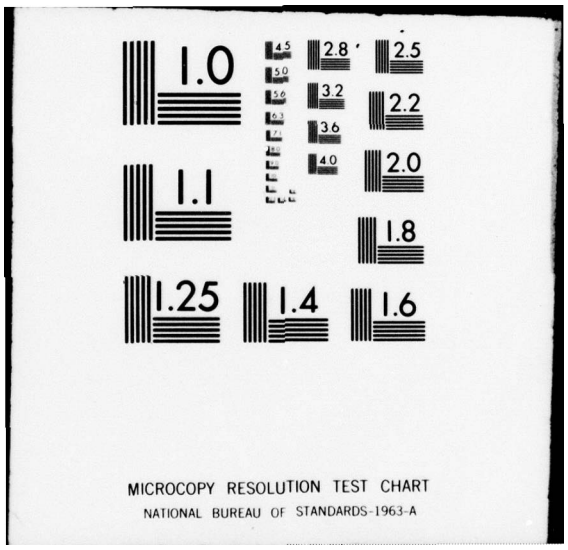
AD-A065 948 MICHIGAN UNIV ANN ARBOR DEPT OF INDUSTRIAL AND OPERA--ETC F/G 5/9
URL/URA TRAINING EXAMPLE.(U)
DEC 78
F19628-76-C-0197
UNCLASSIFIED ESD-TR-78-126 NL

1 OF 3
AD
A065948


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
8.0
9.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

ESD-TR-78-126

LEVEL II

12

URL/URA TRAINING EXAMPLE

ISDOS Project
University of Michigan
Department of Industrial & Operations Engineering
Ann Arbor, MI 48109

December 1978

AD A065948

DDC FILE COPY

DDC
RECEIVED
MAR 20 1979
C

Approved for Public Release;
Distribution Unlimited.

THIS DOCUMENT IS BEST QUALITY PRACTICABLE.
THE COPY FURNISHED TO DDC CONTAINED A
SIGNIFICANT NUMBER OF PAGES WHICH DO NOT
REPRODUCE LEGIBLY.

Prepared for

DEPUTY FOR TECHNICAL OPERATIONS
ELECTRONIC SYSTEMS DIVISION
HANSCOM AIR FORCE BASE, MA 01731

79 03 16 017

LEGAL NOTICE

When U. S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

OTHER NOTICES

Do not return this copy. Retain or destroy.

This Technical Report has been reviewed and is approved for publication.

Charles J. Hartman
CHARLES J. HARTMAN
Technology Applications Division

C. J. Grewe, Jr.
CHARLES J. GREWE, Jr., Lt Colonel, USAF
Chief, Technology Applications Division

FOR THE COMMANDER

Normand Michaud
NORMAND MICHAUD, Colonel, USAF
Director, Computer Systems Engineering
Deputy for Technical Operations

DISCLAIMER NOTICE

THIS DOCUMENT IS BEST QUALITY PRACTICABLE. THE COPY FURNISHED TO DDC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

(18) (19) REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER: ESD-TR-78-126	2. GOVT ACCESSION NO. / 3. RECIPIENT'S CATALOG NUMBER: (9) Technical Rept.
4. TITLE (and Subtitle): (6) URL/URA TRAINING EXAMPLE,	5. TYPE OF REPORT & PERIOD COVERED: Manual, Jan 1976 to June 1976.
	6. PERFORMING ORG. REPORT NUMBER: CDRL Item 007
7. AUTHOR(s): ISDOS Project	8. CONTRACT OR GRANT NUMBER(s): (15) F19628-76-C-0197
9. PERFORMING ORGANIZATION NAME AND ADDRESS: University of Michigan, Department of Industrial & Operations Engineering, Ann Arbor, Michigan 48109	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: (16) PE 64740F, Project 2237
11. CONTROLLING OFFICE NAME AND ADDRESS: (11) Deputy for Technical Operations, Electronic Systems Division, Hanscom AFB, MA 01731	12. REPORT DATE: December 1978
	13. NUMBER OF PAGES: 252
14. MONITORING AGENCY NAME & ADDRESS *(if different from Controlling Office)*: (12) 250p.	15. SECURITY CLASS. *(of this report)*: UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE: N/A

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for Public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Automated Tools	Requirements Analysis
Computer-Aided Design	Requirements Language
Information Processing	Requirements Specification
Information System Requirements	Specification Analysis

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This manual is used during formal training of the Computer-Aided Design and Specification Analysis Tool (CADSAT). A requirements definition of a computer information system is constructed in steps. Examples of the database construction and analysis reports are shown. This report is a part of a series of CADSAT reports that explain the User Requirements Language (URL) and User Requirements Analyzer (URA).

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

403 871

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

PREFACE

This manual is used during a formal five day training session. It describes the eight steps for developing a requirements definition of a computer information system. The database example is described in terms of URA version 3.0. Although the present version of the language is 3.3, the information described in this manual is upward compatible with 3.3. The example does not include some new reporting capability such as dynamic analysis, interval consistency, list changes, projected cost, resource consumption analysis, and security analysis. Refer to ESD Technical Report 78-130 and 78-131 for description of URL/URA Version 3.3.

A060517
A058629
A060780.

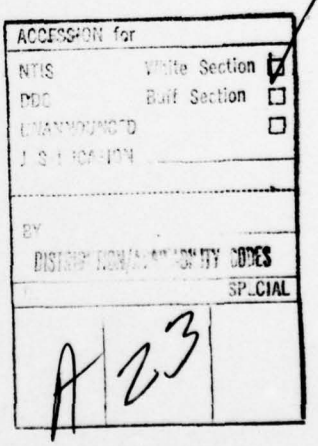


TABLE OF CONTENTS

	Page
INTRODUCTION	1
I. IDENTIFICATION OF URL SYNTAX ERRORS BY URA	3
II. SYSTEM FLOW DESCRIPTION	4
III. SYSTEM PROPERTIES DESCRIPTION	6
IV. SYSTEM STRUCTURE DESCRIPTION	7
V. DATA STRUCTURE DESCRIPTION	10
VI. DATA DERIVATION DESCRIPTION	12
VII. SYSTEM SIZE DESCRIPTION	13
VIII. SYSTEM DYNAMICS DESCRIPTION	14
IX. PROJECT MANAGEMENT DESCRIPTION	15
X. ADDITIONAL REPORT EXAMPLES	16
XI. TECHNIQUES FOR MODIFYING A URA DATA BASE	18
XII. ADDITIONAL EXAMPLES OF NEW NAME GENERATION FACILITY	19
APPENDIX	(see computer output page 21)

FIGURES

		Page
1.	Correspondence between URL User's Manual Topics and Input Files in Example	2
2.	System Diagram for Security Control System	5
3.	Second-Level Diagram for Security Control System	8

INTRODUCTION

The example described in this paper was selected for use as an aid in training Air Force personnel in the use of the User Requirements Language (URL) and User Requirements Analyzer (URA). It illustrates requirements definition for a security control system.

