSO)
WWMCCS ADP Technical Support Directorate
ATTN: JWSA (Ms. Jeanette Carter, Ms. Mary Jane Haley)
45335 Vintage Park Plaza
Sterling, Virginia 22170-6701

Director, Defense Information Systems Agency 1
Defense Network Systems Organization (DNSO)
ATTN: DI (Mr. John Edell)
Virginia Square Plaza, Room 302
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Defense Network Systems Organization (DNSO)
DMS Coordination Division
ATTN: DISDA (CDR Anthony Montemarano)
MITRE Wilson Building
7600 Old Spring House Road
McLean, VA 22102

Director, Joint Interoperability and Engineering Organization 1
Center for Standards Information Processing Directorate
ATTN: JIEO/TBE (CAPT Dante Marzetta)
Kidwell Building
701 South Court House Road
Arlington, VA 22204-2199

JSARO 1
ATTN: Army/Navy/USMC/AF/NSA/DIA
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Center for Interoperability Assurance
Defense Wide Architecture and Planning
ATTN: JIEO/TD (Dr. William Vogelzang)
Virginia Square Plaza, Room 432
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Joint Interoperability and Engineering Organization 1
Director, Center for Standards
ATTN: JIEO/TB (Dr. Jeremy Kaplan)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Joint Interoperability and Engineering Organization 1
Center for Standards (JIEO-TBA)
ATTN: Mr. Joe Pasqueriello, Associate Director
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 3
ATTN: JIEO/TBBG (Mr. Dick Savoye)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Secretary, Protocols Standards Steering Group
ATTN: TBBD (LCDR David Chappell)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Standards Management Division
ATTN: JIEO/TBBG (Mr. Gary Koerner)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Directorate, TADIL Division
ATTN: JIEO/TBC (Maj Linda Smith)
11440 Isaac Newton Square
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Directorate, TADIL Division
ATTN: JIEO/TBC (LCDR Diane Bartch)
11440 Isaac Newton Square
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Standards Support Directorate, Plans and Program Office
ATTN: JIEO/TBDA (Mr. David Sweet)
11440 Isaac Newton Square
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Combat Development Directorate
ATTN: JIEO/TDE (LTC Robert Fernekes)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Interoperability Programs Directorate
ATTN: JIEO/TDF (Mr. Joseph Vitale)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Interoperability Programs Directorate
ATTN: JIEO/TDF (Mr. Jimmie Lee)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Joint Interoperability and Engineering Organization 1
Center for Standards (JIEO-TB)
ATTN: Library
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 3
Center for Standards/TBA
ATTN: Salvatore Manno, Asst Dir for International Affairs
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization
CINC Operations Directorate 1
ATTN: JIEO/TD (Mr. Joseph Vinso)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate
ATTN: JIEO/TBB (COL Kenneth A. Thomas, Deputy Director)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Radio Division
ATTN: JIEO/TBBA (Mr. Louis Pilla)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Systems Integration Division
ATTN: JIEO/TBBB (Mr. Thomas J. Brincka)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Terminal and Signal Processing Division
ATTN: JIEO/TBBC (Mr. Edward F. Kovanic)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Terminal and Signal Processing Division
ATTN: JIEO/TBBC (Mr. Bill Scott)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 3
Center for Standards, Information Transfer Directorate, Data Systems Division
ATTN: JIEO/TBBD (Mr. Richard McLane)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Data Systems Division
ATTN: JIEO/TBBD (LCDR Kathleen Bryant)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Data Systems Division
ATTN: JIEO/TBBD (Dr. Frank D. Curcio)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Data Systems Division
ATTN: JIEO/TBBD (Mr. Andy DeRosa)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability and Engineering Organization 1
Center for Standards, Information Transfer Directorate, Data Systems Division
ATTN: JIEO/TBBD (Mr. Greg Scott)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Joint Interoperability Test Center 1
Tactical Communications Division
ATTN: JITC/TCB (Mr. Leo Hansen)
Fort Huachuca, AZ 85613-7020

Director, Joint Interoperability Test Center 1
Tactical Communications Division
ATTN: JITC/TCDB (Mr. Dwaine Huewe)
Fort Huachuca, AZ 85613-7020

National Communications System 1
ATTN: Code NT (Dennis Bodson, Frank McClelland, Robert Fenichel)
701 South Court House Road
Arlington, VA 22204-2198

Director, Defense Mapping Agency 1
ATTN: DMAA/RE (Mr. Bill James)
3200 South 2nd Street
St. Louis, MO 63118

NATO Integrated Communications Systems Management Agency 1
NACISA
ATTN: USDCFO
APO AE 09724

Director, National Security Agency 3
ATTN: V5 (Mr. Harold Staton)
9800 Savage Road
Fort George Meade, MD 20755-6000

Director, National Security Agency 2
ATTN: T7 (Mr. Gerald Bailey, Andy Hochreiter)
Fort George Meade, MD 20755-6000

Director, National Security Agency 2
ATTN: T71 (Capt Michael St. Johns)
Fort George Meade, MD 20755-6000

Director, National Security Agency 1
ATTN: V3 (Mr. Dick Norman)
Fort George Meade, MD 20755-6000

Director, National Security Agency 3
ATTN: S9 (Mr. George Stephens)
Fort George Meade, MD 20755-6000

Director, National Security Agency 1
ATTN: S11 (Mr. S. J. Buchanan)
Fort George Meade, MD 20755-6000

Director, National Security Agency 2
ATTN: R23 (Mr. Doug Maughan)
Fort George Meade, MD 20755-6000

Director, National Security Agency 1
ATTN: R536 (Mr. Ray McFarland)
Fort George Meade, MD 20755-6000

Director, Defense Intelligence Agency 1
ATTN: DSO-2A (Mr. Richard Weiand)
Washington, DC 20340-3412

Director, Defense Intelligence Agency 1
ATTN: DSE-2 (Mr. Gerard J. Rolape)
Washington, DC 20340

Director, Defense Intelligence Agency 1
INCA Project Office
ATTN: Vicki Williams
Washington, DC 20340

Director, Defense Intelligence Agency 1
DODIIS Program Office
ATTN: DS-SIM (Mr. Walter Jablonski)
Bolling Air Force Base, Building 6000
Washington, DC 20340

Director, Defense Logistics Agency 1
ATTN: DLA-ZID/DRDO (Mr. George Pogharion)
6303 Little River Turnpike at Beauregard Street, Suite 310
Alexandria, VA 22312-5040

Director, Defense Logistics Agency 1
Systems Automation Center
ATTN: DSAC-RSB (Mr. Clyde Grossarth)
P. O. Box 1605
Columbus, OH 43216-5002

Director, DISA
ATTN: XL (Mr. Robert Compton)
P. O. Box 1605
Columbus, OH 43216-5002 — 1

Department of the Army

HQDA ODISC4
Interoperability and Standards Office
ATTN: SAIS-ADO (LTC D.S. Woffinden)
The Pentagon, Room 1C634
Washington, DC 20310-0107 — 15

HQDA ODISC4
Interoperability and Standards Office
ATTN: SAIS-ADO (Mr. L. Tom Hendrick)
The Pentagon, Room 1C634
Washington, DC 20310-0107 — 1

HQDA ODISC4
Interoperability and Standards Office
ATTN: SAIS-ADO (Mr. Robert Johnson)
The Pentagon, Room 1C634
Washington, DC 20310-0107 — 1

Office of the Commanding General
U.S. Army Strategic Defense Command
ATTN: CSSO-DP (MAJ(P) Michael Napoliello)
P.O. Box 15280
Arlington, Virginia 22215-0280 — 3

Commander, US Army Signal Center
Directorate of Combat Development
ATTN: ATZH-CDM (ATTN: Lee Leyda)
Fort Gordon, GA 30905 — 1

Commander, US Army Signal Center
Directorate of Combat Development
ATTN: CPT Mike Thorne
Fort Gordon, GA 30905 — 1

CINCUSAREUR
ATTN: AEAIM-AR-AR (MAJ J. Fleming)
APO AE 09403 — 1

Commanding General, U.S. Army TRADOC
ATTN: ATCD-CB (R. Hill)
Fort Monroe, VA 23651 — 1

Commandant, Field Artillery School
TRADOC System Manager for Fire Support Systems
ATTN: ATSF-TSM-C3S (Mr. Arv Toso)
Fort Sill, OK 73503-5600 — 2

Director, US Army Information Systems Command (USAISC)
Software Development Center
ATTN: ASBH-SDM-S (Mr. Carlo Venditto)
Fort Huachuca, AZ 85613-5450 — 1

Director, USAISC-Pentagon
ATTN: ASQNS-TS-D (Mr. Thomas J. Kenavan)
The Pentagon, Room BE1018
Washington, DC 20310-3053 — 1

Commander, USAISEC
ATTN: ASQB-OSI-S (Mr. Jim Starkey)
Fort Huachuca, AZ 85613-5300 — 1

Commander, USAISMA
ATTN: Mr. Frank Dwulet
Fort Monmouth, NJ 07703 — 1

U.S. Army Material Command
International Standardization Agreements
ATTN: Robert W. Brown, Office of Record, AMCICP-SS
5001 Eisenhower Avenue
Alexandria, VA 22333-0001 — 1

Headquarters, Department of the Army
PEO-IEW
ATTN: Dae-Woo Lee
VHFS
Warrenton, VA 22186-5115 — 1

US Army, PEO STAMIS
ATTN: SFAE-PS-S (Michael Falat, Carl Salvino)
Fort Belvoir, VA 22060-5895 — 1

Commander, U.S. Army CACDA
ATTN: ATZL-CDC-F [MAJ James Edgar]
Ft. Leavenworth, KS 66027-3500 — 1

Commander, CECOM
PM CHS
ATTN: SFAE-CC-CHS (Col A. Taylor, Mr. Stan Levine)
Ft. Monmouth, NJ 07703-5000 — 3

Commander, CECOM
ATTN: SFAE-CC/DPEO GCS (Mr. Robert Giordano, Mr. Alvarelli)
Ft. Monmouth, NJ 07703-5000 — 2

Commander, CECOM
PM FATDS, Technical Management Directorate
ATTN: SFAE-CC-FS-TMD (Henry Saphow, Mike Simpson, Carlo Toussaint)
Ft. Monmouth, NJ 07703-5000 — 3

Commander, CECOM
PM OPTADS
ATTN: SFAE-CC-OPTDS (COL James Doyle, Joe D'Oria)
Ft. Monmouth, NJ 07703-5000 — 1

Director, Joint Tactical Fusion Program
ATTN: PM ASAS (COL Joseph Ganino)
1500 Planning Research Drive
McLean, VA 22102 — 1

Commander, CECOM
ATTN: PM ADDCS (COL David Taylor)
Redstone Arsenal, Alabama 35898 — 1

Commander, CECOM
Architecture and Engineering Directorate
ATTN: AMSEL-RD-AED-DD (Mr. Jack Zavin, Deputy Director)
Ft. Monmouth, NJ 07703-5000 — 1

Commander, CECOM 1
Information Systems Division
ATTN: AMSEL-RD-C3-TP-S (Mr. Wolfgang Fischer, Director)
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 6
Information Systems Division
ATTN: AMSEL-RD-C3-SD (Mr. J. Onufer, Jerry Mohr, Richard Lo, Ken Blum)
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
Information Systems Division
ATTN: AMSEL-RD-CC-F (Mr. Jack Plant)
Ft. Monmouth, NJ 07703-5000

Department of the Army AIRMICS 1
ATTN: Mr. Winfred Fong
115 O'Keefe Building
Georgia Institute of Technology
Atlanta, GA 30332-0800

Commander AMC ARDEC 1
ATTN: SMCAR-FSC (Dr. T. H. Chin)
Building 352 North
Dover, NJ 07801-5001

Department of the Navy

Department of the Navy 1
Information Resources Management
ATTN: Robert A. Green
C/O NAVCOMOCEN
Washington Navy Yard
Washington, DC 20374-1662

Chief of Naval Operations 1
C2 and EW Systems
ATTN: OP-942 (CAPT H. A. Browne, Jr., Director)
The Pentagon, Room 5E523
Washington, DC 20350

Chief of Naval Operations 1
Information Systems Management
ATTN: OP-945
The Pentagon, Room 5E724
Washington, DC 20350

HQ Department of the Navy 1
Navy Information System Management Center
ATTN: Code 03 (Marshall Potter, John Hooder)
Washington Navy Yard, Building 166
Washington, DC 20374-1662

Commander, Space and Naval Warfare Systems Command (SPAWAR) 2
Copernicus Office
ATTN: Capt John R. Wood, LCDR Keven Ebel
NC-1, Room 11E47
2511 Jefferson Davis Highway
Arlington, VA 20363-5100

Commander, Space and Naval Warfare Systems Command (SPAWAR) 3
ATTN: PMW-159 (CAPT Dave Ahern, Mr. Bob McAlpine, Mr. Jim Boland)
NC-1, Room 4N18
2511 Jefferson Davis Highway
Arlington, VA 20363-5100

Commander, Space and Naval Warfare Systems Command (SPAWAR) 1
Warfare Systems Engineering
ATTN: Interoperability Branch, Code 3213 (Mr.Miles Zich)
NC-1, Room 11E41
2511 Jefferson Davis Highway
Arlington, VA 20363-5100

Commander, Naval Research Laboratory 1
ATTN: Code 910 (Robert Parks)
4555 Overlook Avenue, SW, Room 2650
Washington, DC 20375

Director, Naval Ocean Systems Command 1
ATTN: Code 854 (Mr. Lou Gutman)
271 Catalina Boulevard
San Diego, CA 92152-5000

Naval Surface Weapons Center 1
ATTN: Code N35 (David Marlow, Karen O'Doneghue)
Dahlgren, VA 22448

Commander, NUSC 1
ATTN: Code 2222 (Richard Leary)
Building 1171-3
Newport, RI 02841

Office of Naval Technology 1
ATTN: Code 221 (Sherman Gee)
Ballston Center Towers #1, Room 503
800 North Quincy Street
Arlington, VA 22217-5000

Deputy Chief of Staff for Research, Development, and Studies 1
US Marine Corps
Code RD
Navy Annex, Room 3020
Washington, DC 20380

Director, C4 Division, US Marine Corps 1
Command and Control Interoperability Division
ATTN: Code C2I (COL C.T. Reilly, Jr., Deputy Director)
Federal Building 2 (Navy Annex), Room 3201
Washington, DC 20380-0001

Director, C4 Division, US Marine Corps 1
Command and Control Interoperability Division
Code C2I-P4 (Capt John Wiegand)
Federal Building 2 (Navy Annex), Room 3201
Washington, DC 20380-0001

Director, C4 Division, US Marine Corps 1
Command and Control Interoperability Division
Code C2I-O (Maj W. E. Heinzman)
Federal Building 2 (Navy Annex), Room 3201
Washington, DC 20380-0001

Director, C4 Division, US Marine Corps 1
Command and Control Interoperability Division
Code CCT-6 (Col Smith)
Federal Building 2 (Navy Annex), Room 3312
Washington, DC 20380-0001

Commander, Marine Corps Combat Development Command 1
MAGTF Warfighting Center
ATTN: International Standardization Office
Marine Corps Base
Quantico, VA 22134

Commander, Marine Corps Systems Command 1
ATTN: PM MAGTF C2
Marine Corps Base
Quantico, VA 22134-5080

Commander, Marine Corps Systems Command 8
Systems Integration
ATTN: C2OI (Maj Michael Mascarenas)
Marine Corps Base
Quantico, VA 22134-5080

Commander, Marine Corps Computers and Telecommunications Activity (MCTCA) 2
ATTN: LTC Loehman
Marine Corps Base
Quantico, VA 22134-5080

Commander, Marine Corps Tactical Systems Support Activity (MCTSSA) 1
ATTN: Col Brown, Commander
Camp Pendleton, CA 92055-5080

Commander, Marine Corps Tactical Systems Support Activity (MCTSSA) 1
ATTN: TSTB (J. Steenwerth)
Camp Pendleton, CA 92055-5080

Department of the Air Force

HQ USAF 1
DCS Plans and Operations
ATTN: AF/XO
The Pentagon, Room 4E1032
Washington, DC 20330

HQ USAF 1
DCS C4
ATTN: AF/SC
The Pentagon, Room 5B477
Washington, DC 20330

HQ USAF 1
ATTN: AF/SCMC
The Pentagon, Room 5B513
Washington, DC 20330

HQ USAF 1
ATTN: AF/SCXI
The Pentagon, Room 5C1083
Washington, DC 20330-5190

HQ USAF 1
ATTN: AF/SCXS (Mr. Fred Virtue)
The Pentagon, Room 5C1067
Washington, DC 20330-5190

HQ USAF 1
ATTN: AF/SCXS (LTC James G. Thompson)
The Pentagon, Room 5C1067
Washington, DC 20330-5190

HQ USAF Systems Command 1
ATTN: SC (Capt Gonzalez)
Andrews Air Force Base, MD 20334-5000

HQ USAF 1
ATTN: AFIA/IND (Mark Harris)
Bolling Air Force Base
Washington, DC 20332

Rome Laboratories 1
ATTN: C3D
Griffiss AFB, NY 13441-5700

HQ USAF 1
ATTN: SC/XPT (Ms. Elizabeth Crouse)
Gunter Air Force Base, AL 62225-6001

HQ USAF AFCC 1
ATTN: SAS (Mr. Peter Hughes)
Hanscom Air Force Base, MA 01731-5000

Electronics System Division 1
ATTN: OCC-2/MEITS/Ulana (Mr. Rick Cortez)
Hanscom Air Force Base, MA 01731-5000

HQ Tactical Air Forces 1
ATTN: TAC/DRI-SD (LtCol Charles Morris, Maj Thomas Spivey)
Langley Air Force Base, VA 23665-5575

HQ Tactical Air Forces 1
ATTN: TAC/DRI (LTC Frederickson)
Langley Air Force Base, VA 23665-5001

HQ Tactical Air Forces 1
ATTN: TAC/DRI-SP (Capt Bujosa)
Langley Air Force Base, VA 23665-5001

HQ USAF MODEL BASE Program Office 1
323 FTW/SC4
ATTN: Mr. James Johnson
Mather Air Force Base, CA 95655-5000

HQ USAF Space Command 1
ATTN: SYE (Capt Cosgrove)
Peterson Air Force Base, CO 80194-5001

HQ USAF AFCC 1
Technical Integration Center, Computer Standards Office
ATTN: TIC/TIS (Mr. Rex McKinnon, Chief)
Scott Air Force Base, IL 62225-6343

HQ USAF AFCC 1
Technical Integration Center, Computer
Standards Office
ATTN: TIC/TIS (MAJ Del Brashares)
Scott Air Force Base, IL 62225-6343

HQ USAF AFCC 1
Technical Integration Center, Computer
Standards Office
ATTN: TIC/TIS (Maj Doug Naegele,
Kat Goddard, John Wojdyla)
Scott Air Force Base, IL 62225-6343

HQ USAF AFCSIO 1
ATTN: SYTSC (Capt Mike Gillam,
Mr. Hiawatha Cotton)
Scott Air Force Base, IL 62225-6001

Air Force Logistics Command 1
Logistics Management Systems Center
Deputy for Communications Systems
ATTN: Mr. T. Brown
Wright-Patterson Air Force Base, OH 45433

Other Organizations

US Coast Guard 1
ATTN: Comdt G-TA (LCDR Buddenburg)
2100 Second Street, SW
Washington, DC 20583

Information Handling Committee, ICS
Mr. George W. Rogers, Jr., Vice-Chairman 1
Washington, DC 20505

National Institute for Science and Technology 1
ATTN: ICST (Mr. Al Hankinson)
Technology Building, Room B266
Gaithersburg, MD 20899

National Institute for Science and Technology 1
ATTN: ICST (Mr. Roger Martin)
Technology Building, Room B266
Gaithersburg, MD 20899

National Institute for Science and Technology 1
Systems and Network Architecture Division
ATTN: ISE (Mr. Kevin Mills, Chief)
Technology Building #225, Room B-217
Gaithersburg, MD 20899

National Institute for Science and Technology 1
Systems and Network Architecture Division
ATTN: ISE (Mr. Gerald Mulvenna)
Technology Building #225, Room B-217
Gaithersburg, MD 20899

National Institute for Science and Technology 1
Network Protocols Section
ATTN: ISE (Richard Collela, Jim West)
Technology Building #225, Room B-217
Gaithersburg, MD 20899

Center for Naval Analyses 1
401 Ford Avenue
P. O. Box 16268
Alexandria, VA 22302-0268

The MITRE Corporation 1
ATTN: Mr. William Blankhertz, Tactical C3I
145 Wyckoff Road
Eatontown, NJ 07724

The MITRE Corporation 1
ATTN: Ms. Pat Blankenship, Tactical C3I
145 Wyckoff Road
Eatontown, NJ 07724

The MITRE Corporation 1
ATTN: Mr. Rene Dube
Building 66157, Cushing Street
P. O. Box 925
Fort Huachuca, AZ 85613

The MITRE Corporation, Washington C3I 1
ATTN: Mr. Dave Woodall
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mr. David C. Wood
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Ms. Gladys Reichlen
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mail Stop W30 (Mr. Larry Stine)
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Library Services
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mr. Richard Kallagher
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Steve Silverman, Emily McCoy
7525 Colshire Drive
McLain, VA 22102-3481

The MITRE Corporation 1
ATTN: Mr. Lee LaBarre
Burlington Road
Bedford, MA 01730

The MITRE Corporation 1
ATTN: Mr. Paul J. Brusil
Burlington Road
Bedford, MA 01730

The MITRE Corporation 1
US Defense Communications Field Office
ATTN: Mr. Elbert J. Wells
NACISA (USCDFO)
APO AE 09724

ANSI X3.T5 1
ATTN: Kenneth M. Zemrowski, Chair
TRW, Inc.
One Federal Systems Park
Fairfax, VA 22033-4416

ARC Incorporated 1
ATTN: Steve Claiborne
234 S. Fraley Boulevard, Suite 308
Dumfries, VA 22026

Battelle 1
Seattle Research Center
ATTN: C. Richard Schuller
4000 N. E. 41st Street
Seattle, WA 98105

BDM Corporation 1
ATTN: Bill Walden, Charles Hayes,
W. E. Stewart
7915 Jones Branch Road
McLean, Virginia

Booz Allen Hamilton, Inc. 1
ATTN: Elmer McDowell
4330 East-West Highway
Bethesda, MD 20814-4455

CALCULON 1
ATTN: FATDS Programs Support
Office (Mr. Rost)
656 Shrewsbury Avenue
Shrewsbury, NJ 07701

Computer and Business Equipment
Manufacturer's Association 1
ATTN: ANSI X3 Secretariat
311 First Street, NW, Suite 500
Washington, DC 20001-2178

General Electric 1
ATTN: ATCCS Program Office
1301 Virginia Avenue, 4th Floor
Fort Washington, PA 19034

ITT Defense Communications Division 1
ATTN: David Blauvet
492 River Road
Nutley, NJ 07110-3696

Litton Data Systems 1
ATTN: Keith McNally
8000 Woodley Avenue
Van Nuys, CL 91409-7601

LOGICON 1
ATTN: E. Robert Sive, Darvel Stutts
145 Wyckoff Road, Suite 301
Eatontown, New Jersey 07724

LOGICON/Eagle Technologies, Inc. 1
ATTN: Dave Howe, Ray White
Systems Engineering Department
Linpro Park One, Suite 300
1831 Wiehle Avenue
Reston, VA 22090

LOGICON/Eagle Technologies, Inc. 1
ATTN: Judy Simpson, Erskin Sledd, Tom
Blizzard
Systems Engineering Department
P. O. Box 1196
Dumfries, VA 22026

Magnavox Corporation 1
ATTN: John Williams
1313 Production Road
Fort Wayne, Indiana 46808

Miltope Corporation 1
ATCCS Program Office
Hershey, PA

OMNICON, Inc. 1
ATTN: Kathy Dally
115 Park Street, S.E.
Vienna, VA 22180

Open Software Foundation 1
ATTN: Robert Cathaway
11 Cambridge Center
Cambridge, MA 02142

SPARTA, Inc. 1
ATTN: Mr. Bob Harris, Charles Eldrige
7926 Jones Branch Road, Suite 900
McLean, VA 22102

State of Texas 1
Department of Information Resources
ATTN: Mr. Jerry Johnson
Post Office Box 13564
Austin, TX 78711

System Planning Corporation 1
ATTN: Dr. C. Tucker Battle, Vice President
1500 Wilson Boulevard
Arlington, Virginia 22209-2454

TELOS Federal Systems 1
ATTN: Mr. Ernest Hamik
1201 West Gore
Lawton, OK 73501

TRW Defense Systems Group 1
ATTN: Mr. Hershie Krisch
One Space Park
Redondo Beach, CA 90278

X/OPEN 1
1750 Montgomery Street
San Francisco, CA 94111

Defense Technical Information Center 2
Cameron Station
Alexandria, VA 22314

Institute for Defense Analyses 40
1801 N. Beauregard Street
Alexandria, VA 22311-1772

TOTAL: 317

(This page intentionally left blank.)