The purpose of the security control system is to allow users to access information for which they have a need and the necessary clearance, and to prevent unauthorized access. It must also allow security personnel to modify access privileges and to monitor system usage.

The example consists of a series of URL input files. Each contains information to be added to the data base containing all previous input. In this way, an incremental build-up of the system description in the URA data base is obtained.

Each input file illustrates a different aspect of the system description. This is useful for training purposes, but is not necessarily representative of the way in which a URA user would normally describe a system. In practice, the user should modify this scheme according to the needs of his own organization.

Each input file corresponds to a portion of Section 2 in the URL User's Manual, as shown in Figure 1. All the URL statements for a given aspect are contained in a single set of input. The As-Is Source Listing presents the contents of the input set, as input to URA. Following each As-Is Source Listing are several reports illustrating ways in which the information which exists in the data base at that point can be presented and analyzed.

In addition to the As-Is Source Listings and other reports mentioned above, the example contains As-Is Source Listings for input files containing syntax errors (pages 1-5) and reports produced as a result of URA commands which modify the data base (pages 207-217).

It should be noted that URA reports can be produced with various options. Not all of these are illustrated in the reports in this example. A description of all the options is given in the URL/URA User's Manual.

The remaining sections of this paper describe the various aspects of the example in more detail. The Appendix is the example itself, which consists of 223 pages of computer output.

79 03 16 047

Figure 1

Correspondence between URL User's Manual
Topics and Input Files in Example

Topic	Page numbers for As-Is Source Listing in example
1. System flow	6
2. System properties	14-16
3. System structure	23-26
4. Data structure	41-54
5. Data derivation	75-86
6. System size	96-99
7. System dynamics	109-112
8. *Project management*	123-125

I. IDENTIFICATION OF URL SYNTAX ERRORS BY URA (pages 1-5 of Appendix)

The example contains two As-Is Source Listings for URL input files containing syntax errors. These illustrate a number of errors that are detected by the Analyzer. A complete list of diagnostics is given in the URA User's Manual.

The URL statements in these files were input to URA using the UPDATE option, in order to show some of the errors which can be detected only by comparing input to information previously stored in the data base. This is not, in general, a good practice. Instead, the NOUPDATE option should be used for all input files which may contain syntax errors, in order to avoid the necessity of removing incorrect information from a URA data base. Once an input file has been checked by using the NOUPDATE option, the errors may be corrected and it may then be re-input using the UPDATE option to cause the data base to be modified.

II. SYSTEM FLOW DESCRIPTION (pages 6-13 of Appendix)

The system flow description should define the system boundaries. All inputs to and outputs from the system should be named, along with those people, organizations, other systems, etc., which are outside the system boundaries but which generate inputs to the system or receive outputs from the system. Data bases used by the system should also be named. Connections between the objects named as part of the system flow description should be described.

The system flow description for the Security Control System, in the Appendix, corresponds to the picture of the system shown in Figure 2. The dotted lines in the figure indicate the system boundary.

The system flow portion of the Appendix consists of the following reports:

As-is Source Listing with Cross Reference
Name Generation
Formatted Problem Statement
Process Picture
Interface Picture.

The As-Is Source Listing shows the URL system flow description, as input to URA. Since the UPDATE parameter was used, this information was used to update a URA data base, which was initially empty. The Cross Reference shows, for each name appearing in the As-Is Source Listing, the lines on which it appears.

Name Generation was used to produce a file containing all names in the URA data base. These names are listed, with their types, on the Name Generation report. This file of names was then used to produce a Formatted Problem Statement showing all information in the data base. This differs from the URL originally input, in that all complementary statements are shown.

Pictures are given to show graphically all relationships between security-control-system and security-control-interface and the other objects in the data base.

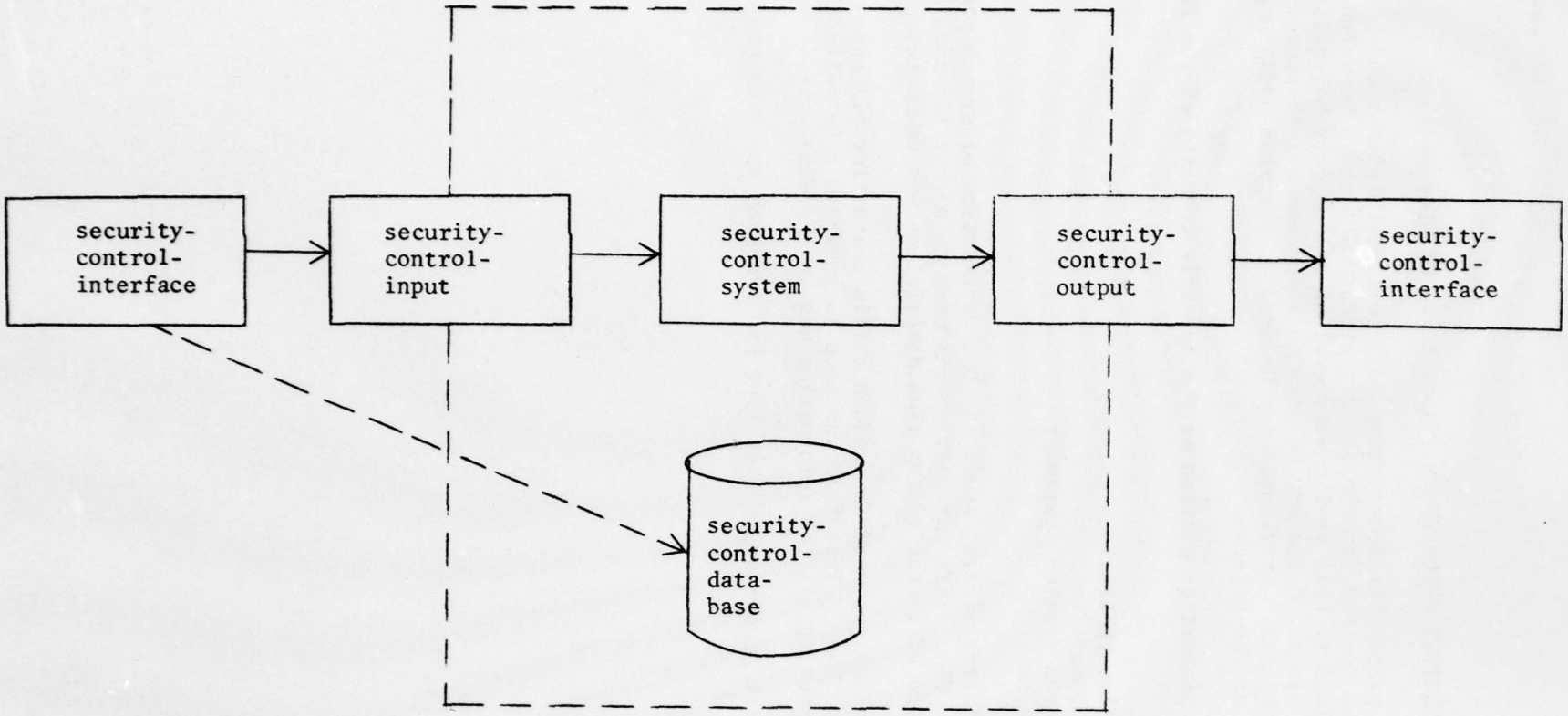


Figure 2

System Diagram for Security Control System

III. SYSTEM PROPERTIES DESCRIPTION (pages 14-22 of Appendix)

The system properties description adds text descriptions and any synonyms desired for the objects already defined. Keywords may be defined to help in the retrieval of all objects belonging to a given class. Memos may be used to make comments about certain groups of objects. Attributes may be used to describe additional properties of the objects.

The system properties portion of the Appendix consists of the following reports:

As-Is Source Listing
Name Generation
Formatted Problem Statement
Name List.

The As-Is Source Listing shows the URL description of system properties, as input to URA. This information was used to update the data base which existed after the system flow description was complete.

Name Generation was used to produce a file containing all names in the updated data base. This file was used to generate a Formatted Problem Statement showing all the information now in the data base.

The Name List report shows the type and synonyms for each name in the data base.

IV. SYSTEM STRUCTURE DESCRIPTION (pages 23-40 of Appendix)

The system structure description breaks the processing down into its major functions, and describes each of these with respect to system flow and system properties. Further information is given about data objects and their decomposition.

The system structure description for the example provides a good deal more detail about the security control system. This second-level description corresponds to the diagram in Figure 3. The names at the top and bottom of the diagram indicate the correspondence between Figure 2 (the top-level diagram) and Figure 3.

The following reports comprise the system structure portion of the Appendix:

- As-Is Source Listing
- Data Base Summary
- Process Structure
- Interface Structure
- Input Structure
- Output Structure
- Name Generation
- Formatted Problem Statement
- Name Generation
- Process Picture

The URL system structure description, as input to URA, is shown in the As-Is Source Listing. This information is added to the data base, which already contains the system flow and system properties descriptions.

The data base summary shows, for each type of name in the data base, the following:

- Number of names
- Number of names having synonyms
- Percentage of names having synonyms
- Number of names having descriptions
- Percentage of names having descriptions.

This is useful in evaluating the size and completeness of the data base.

Structure reports for the PROCESS security-control-system, the INTERFACE security-control-interface and the INPUT security-control-input show, in each case, how an object which is part of the top-level description of the problem is broken down into level-two objects.