REFERENCES

[AAP-4 1990] *NATO Standardization Agreements and Allied Publications*, AAP-4, 1990.

[AC/302 1990] Report of AC/302(TSGCEE) Meeting Held on 23-25 January 1990, U.S. Mission, NATO, 31 January 1990.

[ACCST 1986] *Air Command and Control System Master Plan, Volume IV, Overall ACCS Design, Book 2, Generic Portion*, ACCST(86)282/057, NATO, April 1986, NATO CONFIDENTIAL.

[ACCST 1988] *Air Command and Control System Master Plan, Volume IV*, Overall ACCS Design Generic Portion, ACCST(86)281-282/057 (Revised)/ACC-1086, *Supporting Document 4, Structure and Characteristics of Organizational Components*, May 1988, NATO CONFIDENTIAL.

[ACP 123 1991] *Final Draft ACP 123 Requirements Document*, Prepared by PRC, Incorporated, for the U.S. Defense Information Systems Agency, Deliverable 6, 20 November 1991, UNCLASSIFIED.

[ACP 167 1981] ACP 167(F), *Glossary of Communications-Electronics Terms*, NATO, August 1981.

[Ada 9X 1990] Ada 9X Project Report: *Ada 9X Revision Issues, Release 2, U.S. Office of the Under Secretary of Defense for Acquisition*, May 1990.

[ADatP-2 1985] ADatP-2(D), NATO *Glossary of Automatic Data Processing (ADP) Terms and Definitions*, December 1985, NATO UNCLASSIFIED.

[ADatP-3 1986] ADatP-3 (STANAG 5500), *NATO Message Text Formatting Systems, Part IV, Catalog of Standard Field Formats*, December 1986, NATO UNCLASSIFIED.

[ADatP-3 1986a] ADatP-3 NATO *Message Text Formatting System, Part 1, System Concept and Description*, Third Draft, 6 October 1986.

[ADSIA 1986] *Transmission Independent Data Link Architecture*, ADSIA-RCA-C-10-86, 12 February 1986, NATO UNCLASSIFIED.

[ADSIA 1987] *The Need for Standardization of Data Management and Data Base Information Exchange in the NATO CCIS, Enclosure 2 to ADSIA-RCA-WP/44 (Revised), ADSIA*, September 1987, NATO UNCLASSIFIED.

[ADSIA 1988] *NATO Interoperability Management Plan (NIMP), Third Endorsement Edition, ADSIA-RCU-D/1 (Revised), Allied Data Systems Interoperability Agency*, 1 July 1988, NATO UNCLASSIFIED.

[ADSIA 1988a] *Briefing to the 22nd ADSIA Plenary on the Quadrilateral Interoperability Program, Annex V to ADSIA-RCX-DS/22, ADSIA Staff*, 17-21 October 1988, NATO UNCLASSIFIED.

[ADSIA 1990] *Media Independent Data Link Architecture*, ADSIA-RCA-C-106-90, 28 May 1990, NATO UNCLASSIFIED.

[Ahern 1991] *Report of the U.S. Representative (Capt D. G. Ahern) to WG4*, June 1991, UNCLASSIFIED.

[AHWG 1989] *Response to Q62 on Quality of Service, Chair*, AHWG-OM, 10 March 1989.

[AHWG 1990] *NATO Requirements for Open Systems Management*, TSGCEE SG9 AHWG-OM, 28 June 1990, NATO UNCLASSIFIED.

[AHWG 1990a] *Liaison to SG9 Concerning Work on the Quality of Service Issue*, TSGCEE SG9 AHWG-OM, 27 June 1990, NATO UNCLASSIFIED.

[AHWG 1990b] SG9 AHWG-OSI Management Meeting Report, 25-29 June 1990, Ottawa, U.S. Representative to AHWG-OM, 6 July 1990.

[AHWG-ISDN] Report of the 2nd Ad Hoc Meeting on ISDN, Paris, 24-26 April 1990] 1990, AHWG on ISDN, May 1990, NATO UNCLASSIFIED.

[AHWG-ISDN] ISDN/OSI Integration: Issues, Trends, and Recommendations, 1990a] Contribution from Canada to the Iniial Meeting of 29-31 January 1990, AHWG on ISDN, January 1990, NATO UNCLASSIFIED.

[AHWG-ISDN] *Proposed NATO Standards on Packet Mode Services, U.S.* 1990b] Contribution *to the AHWG on ISDN*, 24 May 1990, NATO UNCLASSIFIED.

[AHWG-MMHS] *Base Standard for MMHS, Working Draft*, Submitted to the 1990) March Meeting of WG/2, AHWG on MMHS, February 1990, NATO UNCLASSIFIED.

[AHWG-MMHS] *Military Message Handling System (MMHS) Rationale Document*, 1990a] Working *Draft*, U.S. Input to the February 1990 AHWG on MMHS Meeting in Brussels, 12 February 1990, NATO UNCLASSIFIED.

[AHWG-MMHS] *MMHS AHWG Input to NATO TSGCEE SG/9 WG/2--12-month* 1990b] Work *Plan, TSGCEE SG9 WG2*, February 1990, NATO UNCLASSIFIED.

[AHWG-OM 1990] *Private communication with the U.S. Representative to the AHWG-OM*, 19 June 1990, NATO UNCLASSIFIED.

[AHWG-S 1990] Chairman's Report of the 8th Meeting, AC/302(TSGCEE)SG/9 Ad Hoc Working Group on Security, May 1990, NATO UNCLASSIFIED.

[AHWG-S 1990a] *Private communication with the Chair, TSGCEE SG9 AHWG on Security*, 18 June 1990, NATO UNCLASSIFIED.

[AJPO 1989] *Rationale for MIL-STD-1838A (CAIS), prepared by SofTech, Inc., for the Ada Joint Program Office*, 30 September 1989.

[Anderson 1989] *"Windows and Widgets (MIT X)," R. Anderson, Computer Systems Europe*, April 1989.

[ANSI 1991] *X3 Announces Solicitation of Comments on the Final Report of the Object-Oriented Database Task Group (OODBTG)*, ASC X3, Information Processing Systems News Release, 1 October 1991.

[ANSI 1991a] X3T5 Meeting at CBEMA in Washington, D.C., 1-2 October 1991.

[APP 1991] *Application Portability Profile (APP): The U.S. Government's Open System Environment Profile, Systems and Software Technology Division, National Computer Systems Laboratory, National Institute of Standards and Technology, NIST Special Report, Public Review Draft* 15 November 1990, January 1991.

[Army 1989] *U.S. Army Transition Strategy*, 1989.

[ASDC3I 1987] Memorandum on Open Systems Interconnection Protocols, ASD(C3I), 2 July 1987.

[ATCCIS 1988] ATCCIS Working Paper 24, *Architecture Definition*, Edition 2, 24 October 1988, NATO UNCLASSIFIED.

[ATCCIS 1990] *ATCCIS Phase II Final Report*, ATCCIS Permanent Working Group, SHAPE, October 1990, NATO RESTRICTED.

[ATCCIS 1991] *ATCCIS Phase III Project Brief*, ATCCIS Permanent Working Group, SHAPE, 22 November 1991, NATO UNCLASSIFIED.

[Bahnji 1990] *Transport Protocols and Internetworking in Low Bandwidth Tactical Networks*, Shiraz G. Bhanji, The MITRE Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Bailey 1990] *MOD(U.K.) Plans for OSI: Civil Section Relationship*, M. A. Bailey, MOD(U.K.) Directorate General of Information Technology Systems (DGITS), Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Bainbridge 1989] Report on JTC1 SC21/WG5 OSI Transaction Processing Rapporteur Group Meeting, Florence, 1-9 November 1989, A. J. Bainbridge, British Standards Institute, IST/21:1850, 14 November 1989.

[Baybrook et al.] *"Integrated Geographic Information Systems (GISs) for Joint/ 1990] Combined C3I Requirements," Thomas G. Baybrook and Tolbert A. Williams, Integraph Corporation, Geo'89 Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, *Symposium Proceedings 6, Volume 1 (Unclassified Papers)*, SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[BBN 1989] *SIMNET Network and Protocols*, Report Number 7102, A. Pope, BBN Systems and Technology Corporation, July 1989.

[Beggs 1992] Private communication with LTC. Robert Beggs, Department of National Defence, Canada, 16 January 1992, NATO UNCLASSIFIED.

[Bevan 1989] Briefing on ISO Standards for User System Interaction, N. Bevan, et al., CHI'89 Conference, May 1989.

[BICES 1988] BICES User Requirements (U), Final Draft, 3 March 1988, CS/C/EL(88)259, AC/302(PG/7) Serial 25, NATO CONFIDENTIAL.

[Billingsley 1990] *The Standards Factor: Standards on the Horizon*, Pat Billingsley, SIGCHI Bulletin, Volume 22, No. 2, October 1990, pp. 10-12.

[Blankertz 1990] *Briefing to the Protocol Standards Steering Group on Tactical Data Networking* In Europe, Bill Blankertz, The Mitre Corporation, 27 February 1990.

[Booz-Allen 1991] *DoD Standardized Profiles*, Briefing to the DTMP by Booz-Allen-Hamilton, July 1991, UNCLASSIFIED.

[Borenstein 1991] *"Multimedia Electronic Mail: Will the Dream Become a Reality?,"* by Nathaniel S Borenstein, in *Communications of the ACM, Volume 34*, No. 4, April 1991, pp. 117-119.

[Brettnacher et al.] *Accueil Logiciel Future*: Overview of the Project, J. M. 1988] Brettnacher, et al., ESPRIT '88--*Putting the Technology to Use, Proceedings of the 5th Annual ESPRIT Conference*, Volume 1, 1988.

[Briggs 1988] *Briefing to ATCCIS PWG on SD&IC Plans by John Briggs*, ADSIA, 7 December 1988, NATO UNCLASSIFIED.

[BSI 1989] Minutes of the IST21 Ad Hoc Security Meeting Held at the BSI Conference Centre, BSI IST21, 11 December 1989.

[C3 1989] *Implementation of Multicommand Required Operational Capability (MROC) 3-88, The Defense Mapping System (DMS), Director for C3 Systems, Joint Staff*, 6 February 1989.

[CA 1989] NATO *Requirements for OSI Testing--Issues and Recommendations, CA Contribution to NATO TSGCEE SG9*, 15 February 1989.

[Cardonna 1988] Briefing to TSGCEE SG9 on Conformance Testing, by Ralph Cardonna, U.S. Precoordination Meeting, 30 August 1988.

[Cargill 1989] Cargill, Carl F. 1989. *Information Technology Standardization: Theory, Process, and Organizations.* Bedford, MA, Digital Press.

[Carlson 1991] *"A Survey of Computer Graphics Image Encoding and Storage Formats,"* by Wayne E. Carlson, in *Computer Graphics, Volume 25*, No. 2, April 1991, pp. 67-75.

[Cassese 1990] *Secure Data Communication Defence System*, Vincenzo Cassese, ALCATEL CIT, France, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[CBEMA 1989] *X-3 Information Processing Systems Accredited Standards Committee Projects Manual*, X3/SD-4, CBEMA, 1989.

[CCTA 1990] *U.K. Government OSI Profile, Volume I, Introduction, Version 3.1, Central Computer and Telecommunications Agency*, London, 1990.

[CCTA 1990a] *U.K. Government OSI Profile, Volume II, Specification, Version 3.1, Central Computer and Telecommunications Agency, London*, 1990.

[CCTA 1990b] *U.K. Government OSI Profile, Volume III, Procurement Handbook, Version 3.1, Central Computer and Telecommunications Agency*, London, 1990.

[CCTA 1991] IS Notice No. 27, *Towards Open Systems: The CCTA "Migration to OSI" Programme*, CCTA, 6 September 1991.

[CCTA 1991a] *Electronic Data Interchange*, IS Notice No. 31, Central Computer and Telecommunications Agency, United Kingdom, 25 November 1991.

[CCTA 1991b] *GOSIP 4 Supplier Set*, Six Volumes; Volume 1 - Overview; Volume 2 - Network Support; Volume 3 - Application Services (1); Volume 4 - Application Services (2); Volume 5 - Interchange Formats and Ancillary Services; and Volume 6 - Annexes (containing interim specifications).

[CCTA 1991b] *GOSIP 4 Purchaser Set*, Five Volumes; Volume 1 - Overview; Volume 2 - Network Support, Volume 3 - Application Services; Volume 4 - Information Interchange and Supporting Services; Volume 5 - Annexes (containing tutorial material and references).

[CECOM 1989] Discussions with staff from the Information Systems Directorate, CECOM, March 1989.

[CEN 1989] *Result of Formal Vote on prENV 40002, CEN*, 22 November 1989.

[Chair 1989] *Private communication with the Chair*, TSGCEE SG9 WG1, 14 March 1989.

[Chesson 1988] *XTP/PE Overview*, Greg Chesson, Silicon Graphics, April 1988.

[CIM 1991] *Technical Reference Model for Corporate Information Management*, Versions 1.0, Center for Information Management, U.S. Defense Information Systems Agency, 4 November 1991, UNCLASSIFIED.

[CIS 1990] *CASE Interface Services Base Document*, CASE Integration Services (CIS) Committee, September 1990.

[Clifford et al.] *"The Development of PEX--A Graphics Extension to X11,"* W. H. 1988] Clifford, et al, *EUROGRAPHICS '88, Proceedings of the European Computer Graphics Conference and Exhibition*, Nice, France, 12-16 September, 1988.

[CODASYL 1980] *A Framework for Distributed Database Systems: Distribution Alternatives and Generic Architecture*, CODASYL, 1980.

[COE 1991] *Fleet Communications in the Copernicus Architecture*, Final Draft, 20 June 1991, UNCLASSIFIED.

[Collela 1992] Private communication with Richard Collela, NIST, 14 January 1992, UNCLASSIFIED.

[Collela 1992a] *Work Plan for the Development of a Common OSI Specification*, Private Communication from Richard Collela, NIST, 14 January 1992, UNCLASSIFIED.

[Computerworld] "ISDN Not Popular in Europe - Yet," in *Computerworld*, 1991] November 25, 1991, p. 45.

[COPERNICUS] *Fleet Communications in the Copernicus Architecture*, Final Draft, 1991] 20 June 1991, UNCLASSIFIED.

[COS 1989] *Cooperation Agreement with Japan, Memorandum for the Members of the COS Board of Trustees, Corporation for Open Systems*, 19 June 1989.

[CSC 1985] *Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Yellow Book)*, CSC-STD-003-85, DoD Computer Security Center, June 1985.

[CSC 1985a] *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Yellow Book Rationale)*, CSC-STD-004-85, DoD Computer Security Center, June 1985.

[CSC 1985b] *Department of Defense Trusted Computer System Evaluation Criteria* (Orange Book), DoD 5200.28-STD, DoD Computer Security Center, December 1985.

[CSC 1987] *Trusted Network Interpretation* (Red Book), NCSG-TG-005, Version 1, National Computer Security Center, July 1987.

[CSI 1990] *Standardization Activities," in Computer Standards and Interfaces, Volume 11, No. 1*, 1990, p. 78.

[DAFTG 1982] *An Architectural Framework for Database Standardization*, Draft, ANSI DAFTG, 1982.

[Davis 1990] *"Relationship Between ECMA PCTE and PCTE+,"* Hugh Davis, PCTE Newsletter, No. 4, June 1990, P. 12.

[DCA 1988] *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy, Defense Communications System Organization, DCA*, May 1988 (promulgated 17 June 1988).

[DCA 1988a] *Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)*, DCA, December 1988.

[DCA 1989] *WWMCCS ADP Modernization (WAM) Decision Coordinating Paper (DCP), Joint Data Systems Support Center, Defense Communications Agency*, November 1989.

[DCA 1989a] *Briefing on OSI Security Standards, Goals of NIST, Briefing to the Protocol Standards Steering Group*, DCA/NSA/NIST, 31 January 1989.

[DCA 1989b] *BFE Interface Control Document, BLACKER Program Office, U.S. Defense Communications Agency*, 21 March 1989.

[DCA 1989c] Briefing to the U.S. Postcoordination Meeting for TSGCEE SG9 on *Defense Message System*, DCA, 21 March 1989.

[DCA 1990] Briefing on BLACKER, INCA Project Office, U.S. Defense Communications Agency, May 1990.

[Deutch 1987] *Database Management System Standards, Report of Past Progress and Future Prospects*, Donald R. Deutch, G.E. *Information Services, U.S. National Institute of Standards and Technology Symposium*, 3 December 1987.

[Dibble 1990] *U.K. Defence Packet Switched Network (DPSN)*, Alan Dibble, DSLC, and John Laws, RSRE, U.K. MOD, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[DIS 8824 1986] *Information Processing Systems - Open Systems Interconnection, Specification of Abstract Syntax Notation One* (ASN.1), ISO/DIS 8824, 1986.

[DIS 8825 1986] *Information Processing Systems - Open Systems Interconnection, Specification of Basic Encoding Rules for Abstract Syntax Notation One* (ASN.1), ISO/DIS 8825, 1986.

[DISA 1990] *X12/DISA Information Manual, Data Interchange Standards Association (DISA), Incorporated (ANSI X12 Secretariat)*, Spring 1990.

[DISA 1991] *Defense Message System Required Operational Messaging Characteristics*, Draft, DISA, 1 November 1991, UNCLASSIFIED.

[DISC 1988] *Army Data Management and Standards Program*, AR-25-9, Office of the Secretary of the Army, DISC4, July 1988.

[DISSP 1991] *Defense-Wide Information Systems Security Program (DISSP)*, Presentation to the JTC3A Architecture Review, National Security Agency (Dave Stephan), 19 September 1991, UNCLASSIFIED.

[DMA c1990] *DMA Standardization*, Defense Mapping Agency, Data Information Sheet, n.d.

[DoD 1976] Department of Defense. 1976. *Development and Use of Non-Government Specifications and Standards*, Department of Defense Instruction 4120.20.

[Dowling 1988] *"Second PCTE+ International Review,"* E. J. Dowling, Ada User, Volume 9, No. 3, 1988.

[DSPO 1991] DoD Memorandum on Coordination of Proposed Revisions A to MIL-D-28000, *Digital Representation for Communication of Product Data: IGES Application Subsets; and MIL-D-28003, Digital Representation for Communication of Illustration Data: CGM Application Profile*, DoD Defense Systems and Programs Office, Alexandria, VA, April 4, 1991.

[ECMA 1985] *ECMA-DB Remote Database Access Service and Protocol*, Final Draft, European Computer Manufacturers Association, 1985.

[ECMA 1987] *Framework for OSI Management*, TR/37, European Computer Manufacturers Association, January 1987.

[ECMA 1988] *Security in Open Systems--A Security Framework*, ECMA TR/46, European Computer Manufacturers Association, July 1988.

[Edelstein et al.] *"Internationalizing Software Engineering Standards,"* D. Vera 1991] Edelstein, Roger Fujii, Craig Guerdat, and Pasquale Sullo, in IEEE Computer, March 1991, pp. 74 - 78.

[EWOS 1990] EWOS/EG FT, *File Transfer Access and Management - FTAM Remote Actions (RA), Service and Protocol*, EWOS/ETG003, January 1990.

[EWOS 1990a] Draft Functional Profile A/3311, Common Facilities--MTA to MTA, Working Draft on the Message Handling System, Version 9.2, *European Workshop for Open Systems (EWOS)*, May 1990.

[EWOS 1991] *Draft Taxonomy for Distributed Transaction Processing*, EWOS/EGTP/91/12; EWOS/TA/91/14, 13 February 1991, DRAFT.

[Favreau et al. 1990] *The U.S. GOSIP Testing Program*, by Jean-Philippe Favreau, Kevin L. Mills, and J. Stephen Nightingale, NIST, 31 July 1990.

[Fisher 1991] *APP Update*, presented by Gary E. Fisher, APP/OSE *Users' Forum*, NIST, 9 May 1991.

[Ford 1987] *Quadrilateral Mapping Schema, Maneuver Control System, CSD-TR2529*, Ford Aerospace & Communications Company for U.S. Army Communications-Electronics Command, 25 September 1987.

[Fox 1991] *"Standards and the Emergence of Digital Multimedia Systems"* by Edward A. Fox, in Communications of the ACM, Volume 34, No. 4, April 1991, pp. 26-29.

[France 1989] *Commentaries on the STANAGs of WG1*, Contribution by France to TSGCE SG9/WG1, February 1989, NATO UNCLASSIFIED.

[Freeman 1991] *Personal Communication* what Murray Freeman, Secretary of X3T2, 12 June 1991, (908) 699-2272.

[G-LOTOS 1988] G-LOTOS: *A Graphical Syntax for LOTOS*, Attachment to SC21 N 3253, December 1988.

[Galitzer 1991] *Measuring GOSIP's Appropriateness for the Tactical User*, Briefing, S. Galitzer, MITRE, 10 April 1991, UNCLASSIFIED.

[Gallagher 1988] Discussions with Lynn Gallagher, Institute for Computer Sciences and Technology, U.S. National Institute of Standards and Technology, Gaithersburg, MD, 24 May 1988.

[Gallagher 1990] *SQL3 Support for CALS Applications*, by Leonard Gallagher, NIST, 21 December 1990.

[Gallagher 1991] Memo to SC21 TAG from Leonard Gallagher Regarding ISO/IEC Projects on SQL and RDA Actions Taken at May/June 1991 SC21/WG3 Meetings in Arles, France.

[Gallagher 1991a] *Database Management Standards: Status and Applicability*, Leonard Gallagher, NIST, 11 July 1991.

[GAM 1987] *Military Real Time Local Area Network*, GAM-T-103, Ministre de la Defense, Republique Francaise, 9 February 1987.

[Gambrel 1991] "Profiles," presented by B. Gambrel, UNISYS, at the *8th APP/OSE Workshop*, NIST, Gaithersburg, MD, 12 November 1991.