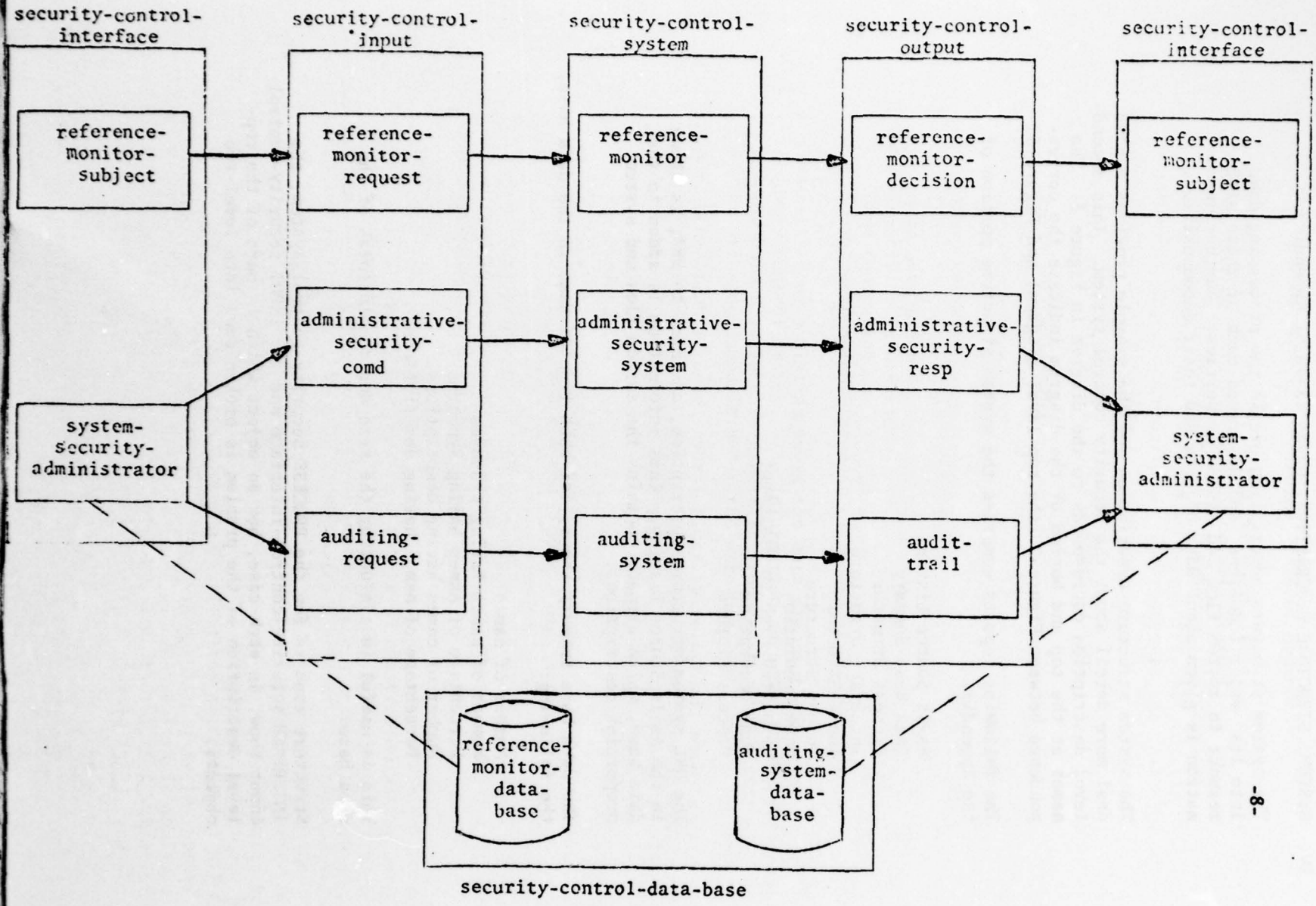


Figure 3

Second-Level Diagram for Security Control System

Name Generation is used to obtain all SET names from the data base, in order to obtain a Formatted Problem Statement for them.

Name Generation is used again to generate all PROCESSES, for use as input to the Picture report. The Picture reports for the PROCESSES now show both data flow information and structure information (PART, SUBPARTS).

V. DATA STRUCTURE DESCRIPTION (pages 41-74 of Appendix)

Each data base, input, or output belonging to the security control system must be described in more detail. Each is decomposed, through as many levels as necessary, into ELEMENTS. All resulting names are given descriptions and synonyms as necessary. All relationships between the objects are defined. The result is the data structure description of the system.

The data structure section in the Appendix consists of the following:

As-Is Source Listing
Data Base Summary
Name Generation
Contents with Index
Name Generation
Consists Comparison
Name Generation
Identifier Information
Name Generation
Formatted Problem Statement

The As-Is Source Listing shows the data structure description for the security control system. The information is added to the data base, and the Data Base Summary report is produced to give a current picture of the size and composition of the data base.

Name Generation is used several times to select all names of a given type for the Contents, Consists Comparison, Identifier Information, and Formatted Problem Statement reports. The use of Name Generation to produce input for another report should, by this time, need no further explanation.

The Contents report is produced for all OUTPUTS, to show the breakdown for each OUTPUT, stated via the CONTAINS statement.

An Index was produced for the Contents report to show, for each name appearing in the report, the pages on which it was used. This feature is available for many other reports.

The Consists Comparison report was produced for all INPUTS in the data base. To produce the report, a matrix is constructed having one row for each INPUT. Each ELEMENT which is CONTAINED in one or more of these INPUTS, either directly or several levels down, will have a column in the matrix. (Any GROUPS which appear at the lowest level will be treated in the same way as ELEMENTS.) As asterisk in the (I, J) entry of the matrix indicates that the ELEMENT represented by column J is contained, directly or indirectly, in the INPUT represented by row I. In the second matrix, each INPUT corresponds to one row and one column. The entry in position (I, I) gives the number of ELEMENTS in the INPUT corresponding to I. The (I, J) entry gives the number of elements in common between INPUTS I and J. This matrix is analyzed to determine, for each pair (I, J) of INPUTS, whether I is a subset of J (i.e., each ELEMENT contained in I is also contained in J), and whether

I and J are equivalent (i.e., consist of the same ELEMENTS). This information can then be used by the analyst to determine whether the data base contains multiple names for a single INPUT, and whether some INPUTS should be SUBPARTS of others. The same report could be produced using SET, OUTPUT, ENTITY, and GROUP names, as well as INPUT names.

The Identifier Information report was produced for all the ENTITIES in the data base. That report consists of a matrix connecting ENTITIES and ELEMENTS which IDENTIFY them, followed by counts for the number of ENTITIES IDENTIFIED by each ELEMENT and the number of ELEMENTS which IDENTIFY each ENTITY.

A Formatted Problem Statement follows which shows all the information in the data base for each RELATION.

VI. DATA DERIVATION DESCRIPTION (pages 75-95 of Appendix)

The data derivation description contains a much more detailed breakdown of the PROCESSES, and shows the ways in which various PROCESSES interact with data described in the data structure description to produce outputs.

This section of the Appendix shows the following:

- As-Is Source Listing
- Data Base Summary
- Name Generation
- Data Process Report
- Extended Picture

The URL input to describe data derivation is shown in the As-Is Source Listing. Once again, the data base is updated and the Data Base Summary report used to show the increase in available information.

The Data Process Report was produced with input consisting of all ELEMENTS in the data base. The result is a matrix showing the PROCESSES which USE or DERIVE each ELEMENT. The matrix is then used to find ELEMENTS which do not interact with any PROCESS and PROCESSES that have no inputs and/or outputs among the ELEMENTS. The Process Interaction Matrix is used to find PROCESSES with no predecessors and/or successors. The same report could be produced using any collection of SET, INPUT, OUTPUT, ENTITY, GROUP, and ELEMENT names.

The Extended Picture report was used to show data flow beginning at a specified PROCESS. Thus it shows all successors (direct or indirect) for that PROCESS, and all data objects used to determine predecessor-successor relationships.

VII. SYSTEM SIZE DESCRIPTION (pages 96-108 of Appe..dix)

A number of components of a system require size and volume description. For example, the frequency with which a PROCESS is performed, the values of an ELEMENT, and the size of a SET must all be described in this way. These, and similar information, are included in the system size description.

The following reports are included in this section of the Appendix:

As-Is Source Listing
Data Base Summary
Name Generation
Formatted Problem Statement
Name Generation
Formatted Problem Statement
Frequency Report

The As-Is Source Listing shows the URL input of system size information for our security control system example. The reader should note the use of SYSTEM-PARAMETERS to describe many quantifiable aspects of the system. A named SYSTEM-PARAMETER is essentially a variable representing some quantity which will be defined numerically later in the system design process, or which may vary.

Once again, the information shown in the As-Is Source Listing is added to the URA data base. The Data Base Summary reflects the continued growth of the data base.

Formatted Problem Statements are given for all SYSTEM-PARAMETERS and for all INTERVALS.

The Frequency Report shows, for a given INTERVAL, all objects which occur some number of times within that INTERVAL, along with the SYSTEM-PARAMETERS or integers which describe the frequency within the INTERVAL.

VIII. SYSTEM DYNAMICS DESCRIPTION (pages 109-122 of Appendix)

The system dynamics description deals with those aspects of the system which change over time. This includes EVENTS (which occur at instants of time), CONDITIONS (whose values may change over time), VOLATILITY (changeability) of ENTITIES and SETS, and the TRIGGERING of PROCESSES.

The following reports are included in the system dynamics section of the Appendix:

As-Is Source Listing
Data Base Summary
Process Chain
Name Generation
Formatted Problem Statement
Name Generation
Formatted Problem Statement

The URL system dynamics description is shown in the As-Is Source Listing. This URL was input and stored in the data base, after which a Data Base Summary was run to indicate changes in the amount of information in the data base.

The Process Chain report shows the sequence of PROCESSES and EVENTS that occur as a result of the specified EVENT.

Formatted Problem Statements show all information in the data base related to all EVENTS and CONDITIONS in the data base.

IX. PROJECT MANAGEMENT DESCRIPTION (pages 1 3-135 of Appendix)

The project management description includes information on the people describing the system, and those portions of the system which each described, security information for the system description, sources of information, and any related memos.

This section of the Appendix contains the following:

As-Is Source Listing
Data Base Summary
Name Generation
Formatted Problem Statement
Name Generation
Dictionary Report
Name Generation
Punched Comment Entries.

The As-Is Source Listing shows project management information added to the data base. The Data Base Summary reflects the final state of the data base, now that the security control system has been described.

Name Generation is used to obtain all MAILBOX, MEMO, and PROBLEM-DEFINER names from the data base, in order to produce a Formatted Problem Statement. The reader should especially note the use of OR in the SELECTION parameter for Name Generation.

Name Generation is also used to obtain all URL objects described by the PROBLEM-DEFINER james-m-amster. The Dictionary Report then gives description, synonym, keyword, and responsible problem definer for each of these.

The descriptions for all MEMOS in the data base were punched. The Punched Comment Entries report shows the information that is contained in the resulting file. The process of punching comment entries is useful in correcting errors in comment entries, as will be demonstrated later in this paper.

X. ADDITIONAL REPORT EXAMPLES (pages 136-206 of Appendix)

The following additional report examples make use of the information in the complete Security Control System data base:

Name List
Name Generation
Attribute Report
Process Structure
Name Generation
Formatted Problem Statement
Output Structure
Name Generation
Formatted Problem Statement
Input Structure
Name Generation
Formatted Problem Statement
Interface Structure
Name Generation
Formatted Problem Statement
Name Generation
Formatted Problem Statement
Name Generation
Formatted Problem Statement
Kwic Index
Consists Matrix Report
Process Input/Output

The Name List report lists all names in the data base, along with their types and synonyms.

Name Generation was used to generate all ATTRIBUTE names from the data base. The Attribute Report then shows, for each of these, those names which it APPLIES TO and the corresponding ATTRIBUTE-VALUES.

The following reports were obtained for all PROCESSES, OUTPUTS, INPUTS, and INTERFACES:

Structure
Name Generation
Formatted Problem Statement.

The reader should particularly note that all objects which are not part of larger objects appear at level one. This is useful in identifying names which have not yet been put into their proper places in the overall structure.

Formatted Problem Statements were also produced for all ENTITIES, ELEMENTS, and GROUPS in the system description.

The Kwic (Keyword in context) index is helpful in locating the names used to describe particular aspects of the target system and in identifying multiple names used to describe the same object.

The Consists Matrix shows, for each GROUP or ELEMENT, the GROUPS, ENTITIES, INPUTS, and OUTPUTS which CONTAIN it. This information is used to obtain counts of the number of objects which CONTAIN each GROUP or ELEMENT, and the number of GROUPS or ELEMENTS CONTAINED in each GROUP, ENTITY, INPUT, or OUTPUT. ENTITY, INPUT, and OUTPUT names may also be used as input to the Consists Matrix report.

The Process Input/Output report gives the DESCRIPTION and a full list of inputs and outputs for each PROCESS used as input to the command.

XI. TECHNIQUES FOR MODIFYING A URA DATA BASE (pages 207-217 of Appendix)

The following reports demonstrate various techniques for making modifications to the data base:

Change-Type Report
Rename Report
Deleted Comment Entries
Deletion
Replaced Comment Entries
Deleted URL
Formatted Problem Statement

Change-Type may be used to modify the type of a name that is already in the data base.

Rename may be used in a similar fashion to change a name. The new name must not, however, appear in the data base prior to the name change.

Delete-Comment-Entry may be used to remove specified comment-entries from the data base.

Replace-Comment-Entry replaces comment-entries currently in the data base with new ones. The reader should note that there is no way to edit comment-entries while they are a part of the data base; they may be altered only by replacement. Thus we can see the usefulness of Punch Comment Entry. It may be used to obtain a file of comment-entries for editing by the computer system editor. The edited comment-entries may then be re-input via Replace-Comment-Entry.

Delete-URL removes all relationships indicated in the URL used as input to the command. This is a "reversing" of the Input-URL process which adds information to the data base.

A Formatted Problem Statement is used to show the results of making the indicated changes to the security control system data base.

XII. ADDITIONAL EXAMPLES OF NEW NAME GENERATION FACILITY (pages 218-223 of Appendix)

Prior to July 1976, the Name Generation facility supplied with URA selected names such that each name satisfied one of the type parameters plus all of the additional selection parameters, such as SUB-PARTS-OF, KEY, and PD.

URA 3.0 allows more flexibility in specifying combinations of conditions for Name Generation. Legal values for the SELECTION parameter are discussed in the URA User's Manual. The examples in the Appendix illustrate some of the possibilities.

A. SELECTION='KEY=level-2 AND PROCESS' generates all PROCESSES appearing at the second level.

B. SELECTION=' (NOT PROCESS) * KEY=level-2' generates all second level names except PROCESSES.

C. SELECTION='ATTR=occurrences,unscheduled AND SO=security-control-input' chooses all subparts of security-control-input having unscheduled arrival times.

D. SELECTION='(INPUT OR OUTPUT) * ATTR=specder,implicit' selects all implicitly derived inputs and outputs.

E. SELECTION='SO=security-control-input OR SO=security-control-output' generates all subparts of either the input or the output specified.