[Gee 1991] *Report of the U.S. Representative (Sherman Gee) on SG9/WG3*, 18 October 1991, UNCLASSIFIED.

[Goldfine et al.] *A Technical Overview of the Information Resource Dictionary*, 1988] NBSIR 86-3700, Alan Goldfine and Patricia Konig, U.S. National Institute of Standards and Technology, January 1988.

[Goldfine 1991] *Personal communication with Alan Goldfine*, NIST, 18 April 1991.

[GOSIP 1988] *Government Open Systems Interconnection Profile (GOSIP)*, FIPS 146,Version 1, U.S. National Institute of Standards and Technology, 15 August 1988.

[GOSIP 1990] *U.S. Government Open Systems Interconnection Profile (GOSIP)*, Version 2.0, Federal Information Processing Standard (FIPS) 146-1, October 1990, DRAFT.

[Greco 1988] *"Windowing Systems Overview,"* F. D. Greco, Program Journal, Volume 6, No. 4, July-August 1988.

[Gutman 1990] Report on the SG/9 AHWG-OSI Management Meeting Held in San Diego During 5-9 February 1990, U.S. Representative (Lew Gutman), 13 February 1990.

[Hall 1991] *Conformance Testing for FIPS 151-1 (POSIX)*, presented at the 7th OSE/APP Users' Forum, May 9, 1991 by James Hall at NIST, Gaithersburg, MD.

[Haber 1991] *"New Image Buzzwords: JPEG and JBIG,"* by Lynn Haber, in Network World, Volume 8, No. 7, February 18, 1991, pp. 41 and 55.

[Hankinson 1988] *Briefing on Applications Software Portability*, Allen L. Hankinson, Institute for Computer Sciences and Technology, U.S. National Institute of Standards and Technology, Gaithersburg, MD, 1988.

[Hankinson 1991] *APP Update*, presented by Al Hankinson, NIST, at the APP/OSE Users' Forum, NIST, 9 May 1991, Gaithersburg, MD.

[Harris 1991] *Software Product Specification for the DoD Connectionless-Mode Network Protocol*, Final Draft, Robert T. Harris, SPARTA, Inc., for the Defense Communications Engineering Center of the Defense Information Systems Agency, 11 March 1991, UNCLASSIFIED.

[Howe 1991] *Report of AC/302 Tri-Service Group on Communications and Electronic Equipment (TSGCE) Meeting of 16-17 September 1991*, U.S. Representative to TSGCE (Mr. Howe), 7 October 1991, NATO UNCLASSIFIED.

[Humphreys 1991] *Security Features in International Standardized Profiles (ISPs)*, Discussion Document by E.J. Humphreys, Chair of IST33, 31 January 1991, distributed as IST/21 N 2652, 14 March 1991.

[IDA 1991] *A Preliminary Description of a Target Architecture for Generic Command and Control Information Systems*, Institute for Defense Analysis Paper P-2490, 7 February 1991, DRAFT.

[IEEE 1983] *Software Engineering Standards, Institute of Electrical and Electronics Engineers, Third Edition*, 1983, Second Printing October 1989.

[IEEE 1991] "IEEE TCOS Standards Status," *POSIX Tracking Report*, Volume 3, Issue 3, July 1991, p. 3.

[IGES 1986] *Initial Graphics Exchange Specification, Version 3.0*, ANSI DP ANS Y14.26M, 1986.

[IMA 1991] *The Army Long Range Plan for the Information Mission Area (IMA)*, Office of the Director of Information Systems for Command, Control, Communications and Computers, 11 January 1991.

[INI 1987] *The MAP Book: An Introduction to Industrial Networking*, Industrial Networking Incorporated, 1987.

[ISO 4646-2 1987] *The Tree and Tabular Combined Notation*, Annex E, ISO 4646-2, December 1987.

[ISO 9545/PDAM 1] *Information Technology - Open Systems Inte· nection* - 1991] *Application Layer Structure - Proposed Draft Amendmen : Extended Application Layer Structure*, ISO/IEC 9545/PDAM 1, 15 April 1991.

[IST/21 1534 1988] Project Description for Project JTC1.21.30.2, *Technical Report--Tutorial for Reference Model of Data Management*, IST/21 1534 (WG3 N 572), SC21/WG3, March 1988.

[IST/21:1721 1989] Notes on IST21 Ad Hoc Meeting on Distributed Applications, IST/21:1721, British Standards Institute IST21, 25 July 1989.

[IST/21:1868 1989] Functional Standards for the X.500 Directory, IST/21:1868, IST21/4/DIR, British Standards Institute, 4 October 1989.

[IST/21:2041 1990] Report of Joint ISO/IEC JTC1 SC21/WG4 and CCITT SG VIII(Q20) Meeting on Enhancements to the Directory, Geneva, February 5th to 14th 1990, IST/21:2041, British Standards Institute IST21, 19 March 1990.

[IST/21:2160, 1990] Report on SC21 Plenary, Held in Seoul, 5-6 June 1990, IST/21:2160, July 1990.

[IST/21:2170 1990] JTC1 Workshop on Security, London, 5-7 November 1990, IST/21:2170, British Standards Institute IST21, 29 June 1990.

[IST/21: 2499 1991] Report on the Anaheim IRDS Meetings, IST/21: 2499, 18 January 1991.

[IST/21: 2525 1991] IST/21 Project File: January 1991, 30 January 1991.

[IST/21: 2852 1991] *POSIX Security Call for New Work Items*, SC22/WG15, IST/21:2852, June 1991.

[ISWG 1991] *NATO Data Management Policy*, Working Paper, AC/317(WG/2)WP/67, ISWG, 28 August 1991, NATO UNCLASSIFIED.

[ITSEC 1990] *Information Technology Security Evaluation Criteria (ITSEC)--Harmonised Criteria of France, Germany, The Netherlands, and the United Kingdom*, Draft, Version 1, 2 May 1990.

[ITSTC 1989] *Study and Investigation Mandate for OSI Conformance Testing Methodology*, ITSTC N 1048, CEN/CENELEC Information Technology Steering Committee, 28 July 1989.

[J6J 1991] *Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior*, Draft, Joint Staff J6J, 17 October 1991, UNCLASSIFIED.

[JTAP 1991] TSG-1 Final Report, JTC1 TAG/Applications Portability Study Group (JTAP), 1 March 1991, DRAFT.

[JTC1 N 1161 1991] Report of the Meeting of the Ad Hoc Technical Study Group on Multimedia and Hypermedia held 12-14 December 1990, New York, NY, ISO/IEC JTC1 N 1161, 8 January 1991.

[JTC1 N 1485 1991] *Final Disposition of Proposal for a New Work Item on RDA Support for Stored SBL Statements*, JTC1 N 1485, 16 August 1991.

[Keane 1991] *CIM Terminology*, Private communication from Mr. John Keane, U.S. DoD CIM Standards Office, CIM/XI, 16 July 1991, UNCLASSIFIED.

[Kemp 1990] Facsimile communication from Alstair Kemp, IEE, London, 10 July 1990.

[Kennedy et al. 1989] *"Management Requirements Arising from a NATO Study of Quality of Service,"* Paul Kennedy, Chris Sluman, and Peter Pranschke, *Integrated Network Management*, B. Meandzija and J. Westcott (Editors), Elsevier Science Publishers B.V., The Netherlands, 1989 (pp 133-140).

[Kenworthy 1991] Personal communication with William Kenworthy, Chair ANSI X3L8, (703) 693-8174, 16 May 1991.

[Kernighan et al.] *The C Programming Language*, Brian W. Kernighan and Dennis 1988] M. Ritchie, Second Edition, Prentice Hall, 1988.

[Kirk 1990] *Time Critical Communication Architecture: A Current Work Item Within Industrial Automation Systems (TC184) of ISO*, M. Kirk, *ERA Technology Limited, U.K., Military OSI Symposium Proceedings*, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[Konoike 1987] *"The Architecture of an Interoperable Database System Based on the OSI/RDA,"* Mitsuo Konoike, et al., Technical Committee 1, INTAP, *International Symposium on Interoperable Information Systems*, 25-27 February 1987.

[Kornfeld 1990] *"Strengthening the U.S. Standards Voice,"* by Marilyn Kornfeld, in *Computer Standards and Interfaces, Volume 11, No. 2*, 1990, p. 134.

[Krick 1991] *Submission of STANAG 4406 (Military Message Handling Systems) for Approval and Ratification*, DS(CCC-ICP)(91)710, Chairman WG2 (M. Krick), 10 December 1991, NATO UNCLASSIFIED.

[Krick 1991a] *MMHS AHWG Chairman's Report to WG2*, Review Draft, 30 September 1991, NATO UNCLASSIFIED.

[Kuhn 1990] *"Briefing on X Window System Standards Update,"* D. Richard Kuhn, presented at the *Applications Portability Profile and Open Systems Environment Users Forum*, U.S. National Institute of Standards and Technology (NIST), Gaithersburg, MD, 9 May 1990.

[Kuhn 1991] "The X Window System Standards Update," Richard Kuhn, NIST, presented at the *8th APP/OSE Workshop*, NIST, Gaithersburg, MD, 12 November 1991.

[Lambert 1987] X/OPEN *On-Line Transaction Processing Reference Model*, Discussion Paper, M. G. Lambert, ICL, United Kingdom, July 1987.

[Landberg 1991] "OSE Implementor's Workshop," Presentation by Ted Landberg, NIST, at the *8th APP/OSE Workshop*, NIST, Gaithersburg, MD, 12 November 1991.

[Lang et al. 1989] *SIMNET Database Interchange Specification*, P. Wever, E. Lang, and C.S. Smyth, *BBN Systems and Technologies Corporation and Spatial Data Research, Inc.*, BBN DARPA Report 7108, July 1989.

[Lang et al. 1990] *"A Universal Data Exchange System,"* Pete Wever and Eric Lang, BBN Systems and Technologies Corporation, and C. Stephen Smyth, Spatial Data Research, Inc., Geo'89 *Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Langsford 1989] *Open Distributed Management Standards--The OSI Management Approach*, A. Langsford, Working Paper, July 1989.

[LeGall 1991] *"MPEG: A Video Compression Standard for Multimedia Applications,,"* by Didier Le Gall, in *Communications of the ACM, Volume 34, No. 4*, April 1991, pp. 47-58.

[Liou 1991] *"Overview of the px 64 Kbit/s Video Coding Standard,"* by Ming L. Liou, in *Communications of the ACM, Volume 34, No. 4*, April 1991, pp. 60-63.

[LLC 1988] *Optional LLC Security Sublayer*, Draft Proposed Addendum to IEEE 802.2 Logical Link Control, P802.2-88/95, Third Draft, IEEE, November 1988.

[Maes 1991] *MIDS Programmers/Implementation Plans and Interoperability Requirements--NACMA Report of Activities*, NACMA(91), Guy Maes, NACMA/PID, 5 November 1991, NATO UNCLASSIFIED.

[McArthur 1991] *Analysis of X.400 Overhead*, L. McArthur and Lt K. Bryant (USN), JTC3A, 20 April 1991, UNCLASSIFIED.

[McCartney 1987] *"Xcellence in Windows: Advantages of a Standard,"* I. McCartney, *Mini-Micro Systems, Volume 20, No. 7*, July 1987.

[McDermott 1991] *The Spatial Data Transfer Standard*, by Matthew H. McDermott, *U.S. Geological Survey*, 510 National Center, Reston, VA 22092 [paper to be presented at the American Congress of Surveying and Mapping's 1991 Annual Convention].

[McKellar 1990] *"An Architecture for the Exchange of Geographic Data,"* David G. McKellar, Directorate of Cartography, National Defence Headquarters, Ottawa, Canada, Geo'89 Symposium on *Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, *Symposium Proceedings 6, Volume 1* (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Man 1990] *Telecommunication Management Network*, Working Document Prepared for the TSGCEE SG9 AHWG on OSI Management, Man 0290/06, February 1990.

[Manno 1989] Private communication with Salvatore J. Manno, Assistant Director for International Affairs, JTC3A, 24 October 1989.

[Manno 1991] Private communication with Sal Manno (U.S. Representative to PG6), JTC3A, 9 December 1991.

[Manno 1991a] *Report of the Tri-Service Group on Communications and Electronics (TSGCE), Subgroup on Communications, AC/302(SG/11) Meeting on 13-14 November 1991*, U.S. Representative to SG11 (Sal Manno), 29 November 1991, NATO UNCLASSIFIED.

[Manvos 1989] The X.400 Blue Book Comparison, Carl-Uno Manvos, Technology Appraisals, London, 1989.

[Marine 1987] *Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP), Volume V*, Protocol Standard, Headquarters, U.S. Marine Corps, July 1987.

[Martin 1989] *Briefing on the Applications Portability Profile*, Roger J. Martin, *U.S. National Institute of Standards and Technology*, 16 May 1989.

[Martin 1990] *Briefing on POSIX and Applications Portability*, Roger J. Martin, Institute for Computer Sciences and Technology, *U.S. National Institute of Standards and Technology*, March 1990.

[Martin 1991] *NIST Update*, provided by Roger Martin at the 13th JTAP Meeting, CBEMA, 8 April 1991.

[Martin 1991a] *Applications Portability and Open Systems Environments: Status Report*, presented by Roger J. Martin at APP/OSE *Users' Forum*, NIST, 9 May 1991.

[Matthews 1990] *"The Demand for Digital Geographic Products*, Brigadier A. E. Matthews, Military Survey, U.K. MoD, Geo'89 *Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[MDLA 1990] *Media Independent Data Link Architecture*, ADSIA-RCA-C-106-90, 28 May 1990, NATO UNCLASSIFIED.

[Mehta 1990] *"User Interfaces and the IEEE P1201 Committee (Standards Report),"* Sunil Mehta, UNIX Review, Volume 8, Issue 1 pp. 14-17, January 1990.

[Messeh 1991] *ISO/CCITT Collaborative Meeting on the Directory in Berlin from 21 October to 1 November 1991*, Ltr to Maj William Campbell, DISA/DEC, from Adel Messeh, National Telecommunications and Data Systems, 12 November 1991.

[Messing et al. 1990] *Performance of a Tactical Application Prototype Using GOSIP, Version 1*, by Judy Messing, Shari Galitzer, and Calvin Lin, The MITRE Corporation, MTR-90W00209, December 1990.

[Mills 1991] *Defense Standardized Profiles (DSPs)*, ltr from NIST (Kevin Mills, Computer Systems Laboratory), to the DTMP, 30 July 1991.

[MITRE 1988] *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy*, The Mitre Corporation for the Defense Communications Engineering Center, May 1988.

[MITRE 1990] *Comments on the Applicability of Asynchronous Transfer Mode (ATM) to the Tactical Environment in the Year 2000 and Beyond*, MITRE, August 1990, UNCLASSIFIED.

[MITRE 1991] *DMS OSI Transition Plan*, Draft, Prepared for DISA by MITRE, 30 April 1991, UNCLASSIFIED.

[MMHS 1990] *Intercept Profile for the Military Message Handling System (MMHS), Issue 2*, March 1990, NATO UNCLASSIFIED.

[MoD 1989] *Scope for MOD Information Technology (IT) Standardization and Responsibilities*, U.K. MOD Information Technology Standards Board, 11 August 1989.

[MODITSB 1989] *Scope for MOD IT Standardization and Responsibilities, MOD Information Technology Standards Board Executive Committee Technical Group*, MODITSB 3/89, 11 August 1989.

[Montgomery et al.] *GEMINI: Government Expert Systems Methodology Initiative*, 1989] T.A. Montgomery and E. Crispin, Fifth International Expert Systems Conference, London, 6-8 June 1989, pp. 45-54.

[MROC 3-88 1989] *Implementation of Multicommand Required Operational Capability (MROC) 3-88, The Defense Mapping System (DMS)*, Director for C3 Systems, Joint Staff, 6 February 1989, UNCLASSIFIED.

[MTS TIDP 1987] *Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP)*, Volume V, Protocol Standard, Headquarters, U.S. Marine Corps, July 1987, UNCLASSIFIED.

[NACISA1988] *Standard Automated Message Interface for NATO ACCIS (STAMINA), Version 3.0 with Amendment List 1*, NACISA/ISD/CCISPT(88)394E, NACISA, 17 November 1988, NATO UNCLASSIFIED.

[NACISA 1989] *NATO C3 Architecture (U), Volume 1, Consolidated Architecture*, NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989a] *NATO C3 Architecture (U), Volume 2, Headquarters and Facilities Subsystem*, NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989b] *NATO C3 Architecture (U), Volume 3, Information System Subsystem*, NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989c] *NATO C3 Architecture (U), Volume 4, Communications Subsystem*, NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989d] *NATO C3 Architecture (U), Volume 5, Sensor and Warning Installations Subsystem*, NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1990] *Statement to TSGCEE SG/9 on STAMINA and Related Activities*, NACISA, May 1990, NATO UNCLASSIFIED.

[NACISC 1989] *NATO Consultation, Command and Control (C3) Master Plan (U), Edition 1*, AC/317-WP-66 (J-1800/77/5), *Information Systems Working Group (ISWG) and Communications Systems Working Group (CSWG) of the NATO Communications and Information Systems Committee (NACISC)*, July 1989, NATO CONFIDENTIAL.

[NACISC 1989a] *TRI-Major NATO Commanders' Command and Control (C2) Plan (U), 2300.12.5/SHORC/89, Edition 4*, ISWG and CSWG of the NACISC, 20 July 1989, NATO SECRET.

[NACISC 1989b] *Political Consultation and NATO Civil Emergency Planning* (PCNCEP) CIS Plan (U), Edition 1, AC/317(WG/1)WP/36 (Revised) and AC/317(WG/2)WP/51 (Revised) (J-1800/77/6), ISWG and CSWG of the NACISC, 18 July 1989, NATO CONFIDENTIAL.

[NACISC 1990] *Data Management*, AC/317(WG/2)WP/60, NACISC, 5 June 1990.

[NATO 1987] *Issues Within the NATO Military Data Communications Internetwork*, Draft Working Paper, TSGCEE SG9, 1 September 1987, NATO UNCLASSIFIED.

[NATO 1987a] *NATO Naval Intra-Ship Tactical control and Data Handling Open Systems Interconnection, Network Independent Interface, Transport Service Definition for Connection-Mode Transmission*, Proposed Draft STANAG, 16 September 1987, NATO UNCLASSIFIED.

[NATO 1991] *NATO Technical Interface Standards (NTIS) Transition Strategy, Sixth Edition*, AC/259-D/1218(Revised), *Conference of National Armaments Directors* (CNAD), *Tri-Service Group on Communications and Electronic Equipment* (TSGCEE), NATO, Brussels, 11 November 1991, NATO UNCLASSIFIED.

[NATO 1989a] *NATO Network Security Information Classification Guide (NU), Version 1.0*, TSGCEE SG9, February 1989, NATO RESTRICTED.

[NATO 1990] *Proceedings of the Military OSI Symposium, Volume 3*, June 1990, NATO SECRET.

[NATO 1990a] U.K. MOD Contribution to TSGCEE SG9/WG1, 23 July 1990, NATO UNCLASSIFIED.

[NATO MC 1987] *Memorandum ISM-UAK-7, NATO Military Committee*, 12 January 1987.

[NATO Naval 1987] *NATO Naval Intra-Ship Tactical Control and Data Handling Open Systems Interconnection, Network Independent Interface, Transport Service Definition for Connection-Mode Transmission*, Proposed Draft STANAG, 16 September 1987, NATO UNCLASSIFIED.

[Neve 1990] *Private communication with Nick Neve*, RSRE, U.K. MOD, 22 March 1990.

[Newcomb c1991] *The Hypermedia/Time-based Document Structuring Language "HyTime,"* by Steven R. Newcomb, Neill A. Kipp, and Victoria T. Newcomb, n.d.

[NIAG 1989] *Programme of Work 1990-1992, Issue 1*, NIAG SG/6 on the Compatibility of Naval Data Handling Equipment, December 1989, NATO UNCLASSIFIED.

[Nieporent et al.] *Use of OSI Protocols for U.S. Army Tactical Command and Control* 1990] Applications, Richard Nieporent and Brajesh Mishra, The Mitre Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[NIIF 1989] Briefing on NACISA Interface Initiative (NIIF) to TSGCEE SG/9 WG/1, June 1989, NATO UNCLASSIFIED.

[NIMP 1988] *NATO Interoperability Management Plan (NIMP)*, Third Endorsement Edition, ADSIA-RCU-D/1 (Revised), Allied Data Systems Interoperability Agency, 1 July 1988 NATO UNCLASSIFIED.

[NIST 1987] *Guide on Data Entity Naming Conventions*, NIST SP 500-149, U.S. National Institute of Standards and Technology, October 1987.

[NIST 1988] *Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 2, Edition 1*, NIST Special Publication 500-16, U.S. National Institute of Standards and Technology, December 1988.

[NIST 1989] *Ongoing Implementation Agreements for Open Systems Interconnection Protocols*: Continuing Agreements, NISTIR 88-3824-2, National Institute of Standards and Technology, February 1989.

[NIST 1990] *Open Systems Standards*: A Federal Strategy, U.S. National Institute for Standards and Technology, Undated (Provide to IDA on 30 April 1990).

[NIST 1990a] 132. Briefing on POSIX, U.S. National Institute of Standards and Technology, 12 June 1990.

[NIST 1990b] *Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 3, Edition 1*, NIST Special Publication 500-177, National Institute of Standards and Technology, March 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop; basis for U.S. GOSIP 2.0).

[NIST 1990c] *Working Agreements. Working Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements, Volume 2, No. 2*, NISTIR 90-4247, National Institute of Standards and Technology, February 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop).

[NMICC 1989] *NATO Maritime Interface Coordination Center Support and Capability* (NMICC) *Project Data and Justification* (U), NATO Common Funded Infrastructure, Third Revision, January 1989, NATO CONFIDENTIAL.

[Nolan 1990] *CASE Integrations Services: Technical Description*, by Chris J. Nolan, CIS 90-008, 31 March 1990.

[NOSA 1988] *NATO OSI Security Architecture* (NOSA), Ad Hoc Working Group on Security, TSGCEE SG9, Draft Version 2.1, March 1988, NATO UNCLASSIFIED.

[NSA 1989] *Secure Data Network System* (SDNS) *Security Protocol 3* (SP3), Specification SDN.301, Revision 1.5, SDNS *Protocol and Signalling Working Group*, 15 May 1989, National Security Agency.

[NSA 1989a] *Secure Data Network System* (SDNS) Security Protocol 4 (SP4), Specification SDN.401, Revision 1.3, SDNS *Protocol and Signalling Working Group*, 2 May 1989, National Security Agency.

[NSA 1989b] *Secure Data Network System* (SDNS) *Key Management Profile, Communication Protocol Requirements for Support of the SDNS Key Management Protocol*, Specification SDN.601, Revision 1.5, SDNS Protocol and Signalling Working Group, 11 August 1989, National Security Agency.

[NSA 1989c] *Secure Data Network System* (SDNS) Message Security Protocol (MSP), Specification SDN.701, Revision 1.5, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989d] *Secure Data Network System* (SDNS) *Directory Specifications for Utilization with the SDNS Message Security Protocol* (MSP), Specification SDN.702, Revision 1.4, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989e] *Secure Data Network System* (SDNS) *Access Control Concept Document*, Specification SDN.801, Revision 1.3, SDNS Protocol and Signalling Working Group, 26 July 1989, National Security Agency.

[NSA 1989f] *Secure Data Network System* (SDNS) Access Control Specification, Specification SDN.802, Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency.

[NSA 1989g] *Secure Data Network System* (SDNS) *Access Control Specification, Addendum 1, Access Control Information Specification* (ACIS), Specification SDN.802/1, Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency.

[NSA 1989h] *Secure Data Network System* (SDNS) *Key Management Protocol, Definition of Services Provided by the Key Management Application Service Element* (KMASE), Specification SDN.902, Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989i] *Secure Data Network System* (SDNS) *Key Management Protocol, Specification of the Protocol for Services Provided by the Key Management Application Service Element* (KMASE), Specification SDN.903, Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989j] *Secure Data Network System (SDNS) Key Management Protocol, SDNS Traffic Key Attribute Negotiation*, Specification SDN.906, Revision 1.3b, SDNS Protocol and Signalling Working Group, 18 September 1989, National Security Agency.

[NST 1988]NATO *Staff Target (NST) for the Battlefield Information Collection and Exploitation Systems* (U), AC/302-D/560, AC/302(PG/7)D/20 (Revised), 28 December 1988, NATO CONFIDENTIAL.

[Oldenburg 1989] *"OSF Motif, the User Interface Standard,"* H. Oldenburg, IEEE Colloquium on User Interface Management Systems, Digest, No. 135, Issue 2, IEEE, 17 November 1989.

[Onufer 1990] *Functional Profiles for Open Systems Interconnection*, Joseph R. Onufer, TSGCEE SG9 WG1, U.S. Army CECOM ISD, Military OSI Symposium, Symposium Proceedings SP-8, Volume 1, 5-8 June 1990.

[Onufer 1991] *Report of the U.S. Representative (Joe Onufer) of the Ad Hoc Meeting on the NATO Open Systems Interoperability Plan (NOSIP), 25 to 27 September 1991*, 16 October 1991, UNCLASSIFIED.

[Onufer 1991a] *Report to SG9 by the Chairman of WG1 on Layers 1-4*, Joe Onufer, 10 December 1991, NATO UNCLASSIFIED.

[Onufer 1991b] *WG11 Statement on the Future of Layer STANAGs and Future Terms of Reference*, TSGCE SG9/WG1, October 1991, NATO UNCLASSIFIED.

[Onufer 1991c] *Response to WG1 AI910521 Relating to the WG1 TOR and 18-Month Work Plan*, Chairman (Joe Onufer) WG1, 27 June 1991, NATO UNCLASSIFIED.

[Onufer 1991d] *Chairman's Report of the May 1991 WG1 Meeting*, Chairman (Joe Onufer) WG1, 26 August 1991, NATO UNCLASSIFIED.

[Ornstein 1991] *Personal communication with David Ornstein*, 4 April 1991, (408) 988-7575.

[OSF 1990] *Announcement of Technology Selection*, Distributed Computing Environment Request for Technology (RFT), Open Software Foundation, 14 May 1990.

[OSF 1990a] *OSF/Motif: The Graphical User Interface for Open Systems, A White Paper*, OSF, October 1990.

[OSN 1988] *"X.400 1988 and X.500 (The Directory) Make Their Debut,"* OSN: *The Open Systems Newsletter, Volume 2, Issue 8,* Technology Appraisals, Limited, London, October 1988.

[OSN 1988a] *"Open Systems Opening Up,"* OSN: *The Open Systems Newsletter, Volume 2, Issue 9/10,* Technology Appraisals, Limited, London, November/ December 1988.

[OSN 1988b] *"EDI1--CCITT Takes First Steps to X.400 and EDI Convergence,"* OSN: *The Open Systems Newsletter, Volume 2, Issue 7,* Technology Appraisals, Limited, London, September 1988.

[OSN 1989c] OSN: *The Open Systems Newsletter, Volume 3, Issue 1,* January 1989.

[OSN 1989] *"OSITOP Reports on Progress,"* OSN: *The Open Systems Newsletter, Volume 3, Issue 3,* Technology Appraisals, Limited, London, March 1989.

[OSN 1989a] *"Harmonization Between Document Filing and Retrieval (DFR) and FTAM,"* OSN: *The Open Systems Newsletter, Volume 3, Issue 12,* December 1989.

[OSN 1989b] *"The ISO Virtual Terminal Standards,"* OSN: *The Open Systems Newsletter, Volume 3, Issue 4,* Technology Appraisals, Limited, April 1989.

[OSN 1989c] *OSN: The Open Systems Newsletter,* Volume 3, Issue 1 (January 1989).

[OSN 1990] *"OSF Releases OSF/1 Version 1.0,"* OSN: *The Open Systems Newsletter, Product News, Volume 4, Issue 12,* December 1990, p. 18.

[OSN 1990a] *OSN The Open Systems Newsletter, Volume 4 Issue 1/Issue 2,* January/February 1990, pp. 17-18.

[OSN 1990b] *"Towards Routing Standards for OSI Networks"* in OSN *The Open Systems Newsletter, December 1990, Volume 4, Issue 12,* p. 10.

[OSN 1990c] *"What is Next in Distributed Computing?"* in OSN: *The Open Systems Newsletter,* December 1990, Volume 4, Issue 12, p. 3.

[OSN 1990d] *OSN: The Open Systems Newsletter, Volume 4, Issue 3,* March 1990, pp. 14-18.

[OSN 1990e] *OSN: The Open Systems Newsletter, Volume 4, Issue 3,* March 1990, pp. 9-11.

[OSN 1990f] *OSN: The Open Systems Newsletter, Volume 4, Issue 4,* April 1990, p. 4.

[OSN 1990g] *"What is Next in Distributed Computing?"* in OSN: The Open Systems Newsletter, December 1990, Volume 4, Issue 12, pp. 1-5.

[OSN 1990h] OSN: *The Open Systems Newsletter, Volume 4, Issue 4,* April 1990, p. 10.

[OSN 1990j] OSN: *The Open Systems Newsletter, Volume 4, Issue 3,* March 1990, pp. 24-25.

[OSN 1991] *"OSF Announces Qualifying Submitters in DME RFT,"* OSN: *The Open Systems Newsletter, Market Messages, Volume 5, Issue, 1,* January 1991, pp. 20-21.

[OSN 1991a] *"NTT Announces Standards for Multivendor Computer Systems,"* OSN: *The Open Systems Newsletter, Product News, Volume 5, Issue 1,* January 1991, p. 20.

[OSN 1991b] *"Open Document Architecture: The Emerging Market,"* OSN: *The Open Systems Newsletter, Volume 5, Issue 3,* March 1991, pp. 19-23.

[OSN 1991c] *"EWOS Reports on Progress, "* OSN: *The Open Systems Newsletter, Volume 5, Issue 3,* March 1991, pp. 7-10.

[OSN 1991d] *"Open Document Architecture Standard Comes of Age,"* OSN: *The Open Systems Newsletter, Volume 5, Issue 4,* April 1991, pp. 4-8.

[OSN 1991e] *"What is New in U.S. GOSIP - Profile of a Profile,"* OSN: *The Open Systems Newsletter, Volume 5, Issue 1,* January 1991, p. 4.

[OSN 1991g] *"EPHOS: Phase I Agreed as Phase II Begins,"* OSN: *The Open Systems Newsletter, Volume 5, Issue 4,* April 1991, pp. 1-3.

[OSN 1991h] "OSINET Joints COS," OSN: *The Open Systems Newsletter,* Volume 5, Issue 1, January 1991, p. 23.

[OSN 1991i] "GOSIP 4 - The New Version of UK GOSIP now Available," *OSN: The Open Systems Newsletter, Volume 5, Issue 7*, July 1991, pp. 19-20.

[OSN 1991j] "Understanding Open Distributed Processing," in *OSN: The Open Systems Newsletter*, Volume 5, Issue 9, September 1991, pp. 1-18.

[OSN 1991k] "Latest SC18 Work Programme," in *OSN: The Open Systems Newsletter*, Volume 5, Issue 9, September 1991, p. 26.

[OSN 1991m] "GOSIP 4 - The New Version of UK GOSIP Now Available," in *OSN: The Open Systems Newsletter*, Volume 5, Issue 7, July 1991, pp. 19-20.

[OSSTR 1991] "The Standards Reporter," in *Open Systems Standards Tracking Report*, Volume 1, No. 1, October 1991, p. 2.

[Pant 1991] *Packet Multicast Service Definition (X.PMS)*, Draft Version 1.3, R. Pant, Associate Rapporteur on Q1 (Multicast), ANSI X3S3.7/91-73, 4 June 1991, UNCLASSIFIED.

[P1175 1989] *"Proposed Standard Eases Tool Interconnection,"* IEEE Software, November 1989, pp. 69-70.

[P1252 1991] *"Standards Actions of the IEEE Standards Board, March 21, 1991,"* in The IEEE Standards Bearer, Volume 5, No. 1, April 1991, p. 8.

[PC 1989] Private communication with the Chair of the TSGCEE SG9 Ad Hoc Working Group on Security, 21 March 1989.

[PCTE 1989] *"PCTE as a Proposed ISO,"* Computer Systems Europe, January 1989.

[PDTR 10167 1989] *Guidelines for the Application of Estelle*, LOTOS and SDL, PDTR 10167, ISO/IEC JTC1 SC21 (SC21 N 3252), February 1989.

[Perez 1991] *Personal communication with Sandra Perez*, Concept Technology, Inc., (703) 425-9268, 23 April 1991.

[Pilla 1991] *Report of the Tri-Service Group on Communications and Electronics (TSGCE), Subgroup on Communications, AC/302(SG/11) Meeting on 13-14 November 1991*, U.S. Representative to SG11 (Lou Pilla), 29 November 1991, NATO UNCLASSIFIED.

[Pink et al. 1991] *Conformance Testing from the European Point of View*; presented by Jane Pink and Jon Leigh, National Centre for Information Technology at the 7th OSE/APP Users' Forum, May 9, 1991, NIST, Gaithersburg, MD.

[PRC 1988] *Army Implementation of DoD and Federal Standards*, Draft, Prepared for U.S. Army Information Systems Engineering Command by Planning Research Corporation, 8 May 1988.

[Price 1990] *Practical Evaluation of OSI Protocols*, J. Price, D.B. Hearn, J. Laws, A.F. Martin, and J. Staromlynska, RSRE, U.K. MOD, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Price 1991] *"Standard for Data Dictionaries Now Is Mandatory,"* by Douglas S. Price, *Government Computer News, Volume 10 No. 8*, April 15, 1991, p. 60.

[PSSG 1991] Minutes of the Protocol Standards Steering Group (PSSG), 43rd Meeting - 8-9 January 1991.

[PSTP 1991] *Recommendations for DoD Actions to Assure GOSIP Message Handling Systems Suitability for Military Requirements, Protocol Standards Technical Panel (PSTP) Working Group Three (Message Handling Systems)*, Revised, 8 January 1991.

[Purton 1987] Draft Compilation of OSI Standards, M. J. Purton, Unpublished, August 1987.

[Putnam 1982] *Putnam, Hayes, and Bartlett, Inc. 1982. The Impacts of Private Voluntary Standards on Industrial Innovation.* Prepared for National Bureau of Standards, Washington, D.C.

[QIC 1988] *Quadrilateral Tactical Interface Requirement, Version 2*, Quadrilateral Interface Committee, 1 August 1988, UNCLASSIFIED (Limited Distribution).

[QIC 1988a] *Quadrilateral Technical Interface Design Plan, Version A.7*, Quadrilateral Interface Committee, 15 April 1988, UNCLASSIFIED (Limited Distribution).

[QIC 1988b] *Quadrilateral Test and Demonstration Management Plan*, Quadrilateral Interface Committee, 15 April 1988, UNCLASSIFIED (Limited Distribution).

[Rannestad 1991] *Workshop on Conformance Testing*, A. Rannestad, NATO International Staff, DS(CCC-IP)(91)292, 7 June 1991, NATO UNCLASSIFIED.

[Rayner 1987] *"OSI Conformance Testing,"* D. Rayner, *Computer Networks and ISDN Systems, Volume 14*, 1987.

[RDA 1990] Proposed NWI: *RDA Support for Stored DBL Statements*, ISO/IEC JTC1/SC21/WG3 N 1125, RDA SEL 24 (Rev 1), October 1990.

[Reed 1988] Briefing to the 22nd ADSIA Plenary on STAMINA and QTIDP, Annex W to ADSIA-RCX-DS/22, Rex Reed, NACISA, 17-21 October 1988, NATO UNCLASSIFIED.

[Reed et al. 1990] *The STAMINA Specification*, J. R. Reed, S. Goldani, and N. Sanli, NACISA, Proceedings of the Military OSI Symposium, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[Reed et al. 1991] *User-System Software Interface Standards: Issues and Prospects*, Paul Reed and Ken Holdaway, 1991.

[Reichlen 1990] *User Performance of Tactical Networks in the ITDN*, Gladys Reichlen and Allison Mankin, The Mitre Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Reynolds 1987] Assigned Numbers, J. K. Reynolds, Request for Comments (RFC) 1010, DDN Network Information Center, SRI International, May 1987.

[Rigden 1991] *TSGCE SG9 (CSNI) Report of the Chairman (C. Rigden) to SG9*, 2 December 1991, NATO UNCLASSIFIED.

[RM 1989] *Information Processing Systems - Computer Graphics - Reference Model of Computer Graphics*, RM/20, Second Working Draft, 3 February 1989.

[Rose 1990] *The Open Book - A Practical Perspective on OSI*, M. T. Rose, Prentice Hall, Englewood Cliffs, New Jersey, 1990.

[SANISI 1989] *Security Architecture for NATO Information Systems Interconnection (SANISI) (NU), Version 2.0*, Ad Hoc Working Group on Security, TSGCEE SG9, AC/302(SG/9)D/53, 14 April 1989, NATO CONFIDENTIAL.

[Savoye 1991] *Report of the U.S. Representative (Dick Savoye) to the U.S. SG9 Coordination Group*, 29 October 1991, NATO UNCLASSIFIED.

[SC21 N 197 1982] *Concepts and Terminology for the Conceptual Schema and the Information Base*, TC97/SC5 N 695 and SC21 N 197, March 1982.

[SC21 N 236 1985] *Assessment Guideline for Conceptual Schema Language Proposals*, TC97/SC21/WG5-3, SC21 N 236, 31 August 1985.

[SC21 N 1927,1987] *Remote Database Access*, Tutorial, SC21 N 1927, SC21/WG3, 28 July 1987.

[SC21 N 2643 1988] *Remote Database Access*: SQL Specialization, SC21 N 2643, SC21/WG3, 9 May 1988.

[SC21 N 3134 1988] *Revised Report of the SC21 Strategic Planning Meeting*, SC21 N 3134, October 1988.

[SC21 N 3342 1989] *Information Processing Systems - Open Systems Interconnection - Remote Database Access*: SQL Specialization, Service and Protocol, SC21 N 3342, SC21/WG3, 26 January 1989.

[SC21 N 3885 1989] *UN/EDIFACT Information Pack*, SC21 N 3885, 19 September 1989.

[SC21 N 3925 1989] *Liaison Statement to JTC1 SC21 from JTC1 SWG-EDI*, JTC1 SWG-EDI, SC21 N 3925, 19 October 1989.

[SC21 N 3930 1989] *Liaison Statement from JTC1/SC18 to JTC1/SC21/WG5 on Comments on Terminal Management*, SC21 N 3930, SC18/WG4, 19 October 1989.

[SC21 N 3991 1989] *Security Exchange Service Element*, SC21 N 3991, November 1989.

[SC21 N 4002 1989] *Extended Application Layer Structure*, ANSI Contribution to SC21/WG6, SC21 N 4002, 19 October 1989.

[SC21 N 4025 1989] ODP: *Working Document on Topic 8.1*--Draft Basic Reference Model of Open Distributed Processing, SC21 N 4025, 11 December 1989.

[SC21 N 4027 1990] Meeting Minutes of the Florence Working Group Meeting on ODP, SC21/WG7, SC21 N 4027, 11 December 1990.

[SC21 N 4176 1989] *Terminal Management Model*, SC21 N 4176, SC21/WG5, December 1989.

[SC21 N 4184] *Request for National Body Comment on Security Enhancements* November 1989] *to FTAM*, SC21 N 4184, SC21/WG5, November 1989.

[SC21 N 4187 1989] *Issues on Upper Layers Conformance Testing*, SC21 N 4187, November 1989.

[SC21 N 4188 1989] *Response to SC18/WG4 N 1183, Comments on Terminal Management, and SC18/WG3 and CCITT SG VII(Q27) Liaison Statement on Terminal Management*, SC21 N 4188, SC21/WG5, December 1989.

[SC21 N 4189 1989] *Comments on the Integration of X-Windows Into the OSI Environment*, SC21 N 4189, December 1989.

[SC21 N 4192 1989] *Proposed FTAM Document Type to Support CGM*, SC21 N 4192, SC21/WG5, December 1989.

[SC21 N 4195 1990] Draft WG3 Position on Conceptual Schema Question, SC21 N 4195, February 1990.

[SC21 N 4210 1989] *Working Draft on Open Systems Security Frameworks*, SC21 N 4210, December 1989.

[SC21 N 4228 1989] ISO 8807/PDAD1, Graphical Representation of LOTOS (G-LOTOS), SC21 N 4228, December 1989.

[SC21 N 4342 1990] *Liaison Statement from SC18 to SC21/WG5 on Conference Application New Study Item Including RODE*, SC21 N 4342, January 1990.

[SC21 N 4352 1990] Revised Text of 4th DP 9834-1, SC21 N 4352, January 1990.

[SC21 N 4356 1990] *Terms of Reference and Plan of Action for the Reassessment of JTM Full Class*, SC21 N 4356, January 1990.

[SC21 N 4472 1990] *Liaison Statement from JTC1/SC18 to JTC1/SC21 on Changes to ASN.1*, SC21 N 4472, SC18/WG3 (title is in error--changes are for ODA, ISO 8613), 22 February 1990.

[SC21 N 4511 1990] *U.S. Comments on Conceptual Schema*, SC21 N 4511, 15 March 1990.

[SC21 N 4519 1990] *Clarification of ALS Modelling Concepts, Workshop on Distributed Applications*, SC21 N 4519, 18 April 1990.

[SC21 N 4520 1990] *Issues for Consideration by Joint ULA/ODP Meeting*, Seoul, May/June 1990, SC21 N 4520, Workshop on Distributed Applications, 18 April 1990.

[SC21 N 4523 1990] *Modelling of Application Program Interfaces and Remote Procedure Calls*, SC21 N 4523, 2 April 1990.

[SC21 N 4524 1990] *Consideration of the Data Management Component of Application Standards*, SC21 N 4524, Workshop on Distributed Applications, 23 April 1990.

[SC21 N 4526 1990] *Application Layer Security Considerations*, SC21 N 4526, 18 April 1990.

[SC21 N 4546 1990] *Liaison Statement of SC21/WG1 on Update of the OSI Reference Model*, SC21 N 4546, CCITT SG VII, March 1990.

[SC21 N 4559 1990] *Liaison Statement of SC21 on OSI Reference Model Update Effort*, SC21 N 4559, CCITT SG VII, March 1990.

[SC21 N 4565 1990] *Liaison Statement to SC21/WG4/WG7 on Time Synchronization*, SC21 N 4565, CCITT SG VII, March 1990.

[SC21 N 4593 1990] *Metadata Use and Standards for Managing Metadata*, SC21 N 4593, ANSI, 4 April 1990.

[SC21 N 4603 1990] *Position on Reassessment of JTM Full Class Protocol*, AFNOR, SC21 N 4603, March 1990.

[SC21 N 4623 1990] *Extensible Matching Rules* (Revised), SC21 N 4623, Canada, 3 May 1990.

[SC21 N 4641 1990] *U.S. Position on JTM Reassessment*, SC21 N 4641, March 1990.

[SC21 N 4648 1990] *Security and Security Exchange Information*, Canadian contribution to SC21/WG6, SC21 N 4648, 28 February 1990.

[SC21 N4655 1990] *Reassessment of Project 1.21.44, Architectural Semantics for FDTs*, SC21 N 4655, 20 April 1990.

[SC21 N 4681 1990] *User Requirements for Multi-Party Communications (MPC)*, SC21 N 4681, Canada, May 1990.

[SC21 N 4759 1990] *USA Position on the Progression of DIS 10026*, SC21 N 4759, 12 March 1990.

[SC21 N 4767 1990] *U.S. Response to SC21/WG6 N 7889 on Requirements for RPC Interface Definition Notation*, SC21 N 4767, 11 May 1990.

[SC21 N 4799 1990] *Letter for Information on Disposition of EDI Messaging Service (EDIMS) Use of Directory*, SC21 N 4799, 21 May 1990.

[SC21 N 4801 1990] *Liaison Statement to SC21 on Joint Efforts Between SG VII(Q20) and SG I(Q16)*, SC21 N 4801, CCITT SG I(Q.16), 21 May 1990.

[SC21 N 4804 1990] *Proposed DIT Structure Rule Definition*, SC21 N 4804, 10 May 1990.

[SC21 N 4806 1990] *Use of External Data Transfer Systems for Shadow Updates*, SC21 N 4806, 10 May 1990.

[SC21 N 4865] *DIS 10040, Systems Management Overview*, SC21 N 4865, 29 May 1990.

[SC21 N 4901 1990] *Second Working Draft for Amendment 1 to ISO 9545 ALS on Extended Application Layer Structure*, SC21 N 4901, SC21/WG6, June 1990.

[SC21 N 4905 1990] *Request for Comment on Introduction of a New Relationship in ALS*, SC21 N 4905, SC21/WG6, June 1990.

[SC21 N 4909 1990] *Disposition of Ballot Comments in JTC1 N 846 on the Proposal for a NWI-- Extension to ISO 9545 ALS for Multi-Level Structures*, SC21 N 4909, SC21/WG6, June 1990.

[SC21 N 4910 1990] *Disposition of Ballot Comments in JTC1 N 764 on the Proposal for a NWI-- Extension to ISO 9545 ALS for Application Layer Recovery Model*, SC21 N 4910, SC21/WG6, June 1990.

[SC21 N 4911 1990] *Modelling for Communications Aspects of Distributed Applications*, SC21 N 4911, SC21/WG6, May 1990.

[SC21 N 4912 1990] *Disposition of Ballot Comments in JTC1 N 766 on the Proposal for a NWI-- Management Information for the OSI Upper Layers*, SC21 N 4912, SC21/WG6, June 1990.

[SC21 N 4926 1990] Liaison to CCITT SG VII(Q19) on OSI RPC, SC21 N 4926, SC21/WG6, June 1990.

[SC21 N 4928 1990] *Remote Call Procedure Definitions and Requirements*, SC21 N 4928, SC21/WG6, June 1990

[SC21 N 4970 1990] *Systems Management Tutorial - Annex A: Access Control*, SC21 N 4970, 30 May 1990.

[SC21 N 4975 1990] *A General Model for Relationship Management*, SC21 N 4975, SC21/WG4, 31 May 1990.

[SC21 N 5002 1990] *Commencement of Work on Security ASEs*, SC21 N 5002, SC21/WG6, 31 May 1990.

[SC21 N 5011 1990] *Modelling Recovery in the Application Layer*, SC21 N 5011, SC21/WG6, 1 June 1990

[SC21 N 5014 1990] *Liaison Statement to CCITT SG VII (Q.23) on Collaborative Work on OSI Registration*, SC21 N 5014, 6 June 1990.

[SC21 N 5074,1990] *Final Answer to Q1/330.6 on Relay, Routing, and Network Management*, SC21 N 5074, SC21/WG1, May 1990.