APPENDIX

for

URL/URA Training Example

ISDOS Working Paper No. 156

by

Claudia R. Stallings
James M. Amster

ISDOS Research Project

Department of Industrial and Operations Engineering
The University Of Michigan
Ann Arbor, Michigan 48109
313/763-3469, 763-5329

This document was prepared for the Air Force Electronic Systems Division under Contract F19628-76-C-0197.

PRECEDING PAGE NOT FILMED
BLANK

PREFACE

This Appendix consists of User Requirements Analyzer (URA) reports for a security control system example. The example was designed for use in a five day course on the User Requirements Language (URL) and User Requirements Analyzer.

Because this output was intended for training purposes, it may not be useful by itself. The body of Working Paper No. 156 contains a description and short explanations of the material in the Appendix. Students in the URL/URA course will receive more detailed instruction in its use.

Table of Contents for URA Example

URA Report	Page
AS-IS SOURCE LISTING (for System Flow errors)	1
AS-IS SOURCE LISTING (for System Properties errors)	3
AS-IS SOURCE LISTING (for System Flow)	6
CROSS REFERENCE (for above)	7
NAME GENERATION (for all names)	8
FORMATTED PROBLEM STATEMENT	9
PICTURE (for security-control-system)	10
PICTURE (for security-control-interface)	12
AS-IS SOURCE LISTING (for System Properties)	14
NAME GENERATION (for all names)	17
FORMATTED PROBLEM STATEMENT	18
NAME LIST	22
AS-IS SOURCE LISTING (for System Structure)	23
DATA BASE SUMMARY	27
STRUCTURE (for PROCESSES)	28
STRUCTURE (for INTERFACES)	29
STRUCTURE (for INPUTS)	30
STRUCTURE (for OUTPUTS)	31
NAME GENERATION (for SET names)	32
FORMATTED PROBLEM STATEMENT	33
NAME GENERATION (for PROCESS names)	35
PICTURES	36
AS-IS SOURCE LISTING (for Data Structure)	41
DATA BASE SUMMARY	55
NAME GENERATION (for OUTPUT names)	56
CONTENTS REPORT	57
INDEX (to CONTENTS REPORT)	60
NAME GENERATION (for INPUT names)	62
CONSISTS COMPARISON REPORT	63
NAME GENERATION (for ENTITY names)	69
IDENTIFIER INFORMATION REPORT	70
NAME GENERATION (for RELATION names)	72
FORMATTED PROBLEM STATEMENT	73
AS-IS SOURCE LISTING (for Data Derivation)	75
DATA BASE SUMMARY	87
NAME GENERATION (for ELEMENT names)	88
DATA PROCESS REPORT	89
EXTENDED PICTURE (for create-access-relation)	94
AS-IS SOURCE LISTING (for System Size)	96
DATA BASE SUMMARY	100
NAME GENERATION (for SYSTEM-PARAMETERS)	101
FORMATTED PROBLEM STATEMENT	102
NAME GENERATION (for INTERVAL names)	105
FORMATTED PROBLEM STATEMENT	106
FREQUENCY REPORT	108
AS-IS SOURCE LISTING (for System Dynamics)	109
DATA BASE SUMMARY	113
PROCESS CHAIN (for occur-release-usage-attr-rel)	114
NAME GENERATION (for EVENT names)	117
FORMATTED PROBLEM STATEMENT	118
NAME GENERATION (for CONDITION names)	121
FORMATTED PROBLEM STATEMENT	122
AS-IS SOURCE LISTING (for Project Management)	123
DATA BASE SUMMARY	126
NAME GENERATION (for MEMO, MAILBOX and PROBLEM-DEFINER)	127

FORMATTED PROBLEM STATEMENT 128
NAME GENERATION (for PD=james-m-amster) 130
DICTIONARY REPORT 131
NAME GENERATION (for MEMO names) 133
PUNCHED COMMENT ENTRIES 134
NAME LIST ORDER=BYTYPE 136
NAME GENERATION (for ATTRIBUTE names) 142
ATTRIBUTE REPORT 143
STRUCTURE (for PROCESSES) 144
NAME GENERATION (for PROCESSES) 146
FORMATTED PROBLEM STATEMENT 147
STRUCTURE (for OUTPUTS) 161
NAME GENERATION (for OUTPUTS) 162
FORMATTED PROBLEM STATEMENT 163
STRUCTURE (for INPUTS) 170
NAME GENERATION (for INPUTS) 171
FORMATTED PROBLEM STATEMENT 172
STRUCTURE (for INTERFACES) 179
NAME GENERATION (for INTERFACES) 180
FORMATTED PROBLEM STATEMENT 181
NAME GENERATION (for ENTITIES) 183
FORMATTED PROBLEM STATEMENT 184
NAME GENERATION (for GROUPS and ELEMENTS) 187
FORMATTED PROBLEM STATEMENT 189
KWIC INDEX 197
CONSISTS MATRIX REPORT 199
PROCESS INPUT/OUTPUT (for delete-object) 206
CHANGE TYPE REPORT 207
RENAME REPORT 208
DELETED COMMENT ENTRIES 209
DELETION 210
REPLACED COMMENT ENTRIES 211
DELETED URL 212
FORMATTED PROBLEM STATEMENT 213
NAME GENERATION (for level 2 PROCESS names) 218
NAME GENERATION (for level 2 non PROCESS names) 219
NAME GENERATION (for unscheduled subparts of security-control-input) 220
NAME GENERATION (for INPUT or OUTPUT names whose specification-derivation is implicit) 221
NAME GENERATION (for subparts of security-control-input or security-control-output) 222