[SC21 N 5081 1990] Draft Answer to Q1/61 on Consistency Among ISO Standards Related to the OSI Reference Model, SC21 N 5081, May 1990.

[SC21 N 5082 1990] Call for Contributions on OSI Conformance Issues, SC21 N 5082, SC21/WG1, May 1990.

[SC21 N 5095 1990] *Liaison to SC6 on Revision of the Reference Model*, SC21 N 5095, May 1990.

[SC21 N 5096 1990] *Liaison to CCITT SG VII on Revision of the Reference Model*, SC21 N 5096, June 1990.

[SC21 N 5099 1990] *Liaison Statement to CCITT SG VII(Q.25) on Service Conventions*, SC21 N 5099, SC21/WG1, May 1990.

[SC21 N 5108 1990] *Report of the Conformance Testing Meeting Held in Seoul*, 22-30 May 1990, SC21 N 5108ADD.

[SC21 N 5110 1990] *Call to National Bodies and Liaison Organizations for Contributions on Technical Structure of Quality of Service (QoS) Architecture*, SC21 N 5110, May 1990.

[SC21 N 5140 1990] Proposal for Registration of Q3/001, SC21 N 5140, SC21/WG3, 19 June 1990.

[SC21 N 5141 1990] Proposal for Registration of Q3/002, SC21 N 5141, SC21/WG3, 19 June 1990.

[SC21 N 5146 1990] Proposal for Registration of Q3/007, SC21 N 5146, SC21/WG3, 19 June 1990.

[SC21 N 5171 1990] *OSI TP Association Management--Statement of Requirements*, SC21 N 5171, SC21/WG5, June 1990.

[SC21 N 5172 1990] Combined Use of RPC and OSI TP, SC21 N 5172, SC21/WG5 and SC21/WG6, June 1990.

[SC21 N 5176 1990] OSI TP Security, New Work Item, SC21 N 5176, SC21/WG5, June 1990.

[SC21 N 5177 1990] OSI TP Association Management--Revised New Work Item, SC21 N 5177, SC21/WG5, June 1990.

[SC21 N 5183 1990] Unstructured Data Transfer (UDT) for OSI Transaction Processing, SC21 N 5183, SC21/WG5, May 1990.

[SC21 N 5184 1990] Queued Data Transfer for TP, SC21 N 5184, SC21/WG5, May 1990.

[SC21 N 5448 1990] *Outline Working Draft for Part 1 of Generic Security Exchange ASE Definition*, SC21 N 5448, 30 October 1990.

[SC21 N 5501 1990] Working Draft of Revised ISO 7498-1 Clauses 7.1 - 7.3, SC21 N 5501, November 1990.

[SC21 N 5545 1990] *Working Draft Input on Scheduling for Management Functions*, Collaborative OSI Systems Management Meeting, 12-16 November 1990, SC21 N 5545.

[SC21 N 5546 1990] *Agreement on Planning Future Releases of CMIS/P*, Collaborative OSI Systems Management Meeting, 12-16 November 1990, SC21 N 5546.

[SC21 N 5561 1990] *Liaison Statement to ISO/IEC JTC1/SC 21 from ISO/IEC JTC 1/SC18 on Problems with Filters in Distributed Office Applications*, SC21 N 5561, 20 November 1990.

[SC21 N 5564 1991] *Proposal for a New Work Item*: ODP Trader - *A Standard to Define the Role and Function of the Trader in Open Distributed Processing (ODP)*, ISO/IEC JTC1/SC21 N 5564, 3 January 1991.

[SC21 N 5583 1991] Report of the Liaison Meeting with SC22/WG11, Amsterdam, September 1990, SC21 N 5583, 7 January 1991.

[SC21 N 5593 1990] *The Role of the Extended Application Layer Structure in the Standardization of RPC*, ECMA TC 32-TG2, SC21 N 5593, 7 January 1990.

[SC21 N 5602 1991] Proposed Liaison Between ISO TC 184/SC5/WG2 and ISO/IEC JTC1/SC21/WG4, SC21 N 5602, 11 January 1991.

[SC21 N 5603 1990] *Rapporteur's Report of the DIS 100225 (TP) Editing Meeting*, San Francisco, 26 November to 14 December 1990, SC21 N 5603, 11 January 1990.

[SC21 N 5618 1991] *Working Document on ASN.1 - Part 1*: General, SC21 N 5618, 5 February 1991.

[SC21 N 5682 1991] *Contribution from JTC 1/SC 22/WG 11, Binding Techniques for Languages*, ISO/IEC JTC1/SC 21 N 5682, 5 February 1991.

[SC21 N 5757 1991] Work on Security within SC21, SC21 N 5757, March 1991.

[SC21 N 5851 1991] *USA Contribution to SC21 on the Conceptual Schema Topic*, SC21 N 5851, 4 April 1991.

[SC21 N 5933 1991] Conventions for the Definition of OSI Services, DIS 10731, SC21 N 5933, 1991.

[SC21 N 5997 1991] *USA Position on Use of RTSE by SC21 Standards*, SC21 N 5997, 12 June 1991.

[SC21 N 6006 1991] *Proposal for a NWI on the Use of Systems Management for Administration of the Directory*, SC21 N 6006, 1 July 1991.

[SC21 N 6007 1991] *NWI on the Definition of a New FTAM Document Type for Directory*, SC21 N 6007, 2 August 1991.

[SC21 N 6008 1991] *Proposed New Question Q4/4 on Directory Schema Migration*, SC21 N 6008, 29 July 1991.

[SC21 N 6012 1991] *Response to SC21 N 5759, Comment on Directory Implementor's Guide*, SC21 N 6012, May 1991.

[SC21 N 6066 1991] *Collection of Liaison Statements from SC21 to SC21*, SC21 N 6066, 4 December 1991.

[SC21 N 6067 1991] *Request for Comments on Requirements for Management in the Upper Layers of OSI*, SC21 N 6067, 2 July 1991.

[SC21 N 6085 1991] *Revised New Work Item on ODP Trader*, SC21 N 6085, SC21/WG7, 30 May 1991.

[SC21 N 6115 1991] *Consolidated Comments on WD Partial Embedded Abstract Test Suite for the Connection-oriented Presentation Protocol (SC21 N 5903)*, SC21 N 6115, 26 August 1991.

[SC21 N 6130 1991] *Generic Transfer Syntax Providing Upper Layers Security*, SC21 N 6130, 15 July 1991.

[SC21 N 6158 1991] *Final Answer to Q1/62 (Quality of Service (QoS) Architectural Issues)*, SC21 N 6158, 22 July 1991.

[SC21 N 6159 1991] *NP for OSI - Quality -of-Service (QoS) Framework*, SC21 N 6159, 2 August 1991.

[SC21 N 6161 1991] *Proposed New Question Q1/48.6 on LOTOS Enhancements*, SC21 N 6161, 22 July 1991.

[SC21 N 6202 1991] *Multi-Party Testing for Connectionless Relay and Routing Protocols*, SC21 N 6202, 22 July 1991.

[SC21 N 6214 1991] *Disposition of Ballot Comments on Document JTC 1 N 957, Proposal for a NWI on Systems Management Tutorial*, SC21 N 6214, 14 August 1991.

[SC21 N 6215 1991] *Disposition of Ballot Comments on Document JTC1 N 960, Proposal for a NWI on Management Information Register and Registration Procedures*, SC21 N 6215, 14 August 1991.

[SC21 N 6217 1991] Resolutions of the ISO/IEC JTC1/SC 21/WG 5 Meeting, Arles, 23-31 May 1991, SC21 N 6217, 3 July 1991.

[SC21 N 6224 1991] *Proposed EDIFACT/FTAM Document Type*, SC21 N 6224, 3 July 1991.

[SC21 N 6225 1991] *Response to Liaison from JTC1/SC24/WG3 about CGM Document Types*, 3 May 1991, SC21 N 6225, 3 July 1991.

[SC21 N 6227 1991] *Virtual Terminal Support of ODA*, SC21 N 6227, 3 July 1991.

[SC21 N 6228 1991] *Liaison Statement on CCR to WG1 and WG6, FTAM Use of CCR*, SC21 N 6228, 3 July 1991.

[SC21 N 6229 1991] *Request for National Body Contributions on Document Type Registration*, SC21 N 6229, 3 July 1991.

[SC21 N 6230 1991] *On Conformance to Document Types*, SC21 N 6230, 3 July 1991.

[SC21 N 6251 1991] *Proposed New Question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM)*, SC21 N 6251, 23 July 1991.

[SC21 N 6252 1991] *Proposal for a NP: Revision of the IRDS Framework*, SC21 N 6252, 1 July 1991.

[SC21 N 6253 1991] *Proposed New Question on the Approach to Remote IRDS Access*, SC21 N 6253, 23 July 1991.

[SC21 N 6304 1991] *Report of the Editing Meeting for ISO/IEC 9594/PDAM 1: Extended Application Layer Structure*, SC21 N 6304, 26 August 1991.

[SC21 N 6403 1991] *Proposal for a New Work Item: Generic Operating System Interface*, SC21 N 6403, 10 September 1991.

[SC21 N 6423 1991] *Notice of Joint ISO-CCITT Meeting on Q.10/X-P.54, Formal Methods in Conformance Testing*, 18-22 October 1991, The Netherlands, SC21 N 6423, 24 September 1991.

[SC21 N 6449 1991] *Calling Notice for SC21 Special Meeting on Conceptual Schema Facilities and Common Data Modelling Facilities, 9-13 March 1992, Renesse, The Netherlands*, SC21 N 6449, 9 October 1991.

[SC21 N 6532 1991] *Liaison to ISO/IEC JTC1/SC21/WG6 & CCITT SG VII Q19/VII ASN.1 Editing Meeting Concerning Directory's Use of Distinguished Encoding Rules*, SC21 N 6532, 4 December 1991.

[SC21/WG4 1989] Liaison Statements to SC21/WG4, SC21 N 3851-3853, 30 August 1989.

[SC6 N 6219 1990] *Liaison to SC21 on Lower Layer Security*, JTC1/SC6 N 6219, 4 October 1990.

[SC6 N 6976 1991] *Request for SGFS Member Comment on Standardization of Profile Test Specifications*, ISO/IEC JTC1/SGFS, JTC1/SC6 N 6976, 10 September 1991.

[SC6 N 6977 1991] *The Way Ahead: Output Document from June 1991 SGFS Meeting*, ISO/IEC JTC1/SGFS, JTC1/SC6 N 6977, 10 September 1991.

[Schneider 1990] *"Standardization of Digital Geographic Data,"* Jan S. Schneider, Defense Mapping Agency, Geo'89 Symposium on Geographical Information Systems for Command and Control, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Schultz 1990] Report of the TSGCEE Subgroup 9 on Data Processing and Distribution Meeting Held 9-11 May 1990, U.S. Representative (O. Schultz), May 1990, NATO UNCLASSIFIED.

[Schutzer 1987] *Artificial Intelligence: An Applications-Oriented Approach*, Daniel Schutzer, Van Nostrand Reinhold Company, 1987.

[SDIO 1991] *Fixed and Mobile Segment (FMS) Standard*, Prepared by GE Aerospace for SDIO, CDRL A122, 17 December 1990, UNCLASSIFIED.

[SGFS 1989] PAGODA Comments on DTR 10000-2 and Proposed FOD Taxonomy, SGFS N 156, 6 November 1989.

[SGFS N 242 1991] *Five-Year Meeting Schedule for JTC1/SGFS Plenary Meetings*, SGFS N 242.

[SGFS N 282 1991] Resolutions of the 4th RWS-CC Meeting, 18-19 October 1990, SGFS N 282, 17 January 1991.

[SGFS N 293 1991] SGFS Report of the Secretariat, SGFS N 293, January 1991.

[SGFS N 294 1991] Issues List - *Items for Future Developments of ISO/IEC TR 10000-1, TR 10000-2*, and SGFS N 201, SGFS N 230, 7 February 1991; Draft Agenda and Hotel Information for the 7th ISO/IEC JTC1/SGFS Meeting, SGFS N 294, 12 February 1991.

[SGFS N 295 1991] Report of the Chairman to JTC1 Advisory Group, SGFS N 295, 12 February 1991.

[SHAPE 1985] *Data Management Standardization for ACE ACCIS*, TM-776, SHAPE Technical Centre, July 1985, NATO UNCLASSIFIED.

[SHAPE 1988] *ACE Manual 96-1-4, Data Management*, SHAPE, 30 October 1988, NATO UNCLASSIFIED.

[SHAPE 1989] *An Architecture Based on OSI Principles for NATO Tactical Data Links*, TM-864, SHAPE Technical Centre, July 1989, NATO UNCLASSIFIED.

[Shirey n.d.] *Defense Data Network Security*, R. W. Shirey, U.S. Defense Communications Agency, Undated.

[SILS 1989] *Standard for Interoperable LAN Security (SILS)*, P802.10/D1, IEEE, 6 January 1989.

[SPACECOM 1991] *Assured Mission Support Space Architecture*, Presentation to the JTC3A Architecture Review, SPACECOM/J5J (LtCol O'Brien, Space Systems), 19 September 1991, UNCLASSIFIED.

[SPAG 1987] *Guide to the Use of Standards, Version 3, Standards Promotion and Applications Group*, January 1987.

[SPARTA 1991] *DoD Multicast Transport Service Specification*, SPARTA, Inc., for the Defense Communications Engineering Center of the Defense Information Systems Agency, 31 January 1991, UNCLASSIFIED.

[Spivey 1989] *The Z Notation*, J.M. Spivey, Prentice Hall, 1989.

[Stallings 1985] *Computer Communications: Architecture, Protocols and Standards, William Stallings*, IEEE Computer Society Press, Silver Spring, MD, 1985.

[Stallings 1987] *Handbook of Computer-Communications Standards*, William Stallings, Volume 1: *The Open Systems Interconnection (ISO) Model and OSI-Related Standards*, MacMillan Publishing Company, New York, 1987.

[Stallings 1987a] *Handbook of Computer-Communications Standards, 3 Volumes*, William Stallings, MacMillan Publishing Company, New York, 1987.

[STAMINA 1990] *Standard Automated Message Interface for NATO ACCIS (STAMINA), Version 4.0*, April 1990.

[STAMINA 1990a] *The STAMINA Specification*, J. R. Reed, S. Goldani, and N. Sanli, NACISA, Proceedings of the Military OSI Symposium, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[STANAG 4406] Draft STANAG 4406, *Military Message Handling System*, Review 1991] Draft, 16 September 1991, NATO UNCLASSIFIED.

[Staton 1991] *Report to the Ad Hoc Working Group on Security to the SG9 Coordination Group*, Hal Staton, Chairman of the AHWG on Security, 29 October 1991, NATO UNCLASSIFIED.

[STC 1991] *NATO ISDN--Standards and Protocols*, Paper Submitted to SG9/WG2, 3 October 1991, SHAPE Technical Centre, NATO UNCLASSIFIED.

[STC 1991a] *Headquarters Information Systems (HIS) and ACCIS Testbed Laboratories*, Briefing to the ATCCIS Permanent Working Group, 8 April 1991, SHAPE Technical Centre Information Systems Division, NATO UNCLASSIFIED.

[Steele 1984] Common LISP, G. L. Steele, Digital Press, 1984.

[STEI 1990] *Definition of Real-Time Services for the OSI Transport Layer*, Pascal Prophete, STEI, French MOD, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Stene 1990] *"The North Sea Project,"* Ovind Stene, Norwegian Hydrographic Service, Geo'89 Symposium on Geographical Information Systems for Command and Control, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Stoffel 1989] *"DEC Opens an X Window for Control Systems,"* J. M. Stoffel, Control Engineering, Volume 36, No. 4, April 1989.

[SUN 1990] *Open Look Graphical User Interface: Application Style Guidelines*, by Sun Microsystems, 1990.

[Swanson 1991] *Software Product Specification for the Group-Oriented Transport Service Protocol*, John Swanson, SPARTA, Inc., for the Defense Communications Engineering Center of the Defense Information Systems Agency, 5 February 1991, UNCLASSIFIED.

[SWG-EDI 1991] *Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI)*, ISO/IEC JTC1/SC21 N 5635, 23 January 1991.

[Tater et al. 1989] *Briefing on Secure Data Network Systems (SDNS) to the Protocol Standards Steering Group*, Gary Tater and Greg Bergren, National Security Agency, 25 October 1988, Record of the 35th Meeting of the PSSG, Defense Communications Engineering Center, 6 January 1989.

[Terrell 1990] *Electronic Information Exchange Standards Requirements*, by Robert Terrell, presented at the *Workshop on Electronic Information Exchange Standards Used in Document Processing Applications*, NIST. Gaithersburg, MD, 30 July 1990.

[Thacker 1987] *"TOP 3.0 Update,"* Bharat Thacker, MAP/TOP Interface, Volume 3, No. 2, MAP/TOP/SME, Spring 1987.

[TSGCE 1985] *Corrigendum to the Terms of Reference for the Subgroup on Data Processing and Distribution (SG9)*, AC302-D162(2nd Revise), 24 July 1985, TSGCEE, NATO UNCLASSIFIED.

[TSGCE 1988] *NATO Requirements for Open Systems Management*, NATO/AC302 (TSGCE)SG/9MAN.0688/01, AHWG on OSI Management, TSGCE SG/9, 1 July 1988, NATO UNCLASSIFIED.

[TSGCE 1989] *Report of AC/302 (TSGCEE) Meeting Held on 10-12 October 1989*, U.S. Mission NATO, 20 October 1989, UNCLASSIFIED.

[TSGCE 1989a] *NATO SG/9 WG/1 18-Month Work Plan*, WG/1, October 1989, NATO UNCLASSIFIED.

[TSGCE 1989b] *Report to SG/9 by the Chairman of WG/1 on the 16th Meeting Held 2-4 October 1989*, 20 October, 1989, NATO UNCLASSIFIED.

[TSGCE 1989c] *Report of AC/302 (TSGCEE) Meeting Held on 10-12 October 1989*, U.S. Mission NATO, 20 October 1989, NATO UNCLASSIFIED.

[TSGCE 1989d] Private communication with the Chair, TSGCEE SG9 WG1, 14 March 1989, UNCLASSIFIED.

[TSGCE 1990] One-Time Meeting on Naming and Addressing, Secretary for TSGCE SG9, 24 May 1990, NATO UNCLASSIFIED.

[TSGCE 1990b] Discussions at the U.S. Postcoordination Meeting, TSGCE SG9, 18-19 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990c] Chairman's Report on the 10th Meeting Held at NOSC San Diego, USA, 5th to 9th February 1990, AC/302(TSGCE) SG/9 Ad Hoc Working Group on OSI Management, February 1990, NATO UNCLASSIFIED.

[TSGCE 1990d] *Use of OSI Standards in NATO-- Strategic and Technical Issues*, Draft for Issue 3, Contribution by the UK to TSGCEE SG9, 4 May 1990, NATO UNCLASSIFIED.

[TSGCE 1990e] *Report to TSGCEE by Chairman Subgroup 9*, TSGCEE SG9, 5 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990f] Briefing to TSGCEE SG9 on a Proposal for a New TOR for SG9, Chairman of SG9, May 1990, NATO UNCLASSIFIED.

[TSGCE 1990g] *The TSGCEE Subgroup 9 Support Programme for OSI in Military Communications*, Ian White, Admiralty Research Establishment (ARE), UK MOD, Proceedings of the Military OSI Symposium, SP-8, Volume 1 (Unclassified Paper), File Reference 9980, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990h] *The Use of OSI in Military Communications*, Ian White, Admiralty Research Establishment (ARE), UK MOD, Proceedings of the Military OSI Symposium, SP-8, Volume 1 (Unclassified papers), File Reference 9980, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990i] *Report of AC/302 SG/9 on WG/2 Activities (Brussels, February 1990)*, WG/2, 14 March 1990, NATO UNCLASSIFIED.

[TSGCE 1990j] *Draft Proposed Terms of Reference for WG3*, WG/3, 22 January 1990, NATO UNCLASSIFIED.

[TSGCE 1990k] *Report of the TSGCEE Subgroup 9 on Data Processing and Distribution Meeting Held 9-11 May 1990*, U.S. Representative (O. Schultz), May 1990, NATO UNCLASSIFIED.

[TSGCE 1990l] *Report on the SG/9 AHWG-OSI Management Meeting Held in San Diego During 5-9 February 1990*, U.S. Representative (Lew Gutman), 13 February 1990, UNCLASSIFIED.

[TSGCE 1990m] *Chairman's Report of the 8th Meeting*, AC/302(TSGCEE)SG/9 Ad Hoc Working Group on Security, May 1990, NATO UNCLASSIFIED.

[TSGCE 1991] *UK Statement on the Current Status of the Quality of Service Work*, Contribution to TSGCE SG9/WG2, 19 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991a] *Use of OSI Standards in NATO--Strategic and Technical Issues*, Draft, for Issue 4, Contribution by the UK to TSGCE SG9, 8 February 1991, NATO UNCLASSIFIED.

[TSGCE 1991b] *Report of the Chairman of SG9 on the Chairman's meeting of 10 December 1991*, TSGCE SG9, December 1991, NATO UNCLASSIFIED.

[TSGCE 1991c] *U.S. Requirements to Reactivate the Multipeer Data Transmission Project (JTC 1.21.09.01)*, U.S. Contribution to SC21/WG1, 7 March 1991, UNCLASSIFIED.

[TSGCE 1991d] *Comments on Transport STANAGs*, UK Contribution to WG1, United Kingdom, 21 March 1991, NATO UNCLASSIFIED.

[TSGCE 1991e] *WG2 Chairman's Report to SG9*, 4 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991f] *Status Report of the AC/302(SG/9) Ad Hoc Management Group*, 1 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991g] *Multifunction Information Distribution System (MIDS) Low Volume Terminal (LVT) International Cooperative Program*, Briefing of U.S. Representative to PG9 to the U.S. SG9 Coordination Group, 29 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991h] *MMHS AHWG Rationale Document*, Working Draft, 30 September 1991, NATO UNCLASSIFIED.

[TSGCE 1991i] *U.S./EUROCOM's Role in Developing Profiles for NATO*, AC302/SG9/WG1-8910/15(NO), 2 October 1989, NATO UNCLASSIFIED.

[TSGCE 1991j] *Phase I Final Report*, TSGCE SG11/PG6 on Tactical Communications Systems for the Land Combat Zone--Post 2000, Submitted to SG11 on 13 November 1991, NATO RESTRICTED.

[TSGCE 1991k] *Report to the Tri-Service Group by the Chairman of the Subgroup on Information Systems*, AC/302(SG/12)D/7, 21 November 1991, NATO UNCLASSIFIED.

[TSGCE 1991m] *Report to the Tri-Service Group by the Chairman of the Subgroup on Information Systems*, AC/302(SG/12)D/7, Appendix 3 to Annex III to AC/302-D/621, AC/302(SG/12)D/7, 21 November 1991, NATO UNCLASSIFIED.

[TSGCE 1991n] *UK Statement on the Current Status of the Quadrilateral Interoperability Programme (QIP) from a National Viewpoint*, Paper Provided to TSGCE SG9/WG2, 19 September 1991, NATO UNCLASSIFIED.

[UK 1988] *Use of OSI Standards in NATO--Strategic and Technical Issues*, AC/302(SG/9)D/19(Revised), United Kingdom for TSGCEE SG9, 1 March 1988, NATO UNCLASSIFIED.