Security-control-example

A S - I S S O U R C E L I S T I N G

```
PARAMETERS FOR: SYNU

   SOURCE NOXREF UPDATE DBREF

  LINE  S T M T                                                    ID FIELD

     1 >  /* SCS system flow */
     2 >
     3 >  PROCESS:    security-control-system;
     4 >       RECIEVES:    security-control-input;
                                                  $
**** RECIEVES
     LEVEL  2,URA201:PLIST   : NAME NOT PART OF HEADER                    ****
                                                  $
**** LEVEL  2,URA011:STACK   : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING ****
                                                  $
**** LEVEL  1,URA020:RECOV   : LAST STATEMENT SKIPPED                     ****
     5 >       GENERATES:   security-control-output;
     6 >
     7 >  INPUT:     security-control-input;
     8 >
     9 >  OTPUT:    security-control-output;
                                                  $
**** OTPUT
     LEVEL  2,URA201:PLIST   : NAME NOT PART OF HEADER                    ****
     LAST ERROR OCCURRED ON LINE      4
                                                  $
**** LEVEL  2,URA011:STACK   : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING ****
                                                  $
**** LEVEL  1,URA020:RECOV   : LAST STATEMENT SKIPPED                     ****
    10 >
    11 >  INTERFACE:  system-administrators-and-subjects;
                                                  $
**** LEVEL  1,URA002:NLEX    : NAME TOO LONG                              ****
     LAST ERROR OCCURRED ON LINE      9
    12 >       GENERATED:   security-control-input;
                                                  $
**** LEVEL  2,URA266:ILLST   : ILLEGAL STATEMENT IN THIS SECTION          ****
     LAST ERROR OCCURRED ON LINE     11
    13 >       RECEIVES:    security-control-input;
                                                  $
```

A S - I S S O U R C E L I S T I N G

```
  LINE  S T M T                                                          ID FIELD

**** security-control-input
     LEVEL  2,URA202:NLIST   : NAME PREVIOUSLY USED DIFFERENTLY - IGNORED ****
     LAST ERROR OCCURRED ON LINE     12
    14 >
    15 >  SET:     security-control-data-base;
    16 >
        $
**** LEVEL  1,URA003:NLEX    : EOF NOT FOUND BEFORE END-OF-FILE          ****
     LAST ERROR OCCURRED ON LINE     13
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
PARAMETERS FOR: SYNU

   SOURCE NOXREF UPDATE DBREF

  LINE  S T M T                                                    TD FIELD

     1 >  /* SCS system properties */
     2 >
     3 >  PROCESS:    security-control-system;
     4 >       SYNONYM:    scs, scsys;
     5 >       DESCRIPTION;
     6 >                 The system will provide a means to allow users to pro< >cess    <
     7 >            information concurrently while providing
     8 >            reasonable assurance that no unauthorized release of
     9 >            information shall take place.  The security features must
    10 >            be an integral part of the operating system.  The
    11 >            contractor can assume that the physical installation
    12 >            will be secured to the highest level of information in
    13 >            the system.  ;
    14 >
    15 >  INPUT:      security-control-input;
    16 >       SYNONYM:    scinp;
    17 >       DESCRIPTION
    18 >                 The input to the security control system
                           ¶
**** LEVEL  2,URA011:STACK   : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING          ****
    19 >            consists of requests by users to access and
    20 >            modify information in the system and of commands
    21 >            by security personnel to monitor the system.  ;
                                                                   ¶
**** LEVEL  1,URA020:RECOV   : LAST STATEMENT SKIPPED                                     ****
     LAST ERROR OCCURRED ON LINE     18
    22 >
    23 >  OUTPUT:     security-control-output;
    24 >       SYNONYM:    scout;
    25 >       DESCRIPTION;
    26 >                 The system will produce outputs of several
    27 >            different types: approvals to data access or modification
    28 >            requests, audit trails on security features, a
    29 >            record of outputs produced, etc.  ;
    30 >
```

A S - I S S O U R C E L I S T I N G

```
  LINE  S T M T                                                          ID FIELD

    31 >  INTERFACE:  security-control-interface;
    32 >       SYNONYM:    scint,scout;
                                  $
**** scout
     LEVEL  2,URA205:SETSYN  : ALREADY SYNONYM FOR SOMETHING ELSE                ****
     LAST ERROR OCCURRED ON LINE     21
    33 >       PROCEDURE;
                        $
**** LEVEL  2,URA266:ILLST   : ILLEGAL STATEMENT IN THIS SECTION                 ****
     LAST ERROR OCCURRED ON LINE     32
    34 >                    There will be several different types of users
    35 >               generating requests on the system and retrieving
    36 >               data from it.  The security controls of the system
    37 >               must be capable of allowing users of different
    38 >               authorizations to process concurrently while preventing
    39 >               the release of information to unauthorized users.  :
    40 >
    41 >  SET:   security-control-data-base;
    42 >       SYNONYM: scdb,#1-file;
                                  $
**** LEVEL  1,URA007:SCAN    : ILLEGAL CHARACTER - IGNORED                       ****
     LAST ERROR OCCURRED ON LINE     33
                                    $
**** LEVEL  1,URA007:SCAN    : ILLEGAL CHARACTER - IGNORED                       ****
                                    $
**** LEVEL  2,URA011:STACK   : ILLEGAL SYMBOL PAIR - SYNTAX ERROR - START SKIPPING ****
                                    $
**** LEVEL  1,URA020:RECOV   : LAST STATEMENT SKIPPED                            ****
    43 >       DESCRIPTION;
    44 >                    The information in this set consists of all
    45 >               data stored and maintained by the security control
    46 >               system.
    47 >
    48 >  DEFINE:      level-1  KEYWORD;
    49 >       DESCRIPTION;
    50 >                    This keyword is given to the highest level
    51 >               objects in the scs description.  ;
    52 >       APPLIES:    scs,scinp,scout,scint,scdb;
                                    $
```

A S - I S S O U R C E L I S T I N G

```
  LINE  S T M T                                                    ID FIELD

**** LEVEL  2,URA266:ILLST   : ILLEGAL STATEMENT IN THIS SECTION          ****
     LAST ERROR OCCURRED ON LINE     42
    53 >
    54 >  EOF
```

Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE XREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS system flow */
   2 >
   3 >  PROCESS:    security-control-system;
   4 >       RECEIVES:    security-control-input;
   5 >       GENERATES:   security-control-output;
   6 >
   7 >  INPUT:      security-control-input;
   8 >
   9 >  OUTPUT:     security-control-output;
  10 >
  11 >  INTERFACE:  security-control-interface;
  12 >       GENERATES:   security-control-input;
  13 >       RECEIVES:    security-control-output;
  14 >
  15 >  SET:      security-control-data-base;
  16 >       RESPONSIBLE-INTERFACE:    security-control-interface;
  17 >
  18 >  EOP
```

Security-control-example

C R O S S R E F E R E N C E

SEQ	NAME	TYPE		
1	security-control-data-base	SET		
	15			
2	security-control-input	INPUT		
	4	7	12	
3	security-control-interface	INTERFACE		
	11	16		
4	security-control-output	OUTPUT		
	5	9	13	
5	security-control-system	PROCESS		
	3			

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ALL' ORDER=BYTYPE

1	security-control-input	INPUT
2	security-control-interface	INTERFACE
3	security-control-output	OUTPUT
4	security-control-system	PROCESS
5	security-control-data-base	SET

Security-control-example

FORMATTED PROBLEM STATEMENT