[UK 1990] *NATO as an ISO International Registration Authority, U.K. Contribution to TSGCEE SG9*, May 1990, NATO UNCLASSIFIED.

[Unix 1991] "UI-ATLAS Formally Launched," *Unix International Gazette*, Volume 3, No. 4, November 1991, p. 1.

[US 1988] *Compatibility of STANAG 4214 and GOSIP Network Layer Addressing*, U.S. Input to WG/1, August 1988, NATO UNCLASSIFIED.

[USPR 1989] Briefing to TSGCEE SG9 WG2 on ACP 127 and CCITT X.400 Service Element Comparison, U.S. Principal Representative, January 1989.

[van der Voort] *Post 2000 Communications Architectures*, A. T. A. M. van de 1990] Voort, TNO Physics and Electronics Laboratory, Netherlands, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Wallace 1991] *"The JPEG Still Picture Compression Standard,"* by Gregory K. Wallace, in Communications of the ACM, Volume 34, No. 4, April 1991, pp. 31-44.

[Walters 1991] Private communication with Dale Walters and Richard Collela, NIST, 8 January 1992.

[Walmsley 1990] *Private communication with Clive Walmsley*, RSRE, U.K. MOD, 27 March 1990.

[Wexelblat et al.] *A Preliminary Description of a Target Architecture for Generic* 1991] Command *and Control Information Systems*, IDA Paper P-2490, 19 August 1991, DRAFT.

[WG/1 1989] NATO SG/9 WG/1 18-Month Work Plan, WG/1, October 1989, NATO UNCLASSIFIED.

[WG/1 1989a] Report to SG/9 by the Chairman of WG/1 on the 16th Meeting Held 27 February to 3 March 1989, AC/302(SG/9)WG/1D-14, 10 May 1989, NATO UNCLASSIFIED.

[WG/1 1989b] Report to SG/9 by the Chairman of WG/1 on the 17th Meeting Held 2-4 October 1989, 20 October, 1989, NATO UNCLASSIFIED.

[WG/1 1990] Report to SG/9 by the Chairman of Working Group 1 on the 18th Meeting Held 26 February to 2 March 1990, WG/1, 21 April 1990, NATO UNCLASSIFIED.

[WG/1 1990c] Report to SG/9 by the Chairman of Working Group 1 on Liaison with WG/2, WG/1, 21 April 1990, NATO UNCLASSIFIED.

[WG/2 1989] Report to AC/302 SG/9 on WG/2 Activities (Brussels, October 1989), WG/2, 8 October 1989, NATO UNCLASSIFIED.

[WG/2 1990] Report to AC/302 SG/9 on WG/2 Activities (Brussels, February 1990), WG/2, 14 March 1990, NATO UNCLASSIFIED.

[WG/2 1990a] *NATO SG/9 WG/2 12-Month Work Plan, WG/2*, May 1990, NATO UNCLASSIFIED.

[WG/2 1990b] *Military Message Handling Registration Recommendation to SG/9, WG/2*, 27 February 1990, NATO UNCLASSIFIED.

[WG/3 1990] Draft Proposed Terms of Reference for WG3, WG/3, 22 January 1990.

[Winkler 1991] *Personal communication with Jerry Winkler*, Chair, ANSI X3H4 on IRDS standards, 18 April 1991.

[WP 60 Annex 1990] *Statement of the Requirement for a NATO Data Management Policy, Annex to AC/317 (WG/2) WP/60 on Data Management, Working Paper, Information Systems Working Group*, NACISA, 5 June 1990, NATO UNCLASSIFIED.

[WP7L 1989] *ATCCIS Working Paper 7L, Data Management, Standardization, and Naming Conventions, Edition 1.0*, 2 June 1989, NATO UNCLASSIFIED.

[X3 1990] *"Standardization Activities,"* in *Computer Standards and Interfaces*, Volume 11, No. 1, 1990, p.78.

[X3 1991] *X3 Announces the Approval of a New Project on Addenda to ISO 8613, News Release from Accredited Standards Committee X3, Information Processing Systems*, April 4, 1991.

[X3 1991a] *X3 Announces the Second Public Review and Comment Period of X3.190-199x, Conformance Testing for SGML, Accredited Standards Committee X3, Information Processing Systems*, News Release, 16 April 1991.

[X3 1991b] *X3 Announces the Approval of a New Project on Group MAC Addresses to be Published as a Type 3 Technical Report, Accredited Standards Committee X3, Information Processing Systems*, News Release, 9 April 1991.

[X3 1991c] *X3 Announces the Approval of a New Project on Source Routing Transparent (SRT) Bridging for Local Area Networks, Accredited Standards Committee X3, Information Processing Systems*, News Release, 9 April 1991.

[X3 1991d] *X3 Announces the Approval of a New Project on Guidelines for Bridged LAN Source Routing Operation by End System to be Published as a Type 3 Technical Report, Accredited Standards Committee X3, Information Processing Systems*, News Release, 9 April 1991.

[X3 1991e] *X3 Announces a Call for Comments on X3 Project 682-D, Domestic Public/Private X.25 Network Interworking, Accredited Standards Committee X3, Information Processing Systems*, News Release, 5 March 1991.

[X3 1991f] *X3 Announces the Formation of a New Technical Committee, X3T6, Non-Contact Information System Interface, Accredited Standards Committee X3, Information Processing Systems*, News Release, 25 March 1991.

[X3 1991g] *X3 Announces the Approval of a New Project on X.25 Data Transfer Phase Procedures for Operating the Packet Layer Transfer Phase of X.25, Committee X3, Information Processing Systems*, News Release, 11 March 1991.

[X3 1991h] *X3 Announces the Approval of a New Project for a Numerical C Extension Technical Report*, Accredited Standards Committee X3, Information Processing Systems, News Release, 10 April 1991.

[X3 1991i] *X3 Announces the Approval of a New Project on X Window System Data Stream Definition Part IV: Mapping onto Open Systems Interconnection (OSI) Services, News Release, Accredited Standards Committee X3, Information Processing Systems*, April 23, 1991.

[X3 1991j] *Concerns on Progression of Management Access Control CD*, X3T5/91-390, 26 September 1991.

[X3 1991k] *X3 Announces the Approval of a New Project for Data Compression, Adaptive Coding with Sliding Window for Information Interchange*, Accredited Standards Committee X3, Information Processing Systems News Release, October 28, 1991.

[X3 1991m] *X3 Announces the Approval of a New Project for Programming Language C Information Bulletins*, Accredited Standards Committee X3, Information Processing Systems News Release, September 16, 1991.

[X3 1991n] *X3 Announces the Public Review and Comment Period of ISO 11404: Information Technology - Programming Languages - Common Language-Independent Data types*, ASC X3, Information Processing Systems News Release, 3 October 1991.

[X.400 1989] *Private communications with three members of the NIST X.400 Special Interest Group*, 25 May-14 June 1989.

[XPG3 1989] *X/OPEN Portability Guide (XPG3), Third Edition, X/Open Group*, 1989.

[X/OPEN 1987] *X/OPEN Portability Guide, Volume 5, Data Management, X/OPEN Group*, Amsterdam, January 1987.

[X/OPEN 1987a] *X/OPEN Portability Guide, Volume 1, System V Specification Commands and Utilities, X/OPEN Group*, Amsterdam, January 1987.

[X/OPEN 1988] Briefing on X/OPEN, X/OPEN Group, Amsterdam, 2 March 1988.

[XTP 1988] XTP/PE Overview, Greg Chesson, Silicon Graphics, April 1988.

[XTP 1989] *XTP Protocol Definition, Revision 3.4, Protocol Engines, Inc.*, Santa Barbara, California, 17 July 1989.

ACRONYMS

4GL	Fourth Generation Language
A	Application (profile)
AAIS	ACE ACCIS Implementation Strategy
ABCA	Australia, Britain, Canada, and America
ABDIS	Abonnee Distributie Systeem
AC	Armament Committee (NATO)
ACBA	Allied Command Baltic Approaches
ACC	Access Control Center (U.S. DoD, BLACKER)
ACCIS	Automated Command and Control Information System
ACCS	Air Command and Control System
ACD	Access Control Domain
ACE	Allied Command Europe
ACIS	Access Control Information System (SDNS)
ACK	Acknowledgement
ACM	Association for Computing Machinery
ACP	Allied Communications Publication
ACSE	Association Control Service Element (OSI Layer 7)
AD	Addendum (ISO)
ADatP	Allied Data Publication
ADCCP	Advanced Data Communications Control Procedures (ANSI X3.66)
ADI	Directory Application (ISP)
ADMD	Administration Management Domain
ADP	Automated (Automatic) Data Processing
ADS	Automated Data System
ADSIA	Allied Data Systems Interoperability Agency
AE	Application Element
AEP	Application Environment Profile (POSIX)
AFATDS	Advanced Field Artillery Tactical Data System
AFCENT	Allied Forces Central Europe
AFNOR	Association Francaise de Normalisation (France)
AFT	File Transfer, Access, and Management Profile
AHWG	Ad Hoc Working Group
AHWG-FP	Ad Hoc Working Group on Functional Profiles (TSGCE SG9)
AHWG-ISDN	Ad hoc Working Group on ISDN
AHWG-MMHS	Military Message Handling System
AHWG-OM	Ad Hoc Working Group on OSI Management
AHWG-OM	Ad Hoc Working Group on OSI Management (TSGCE SG9)
AI	Artificial Intelligence
AIAA	American Institute for Aeronautics and Astronautics
AIE	Ada Integrated Environment (Air Force)
AJPO	Ada Joint Program Office
ALF	Application-Level Facility (ATCCIS)
ALS	Ada Language System (Army); Application Layer Structure (OSI)
AM	ACE Manual
AMH	Automated Message Handling

AMSSA	Assured Mission Support Space Architecture
ANCA	Allied Naval Communications Agency (NATO)
ANS	ANSI National Standard (United States)
ANSI	American National Standards Institute
AO	Accredited Organization (ANSI)
AOW	Asia-Oceania Workshop (Sponsored by POSI)
APDU	Application Program Data Unit
API	Applications Programming Interface
APIU	Adaptive Programmable Interface Unit
APP	Applications Portability Profile (NIST)
APSE	Ada Programming Support Environment
APTL	Accredited POSIX Testing Laboratories
APTL	Accredited POSIX Testing Laboratories (NIST)
AR	U.S. Army Regulation
ARPANET	Advanced Research Projects Agency Network (United States)
AS	Accredited Sponsor (ANSI)
ASC	Accredited Standards Committee (ANSI)
ASCII	American National Standard Code for Information Interchange
ASE	Application Service Element (OSI)
ASME	American Society for Mechanical Engineers
ASN	Abstract Syntax Notation (OSI)
ASN.1	Abstract Syntax Notation One
ASO	Application Service Object (OSI)
ASW	Anti Surface Warfare (Navy)
ATACC	Advanced Tactical Air Command Central (U.S. DoD)
ATAF	Allied Tactical Air Force
ATCA	Allied Tactical Communications Agency (NATO)
ATCCIS	Army Tactical Command and Control Information System
ATCCS	U.S. Army Tactical Command and Control System
ATIS	A Tools Integration Standard
ATLR	Active Transport Layer Relay
ATOC	Allied Tactical Operations Centre
ATOMAL	Security Category
ATP	Allied Tactical Publication; TP Profile
ATS	Abstract Test Suite
AUTODIN	Automatic Digital Network (U.S. DoD)
AVI	Audio Visual Interactive Scriptware (JTC 1)
AVT	VT Profile
AWHQ	Alternate War Headquarters
AXX	Those requiring the COTS (?)
B	ISDN B Service (64 kbit/second)
BAC	Balanced Class of Procedures
BASE	Baseband
BER	Basic Encoding Rules (ASN.1)
BFA	Battlefield Functional Area
BFE	BLACKER Front End (U.S. DoD)
BICES	Battlefield Information Collection and Exploitation Systems
BIH	Bureau International de l' Heure (France)
BISDN	Broadband ISDN
BPS	BICES Pilot Study
BRDF	Draft British Standard

BROAD	Broadband
BSD	Berkeley System Definition (Unix)
BSI	British Standards Institute (United Kingdom)
C2	Command and Control
C2I	Command, Control, and Information
C2RA	Command and Control Requirements Analysis
C3	Consultation, Command and Control
CAD	Computer Aided Design
CAE	Common Applications Environment (X/Open)
CAIS	Common APSE Interface Set
CALS	Computer Acquisitions and Logistics Support (United States)
CAM	Computer Aided Manufacturing
CASE	Common Application Service Elements (OSI Layer 7)
CASE	Computer-Aided Software Engineering
CBEMA	Computer and Business Equipment Manufacturers Association (United States)
CCIR	Comite Consultatif International de Radio (International Radio Consultative Committee)
CCIS	Command and Control Information System
CCITT	Comite Consultatif International de Telegraphique et Telephonique (International Telegraph and Telephone Consultative Committee)
CCR	Commitment, Concurrency, and Recovery (OSI Layer 7)
CCS	Calculus of Communicating Systems (LOTOS)
CCSDS	Consultative Committee on Space Data Systems
CD	Committee Draft (ISO)
CD-ROM	Compact Disk Read Only Memory
CDAD	Committee Draft Addendum
CDAM	Committee Draft Amendment
CDIF	CASE Data Interchange Format
CDTR	Committee Draft Technical Report
CEC	Commission of the European Community
CECOM	US Army Communications-Electronics Command
CEDD	Committee for the Exchange of Digital Data (IHO)
CEN	Comite Europeen de Normalisation (European Committee for Standardization)
CENELEC	Comite Europeen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardization)
CEPT	Conference Europeenne des Postes et Telecommunications
CER	Confidential Encoding Rules (ASN.1)
CG-VDI	Computer Graphics Virtual Device Interface
CGI	Computer Graphics Interface (Interfacing)
CGM	Computer Graphics Metafile
CGMIF	Computer Graphics Metafile Interchange Format
CHILL	CCITT High Level Language
CHS	Common Hardware Software
CIA	CASE Integration Services
CIEG	Common Information Exchange Glossary
CIGOS	Canadian Interest Group on Open Systems
CIGREF	Club Informatique des Grandes Enterprises Francaises (France)
CIM	Center for Information Management (DISA); Corporate Information Management (U.S. DoD initiative)
CINC	Commander-in-Chief
CIS	CASE Integration Services Committee
CL	Connectionless (mode)

CL-TS	CL-TS over CLNS
CLID	Common Language-Independent Data Types
CLIP	Common Language-Independent Procedure Calling Mechanisms
CLIPCM	Common Language-Independent Procedure Calling Mechanisms
CLNP	Connectionless Network Protocol (OSI)
CLNS	Connectionless Network Service (OSI)
CLTS	Connectionless Transport Service (OSI)
CMB	Configuration Management Board
CMF	Common Message Format
CMIP	Common Management Information Protocol (OSI)
CMIS	Common Management Information Service (OSI)
CNAD	Conference of National Armaments Directors (NATO)
CNR	combat net radio
CNSI	Communication System/Network Interoperability
CO	Connection Oriented (mode)
CO-TS	Application profiles using CO-mode transport service (TS)
COE	Common Operating Environment
COLOC	Change of Location of Command
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	continuity of operations
CONS	Connection-Oriented Network Service (OSI)
COS	Corporation for Open Systems
COSINE	Corporation for Open Systems Interconnection Networking in Europe (COSINE)
COTS	Connection-Oriented Transport Service (OSI); Commercial Off-the-Shelf
CP	Command Post
CPCN	Command Post Communication Network
CR	Central Region (NATO)
CSA	Canadian Standards Association
CSDN	Circuit Switched Data Network
CSL	Computer Systems Laboratory (NIST)
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSN	Circuit Switched Network
CSNI	Communications System/Network Interoperability
CSP	Communicating Sequential Processes (LOTOS)
CSPDN	Circuit Switched Public Data Network
CSS	Combat Service Support
CSSCS	Combat Service Support Control System (US Army)
CSWG	Communications Systems Working Group (NACISA)
CTMF	Conformance Testing Methodology and Framework.
CTS	Conformance Testing Services (CEN/CENELEC)
CTS-WAN	Conformance Testing Services-Wide Area Network
CUA	Common User Access (IBM)
D	ISDN D Service (16 kbit/second)
DAD	Draft Addendum (ISO)
DAF	Framework for the Support of Distributed Applications (CCITT)
DAFTG	Database Architecture Framework Task Group (ANSI)
DAM	Draft Amendment (ISO)
DAO	Document Architecture Operations
DAP	Document Application Profile

DAPWG	DFTS Architecture and Procurement Working Group
DARPA	Defense Advanced Research Projects Agency (U.S. DoD)
DBE	Database Enquiry
DBMS	Database Management System
DCA	Defense Communications Agency (see DISA)
DCC	Data Country Code
DCE	Data Circuit-Terminating Equipment
DCF	Data Communication Function
DCPS	Data Communications Protocol Standards
DCT	Digital Communications Terminal (U.S. DoD)
DCW	Digital Chart of the World
DDL	Data Definition Language
DDN	Defense Data Network (U.S. DoD)
DEC	Digital Equipment Corporation
DER	Distinguished Encoding Rules (ASN.1)
DFR	Document Filing and Retrieval
DFTS	Defence Fixed Telecommunications System
DGIWG	Digital Geographic Information Working Group
DIB	Directory Information Base
DID	Data Item Descriptors
DIGEST	Digital Geographic Information Exchange Standard
DIN	Deutsches Institut fur Normung (Federal Republic of Germany)
DIR	Directory
DIS	Draft International Standard (ISO)
DISA	Defense Information Systems Agency (U.S. DoD, formerly DCA)
DISNET	Defense Integrated Secure Network (U.S. DoD)
DISP	Draft International Standardized Profile
DISSP	Defense-Wide Information Systems Security Program
DIT	Directory Information Tree
DMA	Defense Mapping Agency (U.S. DoD)
DME	Distributed Management Environment (OSF)
DMF	Data Management Facility (ATCCIS)
DML	Data Manipulation Language
DMRM	Data Management Reference Model
DMS	Data Management Subsystem (ACE CCISs); Defense Message System (U.S. DoD)
DMS	Defense Message System (U.S. DoD)
DNS	Domain Name System (U.S. DoD)
DOA	Distributed Office Application
DOAM	Distributed Office Applications Model
DoD	Department of Defense (United States)
DoD-STD	DoD Standard
DoDCSC	U.S. Department of Defense Computer Security Center
DoDISS	DoD Index of Standards and Specifications
DP	Draft Proposal (ISO)
DPA	Document Printing Application
DPS	Digital Production System (DMA)
DPSN	Defence Packet Switched Network
DQDB	Distributed Queue Dual Bus (local area network)
DQSO	Defense Quality Standardization Office
DSA	Directory System Agents
DSG	Distributed System Gateway
DSP	Domain Specific Part

DSSSL	Document Style Segmentation and Specification Language
DTAM	Document Transfer and Manipulation
DTD	Document Type Definition
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTMP	DCPS Technical Management Panel (U.S. DoD)
DTP	Distributed Transaction Processing
DTR	Draft Technical Report (ISO)
DUA	Directory User Agent (ISO)
DVI	Digital Video Interactive
E-Mail	Electronic Mail
E3	End-to-End Encryption
EC	European Community
ECCM	Electronic Counter-Countermeasures
ECITC	European Committee for IT Testing and Certification
ECMA	European Computer Manufacturers Association
ED&C	Error Detection and Correction
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce, and Transport
EESP	End-to-End Security Protocol
EFTA	European Free Trading Association
EG	Expert Groups (NIST OSI Implementor's Workshop)
EGDIR	Directory Expert Group (EWOS)
EGTP	Expert Group on Transaction Processing (EWOS)
EIA	Electronic Industries Association
EIFEL	Allied Tactical Operations Centre CCIS (ATOC CCIS, also known as the EIFEL Follow-On
ELINT	Electonic Intelligence
EMD	Engineering and Manufacturing Development
EMUG	European Manufacturing Automation Program (MAP) User Group
EN	European Norm (European Standard) (CEN/CENELEC)
ENSCE	Enemy Situation Correlation Element
ENV	European Norm Vornorm (European Experimental Standard) (CEN/CENELEC)
EPA	Environmental Protection Agency (US Government)
EPHOS	European Procurement Handbook for Open Systems
EPLRS	Enhanced Position Location Reporting System
ES-IS	End System to Intermediate System
ESPRIT	European Strategic Programme of Research and Development in Information Technology
ETSI	European Telecommunications Standards Institute
EUROCOM	Eurogroup on Cooperation of Tactical Communications Systems
EWOS	European Workshop for Open Systems
FAAD	Forward Area Air Defense
FACC	Feature Attribute Coding Catalog
FCG	Computer Graphics Profile
FCS	Frame Check Sequence
FD	Formal Description
FDDI	Fiber Distributed Data Interface
FDI	Directory Data Definitions Profile
FDT	Formal Description Technique

FEC	Forward Error Correction
FFOL	FDDI Follow-On LAN
FFOL-AMAC	FFOL - Asynchronous Media Access Control
FFOL-IMAC	FFOL - Isochronous Media Access Control
FFOL-PHY	FFOL - Physical Layer Protocol
FFOL-PMD	FFOL - Physical Medium Dependent
FFOL-SMT	FFOL - Station Management
FFOL-SMUX	FFOL - Service Multiplexer
FIMS	Forms Interface Management System
FIPS	Federal Information Processing Standard (United States)
FLTSATCOM	Fleet Satellite Communications
FMCT	Formal Methods in Conformance Testing
FMS	Fixed/Mobile Segment
FOD	Office Document Format Profile
FOIRL	Fiber Optic Inter-Repeater Link
FORMETS	Message Text Formatting System (NATO)
FORTRAN	Formula Translation (programming language)
FRP90	Frigate Replacement Program for the 1990s (NATO)
FSK	Frequency Shift Keying
FSSG	Fire Support Subgroup (JTC3A)
FTAM	File Transfer, Access and Management (OSI Layer 7)
FTP	File Transfer Protocol (U.S. DoD)
FTR	Future (standard)
FUI	Flow (Control) Unnumbered Information
FXX	Interchange format/Presentation profiles
G-LOTOS	Graphical LOTOS (profiles)
GAN	Global Area Network
GAP	Stop-gap (nonstrategic standard)
Gbps	Gigabits per second
GDMI	Generic Definition of Management Information (OSI)
GEADGE	German Air Defense Ground Environment
GIF	Graphics Interchange Format
GIS	Geographic Information System
GKS	Graphical Kernel System
GKS-3D	Graphical Kernel System for Three Dimensions
GLOBIXS	Global Information Exchange Systems
GNMP	Government Network Management Profile
GOSI	Generic Operating System Interface
GOSIP	Government Open Systems Interconnection Profile
GSTN	General Switched Telephone Network
GTDI	EDI Standard (syntax)
GUI	Graphical User Interface
HCI	Human-Computer Interface
HD	Harmonized Document (CEN/CENELEC)
HDLC	High-Level Data Link Control (OSI Layer 2)
HDTV	High Definition Television
HDU	Hard Disk Unit
HEROS	Heeres-Fuehrungsinformationssystem fur die rechnergestuetzte Operations- fuehrung in Staeben
HFS	Human Factors Society

HISs	Headquarters Information Systems
HTU	Handheld Terminal Unit
HUI	Human Interface
IAB	Internet Activities Board (US DoD)
IAP	Interfaces for Applications Portability (ISO/IEC JTC1)
IBN	Institut Belge de Normalisation (Belgium)
ICA	Integrated Communications Architecture
ICD	International Code Designator
ICL	International Computers Limited
ICS	Implementation Conformance Statement
ICSI	International Coding System Identifier
ICT	Intercept Recommendation (TSGCE SG9)
ID	Identification
IDI	Initial Domain Identifier
IDN	Interface Definition Notation (ECMA 127)
IDP	Initial Domain Part
IEC	International Electrotechnical Commission
IEE	Institution of Electrical Engineers (United Kingdom)
IEEE	Institute of Electrical and Electronics Engineers (United States)
IEPG	Independent European Programme Group (NATO)
IER	Information Exchange Requirement
IEW	Intelligence and Electronic Warfare
IFF	Interchange File Format
IFIP	International Federation for Information Processing
IFRB	International Frequency Registration Board (UIT)
IFU	Interworking Functional Unit
IGES	Initial Graphics Exchange Specification
IHO	International Hydrographic Organization
IIRS	Institute for Industrial Research and Standards (Ireland)
IJMS	Interim JTIDS Message Standard
IML	Library
INFOSEC	Information Security
INSTAC	Information Technology Standardization Technology Committee
INTAP	Interoperability Technology Association for Information Processing (Japan)
INTEROP	International Operations
IOC	Initial Operational Capability
IOF	Input-Output Facility (ATCCIS)
IP	Internet Protocol; Interoperability Parameter; Internetwork Protocol
IPM	Interpersonal Messaging (MHS Service)
IPMS	Interpersonal Messaging Service
IR	International Registry
IRD	Information Resource Dictionary
IRDS	Information Resource Dictionary System
IS	International Standard (ISO); Intermediate System (OSI)
ISAM	Indexed Sequential Access Method
ISCS	Integrated Satellite Control Services
ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environment (ISEE) Working Group (NIST)
ISO	International Organization for Standardization; International Standard
ISO-DCC	International Organization for Standardization; International Standard-Data Country Code

ISO-SWG	International Organization for Standardization; International Standard-Special Working Group
ISODE	ISO Development Environment
ISP	International Standardized Profile
IST	International Standards
ISWG	Information Systems Working Group
ITDN	Integrated Tactical-Strategic Digital Network (US DoD)
ITI	Industrial Technology Institute
ITS	Integrated Tool Set (COS)
ITSEC	Information Technology Security Evaluation Criteria
ITSTC	Information Technology Steering Technical Committee (UK)
ITU	International Telecommunications Union
IUKADGE	Improved United Kingdom Air Defence Ground Environment
IVD	Integrated Voice and Data (local area network)
IWF	Interworking Function
IWG	Information Working Group
IWU	Interworking Unit (OSI for relay functional profiles)
JANAP	Joint Army, Navy, Air Force Publication
JBIG	Joint Bi-Level Imaging Group
JINTACCS	Joint Interoperability of Tactical Command and Control Systems (US DoD)
JIS	Japanese Industrial Standard
JISC	Japanese Industrial Standards Committee
JMSWG	Joint Messaged Standards Working Group (JTC3A)
JPEG	Joint Photographic Experts Group
JROC	Joint Requirements Oversight Council (U.S. DoD)
JSA	Japanese Standards Association
JTAP	JTC1 TAG Applications Portability Study Group
JTC	Joint Technical Committee
JTC1	Joint Technical Committee One (ISO/IEC)
JTIDS	Joint Tactical Information Distribution System
JTM	Job Transfer and Manipulation (OSI Layer 7)
JTSSG	Joint Technical Standards Steering Group (DoD)
KAPSE	Kernel Ada Programming Support Environment
KBS	Knowledge Based Systems
KDC	Key Distribution Center (BLACKER)
KIT	KAPSE Interface Team
KITIA	KAPSE Interface Team from Industry and Academia
KMAE	Key Management Application Entity
KMAP	Key Management Application Process
KMASE	Key Management Application Service Element
LAAD	Low-Altitude Air Defense
LAN	Local Area Network
LAP B	Link Access Procedure, Balanced
LAP D	Link Access Procedure, Version D (used for ISDN)
LAS	Local Access Subsystem
LCAS	Language Compatible Arithmetic Standard
LCC	Limited Capability Configuration
LISA	Link in Support of ACCS
LLC	Logical Link Control (OSI Network Layer)

LOCE	Limited Operational Capability-Europe
LOTOS	Language of Temporal Ordering of Specification
LTACFIRE	Lightweight Tactical Fire Direction System
LTDP	Long-Term Defence Plan
LVT	Low Volume Terminal
LWER	Light Weight Encoding Rules
MAC	Media Access Control
MACF	Multiple Association Control Function
MAN	Metropolitan Area Network
MAP	Manufacturing Automation Protocol
MAPSE	Minimum Ada Programming Support Environment
MAS	Military Agency for Standardization
Mbps	Megabits per second
MC&G	Mapping, Charting, and Geodesy (DMA)
MCG	Mapping, Charting, and Geodesy
MCGT	Mapping, Charting and Geodesy Technology Standardization Area (U.S. DoD)
MCS	Maneuver Control System (US Army)
MF	Mediation Function
Mgd	Managed
Mgmt	Management
MHEG	Multimedia and Hypermedia information coding Experts Group
MHS	Message Handling System (OSI Layer 7)
MHz	Megahertz
MIA	Multivendor Integration Architecture
MIB	Management Information Base
MIDLA	Media-Independent Data Link Architecture (TSGCE)
MIDS	Multinational Information Distribution System (NATO)
MIL-STD	Military Standard (US DoD)
MILNET	Military Network (United States)
MIPS	Management Information Protocol Specification (see CMIP)
MIR	Management Information Register
MIS	Management Information Service (OSI); Management Information System
MISD	Management Information Service Definition (see CMIS)
MIT	Massachusetts Institute of Technology
MITI	Ministry of International Trade and Industry (Japan)
MM	Mixed Mode (of Operations in DTAM)
MMHS	Military Message Handling System
MMI	Man-Machine Interface
MML	Man-Machine Language (CCITT Z.300 s ies)
MMS	Manufacturing Message Specification (MAP)
MNC	Major NATO Command
MO:DCA	Mixed Object Document Content Architecture
MOCS	Managed Object Conformance Statement
MOD	Ministry of Defence (United Kingdom)
MOT	Means of Testing
MOTIS	Message-Oriented Text Interchange System (OSI Layer 7)
MPC	Multi Party Communications
MPD	Multipeer Data
MPDT	Multipeer Data Transmission (OSI)
MPEG	Moving Pictures Expert Group
MPTM	Multi-party Test Methods

MROC	Multicommand Required Operational Capability
MS	Message Store (MHS)
MSC	Major Subordinate Command (NATO)
MSDSG	Multi-System Distributed System Gateway
MSE	Mobile Subscriber Element (U.S. Army)
MSF	Man-Machine Support Facility
MSP	Message Security Protocol (SDNS)
MT	Message Transfer
MTA	Message Transfer Agent (MHS)
MTACCS	Marine Tactical Command and Control System
MTF	Message Text Formats
MTS	Marine Tactical Systems (U.S. DoD)
MTS	Message Transfer System (MHS)
N	Notice (ISO Working Paper)
NACISA	NATO Communications and Information Systems Agency
NACISC	NATO Communications and Information Systems Committee
NACISO	NATO Communications and Information Systems Organization
NACMA	NATO ACCS Management Agency
NAEW	NATO Airborne Early Warning
NAOIW	North American OSI Implementor's Workshop
NATO	North Atlantic Treaty Organization
NATO-ICD	NATO-International Code Designator
NBS	US National Bureau of Standards (now NIST)
NBSIR	NBS Interim Report
NC	NATO Confidential
NCC	National Computing Centre
NCCIS	NATO Command, Control and Information System
NCIS	NATO Common Interoperability Standards
NCISI	Non-Contact Information Systems Interface
NCS	National Communications System (U.S. DoD)
NCS	Network Computing Services
NCSL	National Computer Systems Laboratory (NIST)
NDE	News Development Environment (Sun Microsystems)
NDI	Nondevelopmental Item
NDL	Network Database Language (OSI)
NEC	Northern European Command
NEF	Network Element Function
NET	Telecommunications European Norm
NFR90	NATO Frigate Replacement for the 1990s
NFS	Network File Service
NIAG	NATO Industrial Advisory Group
NIDL	Network Interface Definition Language
NIIF	Network Independent Interface (NIAG SG6)
NIIS	NATO Interconnected Information System
NILS	Network Internal Layer Structure
NIMP	NATO Interoperability Management Plan
NIPD	NATO Interoperability Planning Document
NIS	NATO Identification System
NIST	U.S. National Institute of Standards and Technology
NLR	Network Layer Relay
NLS	Native Language Support (X/Open)

NLSP	Network Layer Security Protocol
NM	Network Management
NMForum	Network Management Forum
NMOS	NATO Maritime Operational Intelligence Support
NMP	Network Management Profile
NMSIG	Network Management Special Interest Group (NAOIW)
NNI	Nederlands Normalisatie-Instituut (Netherlands)
NOSA	NATO OSI Security Architecture
NOSIP	NATO Open Systems Interconnection Profiles
NP	New Project (ISO, formerly New Work Item)
NPDU	Network Protocol Data Unit
NPICS	NATO Protocol Implementation Conformance Statement
NPS	Nuclear Planning System
NR	NATO Restricted
NS	NATO Secret
NSA	National Security Agency (United States)
NSAI	National Standards Authority of Ireland
NSAP	Network Service Access Point (OSI)
NSP	NATO Standardized Profiles
NSS	National Standards System (Canada)
NTF	National Transfer Format (United Kingdom)
NTIS	National Technical Information Service (United States)
NTIS	NATO Technical Interoperability Standards
NTP	Network Time Protocol
NTT	Nippon Telegraph and Telephone Corporation (Japan)
NU	NATO Unclassified
NVLAP	National Voluntary Laboratory Accrediation Program (NIST)
NWI	New Work Item (ISO) (see also NP)
ODA	Office Document Architecture
ODAC	Office Document Architecture Consortium
ODIF	Office Document Interchange Format
ODL	Office Document Language
ODP	Open Distributed Processing
OIW	(North American) OSI Implementor's Workshop
OM	OSI Management
OODBTG	Object-Oriented Database Task Group (ASC X3)
OS	Operating System
OS/2	Operating System 2 (IBM)
OSCRL	Operating System Command and Response Language
OSD	Office of the Secretary of Defense (U.S. DoD)
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSINET	Open Systems Interconnection Network
OSITOP	Open Systems Interconnection for Technical and Office Protocol
OSITP	OSI Transaction Processing
OSN	Open Systems Newsletter
OSTC	Open Systems Testing Consortium
PAD	Packet Assembly/Disassembly
PAR	Project Authorization Request (IEEE)

PCDAM	Proposed Committee Draft Amendment (ISO)
PCIS	Portable Common Interface Set
PCNCEP	Political Consultation and NATO Civil Emergency Planning
PCTE	Portable Common Tool Environment
PCTS	POSIX Conformance Test Suite
PCU	Portable Computer Unit
PDAD	Proposed Draft Addendum (ISO)
PDAM	Proposed Draft Amendment (ISO)
PDES	Product Definition Exchange Specification
PDIF	Product Definition Interchange Format
PDISP	Proposed Draft International Standardized Profile
PDL	Page Description Language
PDN	Public Data Network
PDTR	Proposed Draft Technical Report
PDU	Protocol Data Unit
PEO-CCS	Program Executive Officer, Command and Control Systems
PER	Packed Encoding Rules (ASN.1)
PHIGS	Programmer's Hierarchical Interactive Graphics System
PHY	Physical
PICS	Protocol Implementation Conformance Statement
PLI	Position Location Information
PLP	Packet Level Protocol (X.25)
PLPS	Presentation Level Protocol Syntax
PM	Processable Mode (of Operations in DTAM)
PMD	Physical Layer Medium Dependent
PMS	Packet Multicast Service
PN	Project Number
POC	Profile for Open System Environment Components (EWOS)
POCAC	APIs for Communications Services (EWOS OSE Profiles)
POCAI	APIs for Information Services (EWOS OSE Profiles)
POCAS	APIs for System Services (EWOS OSE Profiles)
POCAU	APIs for End-User Services (EWOS OSE Profiles)
POCF	Formats (EWOS OSE Profiles)
POCL	Look and Feel Definitions (EWOS OSE Profiles)
POCP	Protocols (EWOS OSE Profiles)
PODA	Piloting Open Document Architecture
POE	Profiles for Open System Environment (EWOS)
POSI	Promoting Conference for OSI (Asia-Oceania Regional Workshop)
POSIX	Portable Operating System Interface for Computer Environments
PPRDB	Partitioned, Partially Replicated Database
PPSC-IT	Public Procurement Subcommittee in the Information Technology Sector (CEC)
PPTM	Protocol Profile Conformance Testing Methodology
prENV	Draft European Prestandard
PRMD	Private Management Domain
PSC	Principal Systems Command; Principal Subordinate Command
PSDN	Packet Switched Digital Network
PSN	Packet Switched Network
PSPDN	Packet Switched Public Data Network
PSPvtDN	Packet Switched Private Data Network
PSSG	Protocol Standards Steering Group
PSTN	Public Switched Telephone Network
PSTP	Protocol Standards Technical Panel (see DTMP)

PTI	Public Tool Interface
PTLR	Passive Transport Layer Relay
PTT	Postal, Telegraph, and Telephone
PVC	Permanent Virtual Circuit
PWG	Permanent Working Group
Q&A	Question and Answer (NATO Identification System)
QIP	Quadrilateral Interoperability Programme
QMHS	Quadrilateral Message Handling System
QoS	Quality of Service
QP	Quadrilateral Profile
QSTAG	Quadrilateral Standardization Agreement
QTDMP	Quadrilateral Test and Demonstration Management Plan
QTIDP	Quadrilateral Technical Interface Design Plan
QTIR	Quadrilateral Technical Interface Requirements
R	Relay (profile)
RA	Remote Action
RACWG	Requirement and Design Criteria Working Group (CAIS)
RAM	Random Access Memory
RARE	Reseaux Associes pour le Recherche Europeenne (Association of European Research Networks)
RD	Restricted Data
RDA	Remote Data Access (OSI)
RDT	Referenced Data Transfer
RFC	Request for Comment
RFP	Request for Proposal
RFT	Request for Technology
RGB	Red-Green-Blue
RLE	Run Length Encoding
RM	Reference Model
RO	Remote Operations
RODE	Remote Open Document Editing
ROMC	Required Operational Messaging Characteristics
ROS	Remote Operation Service (OSI)
ROSE	Remote Operation Service Element (OSI)
RPC	Remote Call Procedure
RSRE	Royal Signals and Radar Establishment
RSTA	Reconnaissance and Target Acquisition
RT	Reliable Transfer
RTA	Reliable Transfer Agent
RTS	Reliable Transfer Service (OSI)
RTSE	Reliable Transfer Service Element
RTTS	Real-Time Transport Service
RWCC	Regional Workshop Coordinating Committee
RWS-CC	Regional Workshop Coordinating Committee
SAA	Systems Application Architecture (IBM)
SACF	Single Association Control Function
SAMeDL	QL-Ada Module Description Language
SANISI	Security Architecture for NATO Information Systems Interconnection
SANTIS	Single Architecture of NATO Technical Common Interface Standards

SAO	Single Association Object
SAP	Service Access Point; Subnetwork Access Protocol (Network Layer)
SASO	Saudi Arabian Standards Organization
SATCOM	Satellite Communications
SC	Sub-Committee (ISO); Study Committee
SCARS	Status Control Alerting and Reporting System
SCC	Standards Council of Canada
SCCS	Source Code Control System (AT&T)
SCF	Service Control Facility (ATCCIS)
SCSI	Small Computer System Interface
SD&IC	System Design and Integration Contract (ACE ACCIS)
SDCP	Subnetwork Dependent Convergence Protocol (OSI Network Layer)
SDH	Synchronous Data Hierarchy
SDIF	SGML Document Interchange Format
SDIO	Strategic Defense Initiative Office
SDL	System Development Language (FDT)
SDN	Secure Data Network
SDNS	Secure Data Network System (U.S. National Security Agency)
SDS	Strategic Defense System
SDTS	Spatial Data Transfer Specification
SDU	Standalone Display Unit
SE	Service Element
SECAN	Military Committee Communications Security and Evaluation Agency (NATO)
SEI	Security Exchange Information
SFA	Specified Subfunctional Area
SFS	Suomen Standardisoimisliitto (Finland)
SG	Subgroup
SGFS	Special Group on Functional Standardization (ISO/IEC JTC1)
SGML	Standard Generalized Markup Language
SHAPE	Supreme Headquarters Allied Powers Europe
SHIF	SHAPE Information Flow
SICF	Systeme Informatique de Commandement des Forces Terrestres
SICP	Subnetwork Independent Convergence Protocol (OSI Network Layer)
SIG	Special Interest Group (NIST OSI Implementor's Workshop)
SIGCOMM	Special Interest Group on Data Communications (ACM)
SIGINT	Signals Intelligence
SII	System Interconnection Interface (MIA)
SILS	Standard for Interoperable LAN Security
SIMNET	Simulation Network (US DoD)
SINCGARS	Single-Channel Ground/Air Radio System (U.S. DoD)
SIS	Standardiseringskommisionen i Sverige (Sweden)
SM	System Manager
SMF	System Management Facility (ATCCIS)
SMI	Structure of Management Information (OSI)
SMPTE	Society of Motion Picture and Television Engineers
SMS	Swedish Mechanical Standardization
SMT	Station Management (FDDI)
SMTP	Simple Mail Transfer Protocol (U.S. DoD)
SN	Subnetwork
SNDCF	Subnetwork-Dependent Convergence Function
SNDCP	Subnetwork Dependent Convergence Protocol (OSI Network Layer)
SNICP	Subnetwork Independent Convergence Protocol (OSI Network Layer)

SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SOGITS	Senior Official Group for Information Technology Standardization (CEC)
SOGT	Senior Official Group on Telecommunications (CEC)
SOSTA	Stand-Off Surveillance Target and Acquisition
SOTAS	Stand-Off Target Acquisition System
SP	Security Protocol (SDNS)
SPACECOM	Space Command
SPAG	Standards Promotion and Applications Group
SPARC	Standards and Planning Requirements Committee
SPDL	Standard Page Description Language
SQL	Standard Query Language (ISO)
SRT	Source Routing Transparent (LAN Bridging)
SSI	System Software Interface
SSP	Subnetwork Specific Protocol (Network Layer)
STAMINA	Standard Automated Message Processing Interface for NATO's ACCISs
STANAG	NATO Standardization Agreement
STC	SHAPE Technical Centre
STDL	Structured Transaction Definition Language (MIA)
Stds	Standards
STE	Signalling Terminal
STEP	Standard for the Exchange of Product Model Data
STL	Standard Text Language
STN	Switched Telephone Network
STR	Strategic (standard)
STRIDA	Systeme de Traitement et de Representation des Informations de Defense Aerienne
SUCOC	Succession of Command
SUMM	Semantic Unification Meta Model (IRDS)
SVID	System V Interface Definition (AT&T Unix)
SWG	Special Working Group (ISO JTC1)
SWG-EDI	Special Working Group on Electronic Data Interchange
T	Transport (profile)
Tac	Tactical
TACFIRE	Tactical Fire Direction System
TACSATCOM	Tactical Satellite Communications
TADIL	Tactical Digital Information Link
TADIXS	Tactical Information Exchange System (US Navy)
TAOM	Tactical Air Operations Module (U.S. DoD)
TBD	To Be Determined
TC	Transport Connections; Technical Committee (ISO)
TCAC	Technical Control and Analysis Center
TCCA	Time-Critical Communications Architecture
TCCS	Time-Critical Communications System
TCG	Technical Coordination Group
TCIS	Technical Common Interface Standards (TSGCE SG9)
TCOS	Technical Committee on Operating Systems (IEEE)
TCP	Transmission Control Protocol (U.S. DoD)
TCS	Trusted Communications Sublayer (SANISI)
TCSEC	Trusted Computer System Evaluation Criteria
TCT	Tactical Computer Terminal
TCU	Transportable Computer Unit

TDC	Time Dispersal Coding
TEK	Traffic Encryption Key
TELNET	Telecommunications Network
TF	Transfer Facility (ATCCIS)
TFA	Transparent File Access (POSIX)
TGA	Targa Image Format
TGRM	Technical Group on Reference Models (ECMA)
TIDP	Technical Interface Design Plan
TIFF	Tag Image File Format
TLSP	Transport Layer Security Protocol
TLV	Tag-Length-Value
TM	Technical Management; Technical Memorandum; Terminal Management
TMD	Terminal Management Domain (TM)
TMN	Telecommunication Management Network
TOP	Technical and Office Protocol
TOR	Terms of Reference
TP	Transaction Processing; Transaction Processing (OSI); Transport Protocol (OSI)
TPDU	Transport Protocol Data Unit (OSI)
TPSUI	Transaction Processing Service User Invocation
TR	Technical Report (ISO)
TRI-MNC	Tri-Major NATO Commanders' Command and Control Plan
TRI-TAC	Joint Tactical Communications Program (U.S. DoD)
TS	Transport Service (OSI)
TSA	Time Synchronization Agent
TSDN	Transfer Syntax Description Notation (ASC X3T2)
TSG	Technical Study Group (ISO/IEC JTC1)
TSGCE	Tri-Service Group on Communications and Electronics (NATO) (formerly TSGCEE)
TSGCEE	Tri-Service Group on Communications and Electronics Equipment (see TSGCE)
TSS	Time Synchronization Service
TTC	Telecommunications Technology Committee (Japan)
TTCN	Tree and Tabular Combined Notation (ISO)
TUA	Time User Agent
UA	User Agent (MHS)
UAVs	Unmanned Aerial Vehicles
UDO	User Descriptor Object (TM)
UDT	Unstructured Data Transfer
UER	Union Europeenne de Radiodiffusion
UI	Unix International
UIL	User Interface Language
UIMS	User Interface Management System
UIT	Union Internationale des Telecommunications (CCITT)
UK	United Kingdom
ULA	Upper Layer Architecture (OSI)
ULTDS	Unit Level Tactical Data Switch
UOD	Universe of Discourse
USAREUR	U.S. Army in Europe
USGS	U.S. Geological Survey
UTACCS	USAREUR Tactical Command and Control System
UTC	Coordinated Universal Time
UTE	Union Technique de l'Electricite (France)

VC	Virtual Circuit
VDM-SL	Vienna Development Method-Specification Language
VDT	Visual Display Terminal
VFUIF	Voice/Fax User Interface Forum
VMF	Variable Message Format
VMUIF	Voice Messaging User Interface Forum
VPS	Vector Product Standard
VSAT	Very Small Aperture Terminal
VT	Virtual Terminal (OSI Layer 7)
VTE	Virtual Terminal Environment
VTP	Virtual Terminal Protocol
WAM	WWMCCS Automated Data Processing (ADP) Modernization
WAN	Wide Area Network
WD	Working Draft
WDAD	Working Draft Addendum (ISO)
WDAM	Working Draft Amendment (ISO)
WDISP	Working Draft International Standardized Profile
WDS	WRRE Demonstrator System
WES	Wavell Enhancement System
WG	Working Group
WHIDDS	War Headquarters Information Dissemination and Display System
WIN	WWMCCS Intercomputer Network
WIS	WWMCCS Information System
WP	Working Paper (ATCCIS)
WRRE	Wavell Risk Reduction Exercise
WSF	Workstation Function
WWMCCS	Worldwide Military Command and Control System
X11	X-Windows, Version 11
XALS	Extended ALS (OSI)
XID	Exchange Identification
XPG3	Third Edition of the X/Open Portability Guide
XSI	X/Open System Interfaces
XTP	Xpress Transfer Protocol
XVS	X/OPEN System V Specification
XVT	Extensible Virtual Toolkit

INDEX

AAP-3, 306
AAP-6, 95
ABDIS, 378
Abstract Syntax Notation One, 131
Abstract Test Suite, 189
ACCS, 5, 316, 353, 362, 363, 364, 406
ACE ACCIS, 11, 94, 95, 113, 353, 360, 361, 362, 365, 372, 406
ACE Architectural Design Study, 360
ACP 123, 113, 114
ACP 127, 114, 142
ACP 129, 142
ACP 167, 95
ACSE, 72, 108, 115, 125, 126, 127, 155, 158, 162, 166, 187, 234, 314
Ada, 61, 62, 64, 70, 147, 148, 214, 239, 240, 241, 243, 244, 245, 248, 249, 250, 251, 255, 256, 257, 259, 357, 391
Ada Programming Support Environment, 244
ADatP-2, 95
ADatP-3, 96
ADDS, 389
ADS, 50
ADSIA, 92, 93, 94, 302, 316, 318, 363, 364, 369
ADSIA Recommendations on Data Management, 93
Advanced Field Artillery Tactical Data System, 388
AEP, 147, 264
AFATDS, 388
AFNOR, 124
AHWG on ATCCIS, 359
AHWG on ISDN, 164, 302, 322
AHWG on MMHS, 301, 329
AHWG on Security, 164, 301, 327
AHWG-OM, 183, 184, 185, 301, 302, 319, 322
Air Command and Control System, 362
AIX, 152, 262, 263, 274
ALFs, 4, 18, 26
All Source Analysis System, 388
ALS, 106, 107, 108, 245
AMSSA, 62
ANSI X12, 205
ANSI X3, 81, 82, 84, 201, 223, 246
ANSI X3B5, 223
ANSI X3H2, 69, 70
ANSI X3H3, 234, 235, 269
ANSI X3H4, 78, 80, 81, 253
ANSI X3J11, 148, 150, 246, 247, 262, 272
ANSI X3J13, 248
ANSI X3J3, 247
ANSI X3J4, 247
ANSI X3L8, 92
ANSI X3S3, 103, 104, 111, 349
ANSI X3T2, 132
ANSI X3T6, 105
ANSI X3T9, 63, 141
ANSI X3V1, 199, 202, 224, 228, 229
APDU, 108, 124
API, 147, 235, 236, 237, 264, 277, 309, 332
APP, 30, 34, 41, 61, 151, 261, 262, 264, 265, 266, 268, 269, 394
Application Layer Concepts, 105
Application Layer STANAGs, 345
Application Layer Structure, 106
Application Profiles, 285
Application Service Elements, 107
Applications Portability Profile, 264
Applications Portability Standards, 270
APSE, 244
ARCHITEL, 375
Army Tactical Command and Control System, 388
ARPANET, 134
ASAS, 388
ASE, 155, 158, 160, 162, 165, 233
ASEs, 107
Asia Oceania Workshop, 283
Asia-Oceania Workshop, 39
Asia/Oceania Workshop, 281
ASN.1, 91, 124, 127, 128, 130, 131, 132, 133, 162, 179, 218, 270, 314, 335, 344, 345, 364
Association, 106
Association Control Service Element, 125
Assured Mission Support Space Architecture, 62
Asynchronous Transfer Mode, 53, 139
ATACC, 396
ATCCIS, 1, 2, 3, 4, 5, 6, 9, 10, 11, 12, 13, 14, 18, 23, 26, 33, 40, 43, 50, 51, 52, 92, 297, 302, 350, 353, 354, 357, 358, 359, 363, 367, 373, 379, 382, 394, 403, 405, 406
ATCCIS Objectives, 9
ATCCIS Architecture, 14
ATCCIS Facilities, 18

ATCCIS Phase II Findings, 11
ATCCIS WP 7L, 92
ATCCIS-Conformant Systems, 22
ATCCS, 388, 398
ATCCS CHS, 389, 396
ATCCS Common Hardware Software, 388
ATLAS, 278
ATLAS 400, 375
ATM, 53, 54, 139
Audio Exchange Standards, 224
AutoKo, 377
Automated Data Systems, 208
Automatic Message Processing System, 372
BASIC, 248
Basic Encoding Rules, 132
Basic Ensemble, 20
Basic Facilities, 18
Basic Interoperability, 2, 13, 40
Basic Options in OSI Standards, 44
Basic Reference Model of ODP, 89
Battlefield Information Collection and Exploitation Systems, 365
BER, 132
Berkeley UNIX, 151
BICES, 365, 406
BICES Pilot Study, 372
Bindings, 248
BISDN, 138
BLACKER, 168, 386
Broadband ISDN, 138
Buffer/gateway, 40
C, 131, 142, 147, 148, 150, 213, 235, 239, 241, 246, 247, 248, 249, 250, 251, 256, 262, 269, 270, 271, 272, 273, 274, 376
C4I for the Warrior, 387
CAE, 150, 270, 277
CAIS, 244, 245, 257
CALS, 71, 202, 225
Canadian Open Systems Applications Criteria, 288
CASE, 250
CCITT, 38
CCITT SG VII, 105, 121, 132, 188
CCITT SG/VIII, 206
CCITT SGVII, 130, 195
CCITT SGVIII, 120
CCR, 72, 86, 108, 117, 125, 126, 127, 193
CEDD, 219
CER, 132
CGI, 213, 214, 248, 249
CGM, 116, 117, 203, 206, 209, 210, 212, 213, 268, 275
CIM, 30, 54, 383
CIM Technical Reference Model, 54, 56
CLNS, 134, 166, 276, 286, 293, 307, 340, 342
CMIS/CMIP, 152
CNET, 375
CNR, 389
COBOL, 70, 77, 116, 247, 256, 268, 272, 273, 274, 277, 284
CODASYL, 91
COE, 60, 61, 62
Combat Service Support Control System, 389
Commitment, Concurrency, and Recovery, 126
Common Applications Environment, 150, 270
Common APSE Interface Set, 244
Common Language Independent Data Types, 130
Common Language Independent Procedure Call Mechanism, 130
Common Management Information Protocol, 171, 176
Common Management Information Service, 176
Common Message Format, 113, 114
Common Operating Environment, 60
Compatibility, 40
Component, 21
Computer Graphics Interface, 213
Computer Graphics Metafile, 212
Computer Graphics Reference Model, 212
Conceptual Data Modeling Facility, 82
Conceptual Data Modelling Facility, 83
Conceptual Schema, 66, 81, 83
Confidential Encoding Rules, 132
Conformance Test Service, 190
Conformance Testing, 187
Connection-Oriented, 46
Connectionless-Oriented, 46
Copernicus, 392
Corporate Information Management, 383
Corporation for Open System, 189
COS, 295
COSAC, 288
COSINE, 295
CPCN, 378
CSNI, 316, 328
CSSCS, 389
CSWG, 50
DAPWG, 380
Data Compression, 221
Data Element Standardization, 91
Data Link Layer STANAGs, 336
Data Link Standards for NATO, 331
Data Management, 92
Database, 161
Database Services, 68
DCT, 396

DCW, 220
DDL, 66, 69
DDN, 385
Defence Fixed Telecommunications System, 380
Defense Data Network, 385
Defense Mapping Agency, 216
Defense Message System, 386
Defense-Wide Information Systems Security Program, 63
Degrees of Interoperability, 14
DER, 123, 132
DFR, 160, 207
DFTS, 380
DGIWG, 216
DIGEST, 216, 218
Digital Chart of the World, 220
Digital Geographic Information Exchange Standard, 216
Directory, 77, 83, 108, 117, 118, 119, 120, 121, 122, 123, 124, 135, 142, 161, 163, 166, 172, 182, 264, 270, 275, 289, 295, 314, 326, 381, 386, 387
Directory Services and Models, 118
Directory Standards, 119
DISNET, 168, 385
DISSP, 59
Distinguished Encoding Rules, 132
Distributed Applications, 96, 108, 159
Distributed Office Applications Model, 204
Distributed Processing, 173
DMF, 3, 18, 23
DML, 69
DMS, 386
DNS, 135
DOAM, 204
Document Application Profiles, 225
Document File and Retrieval, 207
Document Transfer and Manipulation, 206
DoD Trusted Computer System Evaluation Criteria, 168
DODIIS, 62
Domains, 66
DTAM, 160, 206, 207, 232
DTMP, 293, 308
DTMP/WG1, 308
ECMA, 167, 186, 250
EDI, 82, 96, 163, 205, 226
EDIFACT, 116, 205
Eight Military Features, 298
Eight Service Areas, 32
Electronic Data Interchange, 205
End-to-End Security Protocol, 154, 327
Ensemble, 20
EPHOS, 292
EPLRS, 389
ESPRIT, 114, 250, 256
Estelle, 191, 192
EUROCOM, 349
European Procurement Handbook for Open Systems, 292
EWOS, 39, 86, 117, 123, 186, 200, 231, 262, 273, 277, 283, 296, 310, 314, 321, 330, 345, 351
Extended ALS, 107
FAAD C2I, 388
FDDI, 140, 289
FDDI Follow-On LAN, 141
FDTs, 191
Fiber Distributed Digital Interface, 140
FIMS, 232, 237
Fixed/Mobile Segment, 63
FOD, 200
Form Interface Management System, 237
Formal Description Techniques, 191
Formal Methods in Conformance Testing, 188
FORMETS, 364
FORTRAN, 247
FTAM, 47, 108, 114, 115, 116, 117, 122, 124, 135, 157, 160, 187, 188, 206, 207, 208, 270, 275, 284, 285, 289, 293, 296, 312, 313, 314, 345, 364, 380, 400
FTAM Options and Profiles, 117
FTAM Standards, 114
FTP, 135
Functional Profiles, 306
G-LOTOS, 194
GAM-T-103, 348, 374
Generic Operating System Interface, 149
Geographic Document Architectures, 218
Geological Survey, 215
GKS, 190, 234, 239, 240, 248, 267, 268, 274, 275, 391
GNMP, 170, 267
Government Network Management Profile, 170
Graphical Data Exchange, 210
Graphical Information Product Exchange, 210
Graphical Kernel System, 239
GUI, 61, 235, 236
Guide to Open Systems Security, 154
HCI, 17
HEROS-2/1, 377
IAP, 263, 264
IEEE, 146, 261
IEPG, 251
IGES, 203, 206, 209, 210, 211, 267, 268, 275
IGOSS, 39, 294

IJMS, 363
Indexed Sequential Access Method, 150, 262
Industry/Government Open Systems Specification, 294
Information Models, 15
INTAP, 295
Integrated Communications Architecture, 60
Integrated Digital Network, 137
Integrated Services Digital Network, 137
Integrated Tactical-Strategic Demonstration Network, 169
Interchange Format and Presentation Profiles, 284
Interface Definition Notation, 128
Interfaces for Applications Portability, 263
INTERLISP, 248
International Standardized Profiles, 282
Internet, 134
Interoperability, 40
Interworking of Lower Layers in OSI, 103
IOFs, 4, 19, 26
IP, 134, 168, 396
IRD, 75
IRDS, 71, 75, 76, 77, 78, 79, 80, 81, 82, 84, 97, 98, 148, 160, 250, 253, 266, 268
ISDN, 38, 53, 60, 137, 138, 139, 183, 188, 269, 286, 301, 304, 311, 313, 314, 322, 323, 324, 325, 326, 327, 336
ISO, 35
ISO Development Environment, 295
ISO/IEC, 37
ISODE, 295
ISP, 161
ISPs, 282
ISWG, 50, 92, 93
ITDN, 169, 400
JBIG, 222
Job Transfer and Manipulation, 124
Joint Bi-Level Imaging Group, 222
Joint Photographic Experts Group, 222
JPEG, 222
JTC1, 37
JTIDS, 389
JTM, 117, 124, 125
KAPSE, 244
KBS, 253
Key Management Protocol, 166
Knowledge-Based Systems, 253
LENA-2, 362
Light Weight Encoding Rules, 132
Lightweight Protocols, 348
LISP, 247
Local Access Subsystem, 52
LOTOS, 191, 192
Lower Layer Addressing, 310
Lower Layer Security Model, 158
Lower Layer STANAGs, 306
LWER, 132
MACLISP, 248
Maneuver Control System, 388
Manufacturing Message Specification, 114
MAP, 114, 189, 294
MAPSE, 244
Marine Tactical Command and Control System, 391
MAS, 12
MCS, 388
Media Access Control, 103
Message Handling Standards, 111
Message Security Protocol, 166
MHS, 108, 111, 121, 127, 135, 142, 187, 275, 289, 313, 328, 329, 330, 345, 347, 369, 374, 375, 381
MHS-84, 111, 112, 113, 128, 142, 366, 368
MHS-88, 111, 113, 142
MIA, 276
MIDLA, 318, 331
MIDS, 331
MIDS Low Volume Terminal, 333
MILNET, 385
MMHS, 114, 141, 301, 312, 313, 314, 316, 329, 330, 331, 332, 333, 345, 346, 347
MMS, 114, 289
Mobile Hosts, 309
Mobile Subsystem, 52
MOTIF, 61, 62, 63, 228, 235, 236, 277
MOTIS, 111, 207
Moving Picture Experts Group, 222
MPDT, 102, 308, 313
MPEG, 222
MSE, 389
MSF, 4, 17, 19, 26
MSP, 166
MTACCS, 391
Multiendpoint Connection, 309
Multihoming, 309
Multipeer Data Transmission, 308
Multivendor Integration Architecture, 276
NACISA, 93, 94, 316, 347
NACISC Policy on Data Management, 92
NACMA, 362
NAOIW, 39, 120, 123, 167, 231, 281, 283, 289
National Security Agency, 165
National Transfer Format, 221
National Voluntary Laboratory Accreditation Program, 149

NATO C3 Architecture, 13, 50, 327
NATO C3 Master Plan, 50
NATO Geographic Conference, 220
NATO GOSIP, 293, 313
NATO Interconnected Information System, 92
NATO Maritime Operational Intelligence Support, 365
NATO Open Systems Interconnection Profiles, 302
NATO OSI Reference Model, 164
NATO OSI Security Architecture, 154, 327
NATO OSI STANAGs, 333
NATO Reference Model, 334
NATO Standardized Profile, 306
NATO Standardized Profiles, 293, 307
NATO Tactical Communications Architecture Post-2000, 52
NCCIS Architecture, 50
NDL, 69, 77, 78, 91, 97, 98
Network Independent Interface, 347
Network Layer Security Protocol, 154, 158, 327
Network Layer STANAGs, 337
Network Management Experts Group, 186
Network Management Forum, 186
Network Services, 109
NIAG SG6, 348
NIIF, 347
NILE, 331
NIMP, 40, 94, 297, 302, 303
NIST, 149, 167, 189, 213, 235, 250, 261, 264, 281
NLSP, 158
NMOS, 365
Non-Contact Information Systems Interface, 105
North American OSI Implementor's Workshop, 39
NOSA, 154, 164, 327
NOSIP, 302, 304, 306
NTIS Transition Strategy, 283, 304, 334, 348
Object-Oriented Database Task Group, 84
ODA, 161, 198, 225, 268
ODIF, 198, 267, 268
ODL, 198, 201, 225
ODP, 68, 88, 263
Office Document Architecture, 198
Open Distributed Processing, 88
OPEN LOOK, 228, 235, 236, 277
Open Software Foundation, 262, 274
Open Specifications, 40
Open System, 31, 40
Open System Environment, 40, 261
Open Systems Testing Consortium, 190
OPEN88, 151
Orange Book, 168, 169
OSCRL, 151
OSE, 277
OSF, 262
OSF/1 Operating System, 151
OSI Base Standards, 109
OSI Management, 173
OSI performance, 49
OSI Reference Model, 43, 101, 102, 170, 196
OSINET, 189
OSITOP, 276
Packed Encoding Rules, 132
Partitioned, Partially Replicated Database System, 66
Pascal, 192, 245
PCNCEP CIS Plan, 50
PCTE, 245, 250, 257, 268
PDIF, 275
PEDI, 206
PER, 132
Permanent Working Group, 9
PHIGS, 234, 240, 267, 268
Physical Layer STANAGs, 335
PICS Proforma, 191
Portability, 40
Portable Common Tools Interface Set, 251
POSI, 295
POSIX, 25, 34, 40, 61, 62, 64, 146, 147, 148, 149, 150, 151, 152, 154, 161, 163, 190, 195, 228, 248, 259, 260, 261, 262, 266, 268, 269, 272, 274, 277, 394, 396
POSIX Conformance Test Suite, 149
Post-2000 NATO Reference Model, 52
Precedence and Preemption, 310
Presentation Layer STANAGs, 344
Profile, 262
Profile Alignment Group for ODA, 200
Programmer's Hierarchical Interactive Graphics System, 240
Prolog, 257
Protocol Profile Conformance Testing Methodology, 188
PSDNs, 104
QoS, 170, 183, 184, 320
Quadrilateral Interoperability Programme, 5, 366
RDA, 160, 268, 289
RDT, 208
Real Time Transport Service, 374
Reference Model for Computer Graphics, 239
Reference Model for Data Management, 68
Referenced Data Transfer, 208
Regional Workshop Coordinating Committee, 39, 281

Registration Authorities, 195
Relay Profiles, 287
Reliable Transfer Service Element, 127
Remote Open Document Editing, 207
Remote Operations Service Element, 127
Remote Procedure Call, 128
RETINAT, 374
RITA, 376, 389
Robust Protocols Research Programme, 379
ROSE, 72, 108, 125, 127, 131, 207
RPC, 88, 125, 128
RTSE, 108, 125, 127
RTTS, 348, 374
SAFENET, 348
SANISI, 154, 164, 327
SAP, 48
SC18/WG1, 198, 204
SC18/WG4, 207, 208, 228
SC18/WG9, 228, 229
SC2/WG11, 222
SC2/WG12, 225
SC20/WG3, 155
SC21 WG5, 116
SC21/WG1, 102, 119, 142, 154, 156, 158, 159, 187, 188, 191, 192, 195, 196
SC21/WG3, 69, 74, 78, 79, 80, 81, 82, 83, 84, 87, 96, 154
SC21/WG4, 119, 120, 121, 122, 137, 170, 174, 175, 177, 178, 182, 186, 228, 264
SC21/WG5, 85, 86, 87, 116, 206, 208, 231, 232
SC21/WG6, 87, 106, 108, 129, 130, 154, 156, 162, 264, 276
SC21/WG7, 88, 89, 90
SC22/WG11, 129, 130, 249
SC22/WG14, 273
SC22/WG15, 148, 228, 283
SC22/WG18, 237
SC22/WG4, 273
SC6/WG2, 156, 158, 170
SC6/WG4, 156, 158, 170, 177
SC7/WG2, 228
SC7/WG3, 228
SC7/WG4, 81
Scalability, 40
SCF, 3, 18, 25
SD, 191
SD&IC, 361
SDCP, 48
SDL, 193
SDNS, 165
SDTS, 220
Secure Data Network System, 165
Security Activities, 327
Security Architecture for NATO Information Systems Interconnection, 327
Security Exchange Service Element, 162
Security Framework, 156, 157
Security Models, 156
Security Techniques, 156
Services, 29
Session Layer STANAGs, 343
SG11/PG6, 355
SG11/PG8, 355
SG11/WG2, 355
SG11/WG5, 355
SG12 AHWG on ATCCIS, 359
SG12/WG2, 357
SG9/WG1, 164, 305, 311, 335, 347
SG9/WG2, 113, 141, 142, 164, 185, 312, 313, 335
SG9/WG3, 316
SG9/WG4, 316, 331
SGFS, 36, 283
SGML, 198, 201, 225, 267, 268, 289
SHAPE Information Flow, 361
SICF, 376
SICP, 48
SIMNET, 218
SINCGARS, 389, 395
SMF, 3, 18, 26
SMTP, 135, 396
Software Engineering Environments, 250
SP3, 165
SP4, 165
SPAG, 189
SPARC, 91
Spatial Data Transfer Specification, 220
SQ, 70
SQL, 25, 61, 62, 64, 69, 70, 71, 72, 73, 74, 75, 77, 78, 79, 80, 82, 84, 97, 98, 148, 150, 160, 259, 262, 266, 268, 272, 273, 274, 277, 304, 380, 391
SQL2, 70, 74, 75, 84, 161
SQL3, 70, 71, 75, 84, 98
STAMINA, 113, 367
STANAG 4406, 312, 330
Standard for Interoperable LAN Security, 168
Standard Generalized Markup Language, 201
Standards for Applications Portability, 262
Standards Organizations, 35
STC, 94
STC Testbed Laboratory, 361
STEP, 71, 267, 268
Strategic Defense Initiative Office, 63

Structure of Management Information, 173, 175, 181
STUR, 375
SWG-EDI, 96, 163, 206
Systems Management, 175, 179
Systems Management Overview, 175
Systems Management Tutorial, 178
TAOM, 396
Taxonomy, 40
Taxonomy for International Standard Transport Profiles, 287
TC159/SC4/WG5, 229
TC184/SC5/WG1, 114
TC184/SC5/WG2, 137
TCP, 134, 396
TCS, 154, 164, 165
Technical and Office Protocol, 274
Telecommunication Management Network, 182
TELNET, 135, 396
Terminal Management, 232
TF, 3, 18, 25
Time Critical Communications Architecture, 320
Time Synchronization, 136
TLSP, 159
TM, 232, 237
TMN, 182
TOP, 274, 294
TP, 85, 161, 289
TPDU, 48
TRADACOMS, 205
Transaction Processing, 85
Transparent File Access, 148
Transport Layer Security Protocol, 154, 159
Transport Layer STANAGs, 341
Transport Profiles, 286
Tree and Tabular Combined Notation, 187
TRI-MNC C2 Plan, 50
Trusted Communications Sublayer, 154, 327
TSGCE SG11, 52, 350, 354
TSGCE SG12, 357
TSGCE SG9, 39, 49, 170, 297, 300, 303, 333, 350, 404
TTCN, 187
UCA, 294
UIMS, 17, 233, 235
UK GOSIP, 288
ULA, 90, 127
ULTDS, 396
UNIX System V Interface Definition, 150
Upper Layer Security Model, 156
US GOSIP, 268, 288, 292, 294
US/EUROCOM, 349
Use of OSI in NATO, 307
User Interface Reference Models, 235
Utility Communications Architecture, 294
VDT, 229
Vector Product Standard, 220
Versions and Extensibility, 107
Video Data Exchange, 223
Virtual Terminal, 230
Visual Display Terminal, 229
VME, 62, 63
VPS, 220
VT, 108, 135, 230, 289
WAM, 30, 57, 58, 59, 387
Wavell, 381
Wavell Enhancement System, 382
WDS, 381, 382
WES, 382
WHIDDS, 362
Wide Area Subsystem, 52
Workshop on Quality of Service, 185
Workshop on Security, 163
WRRE, 381
WWMCCS, 387
WWMCCS ADP Modernization, 57
X-Windows, 152, 233, 237, 268, 274
X/Open Portability Guide, 152
X/Open System V Specification, 150, 272
X/Windows, 274
XALS, 107
XTP, 348
XVT, 267
Z, 194
ZODIAC, 378

(This page intentionally left blank.)