```
PARAMETERS FOR: PPS

   FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=70 CMARG=1 HMARG=40 DESG
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 INPUT                                  security-control-input;
    2     GENERATED BY:                     security-control-interface;
    3     RECEIVED BY:                      security-control-system;
    4
    5 INTERFACE                              security-control-interface;
    6     GENERATES:                        security-control-input;
    7     RECEIVES:                         security-control-output;
    8     RESPONSIBLE FOR:                  security-control-data-base;
    9
   10 OUTPUT                                 security-control-output;
   11     GENERATED BY:                     security-control-system;
   12     RECEIVED BY:                      security-control-interface;
   13
   14 PROCESS                                security-control-system;
   15     RECEIVES:                         security-control-input;
   16     GENERATES:                        security-control-output;
   17
   18 SET                                    security-control-data-base;
   19     RESPONSIBLE-INTERFACE IS:         security-control-interface;
   20
   21 EOF EOF EOF EOF EOF
```

PICTURE

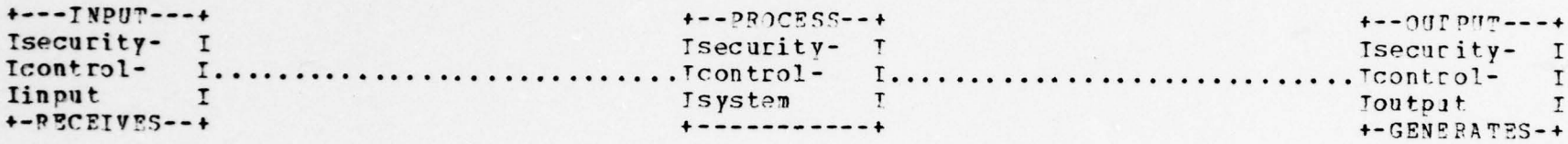
PARAMETERS FOR: PIC

NAME=security-control-system NOINDEX DATA STRUCTURE FLOW

Security-control-example

PROCESS PICTURE

security-control-system



PICTURE

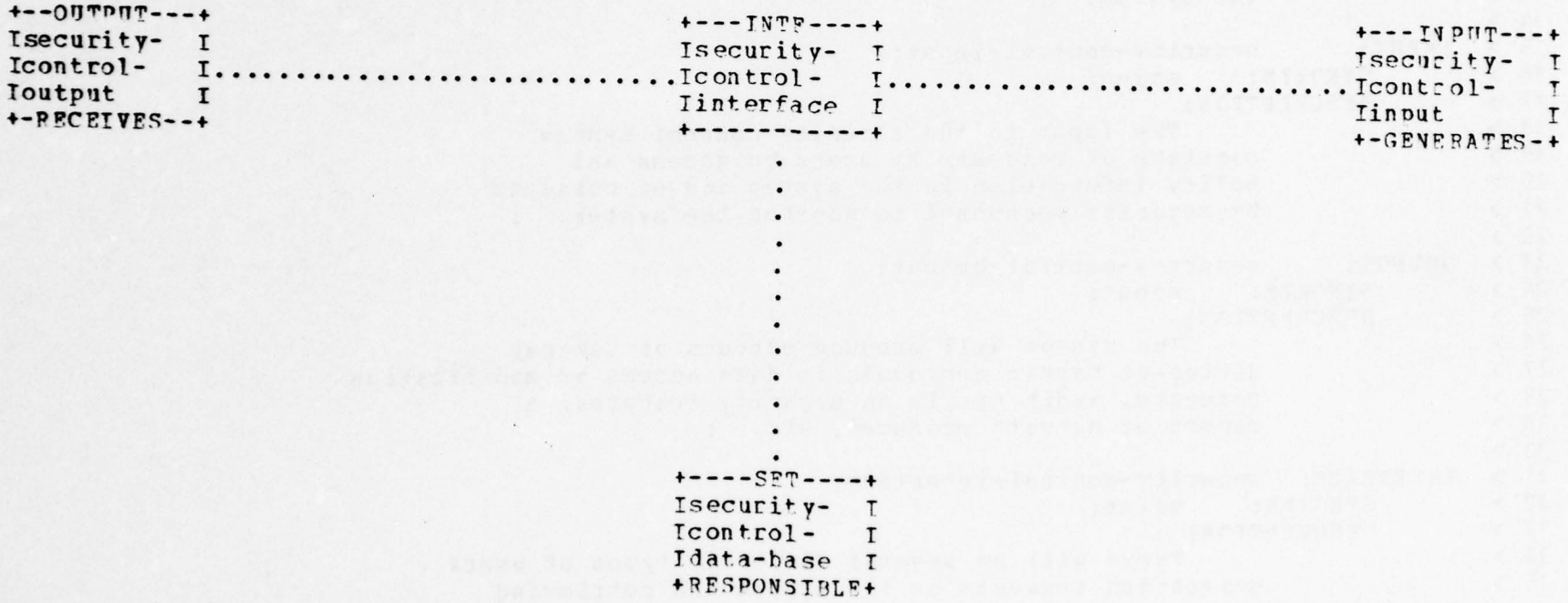
PARAMETERS FOR: PIC

NAME=security-control-interface NOINDEX DATA STRUCTURE FLOW

Security-control-example

INTERFACE PICTURE

security-control-interface



A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS system properties */
   2 >
   3 >  PROCESS:    security-control-system;
   4 >       SYNONYM:    scs, scsys;
   5 >       DESCRIPTION;
   6 >                 The system will provide a means to allow users to
   7 >            process information concurrently while providing
   8 >            reasonable assurance that no unauthorized release of
   9 >            information shall take place.  The security features must
  10 >            be an integral part of the operating system.  The
  11 >            contractor can assume that the physical installation
  12 >            will be secured to the highest level of information in
  13 >            the system.  ;
  14 >
  15 >  INPUT:      security-control-input;
  16 >       SYNONYM:    scinp;
  17 >       DESCRIPTION;
  18 >                 The input to the security control system
  19 >            consists of requests by users to access and
  20 >            modify information in the system and of commands
  21 >            by security personnel to monitor the system.  ;
  22 >
  23 >  OUTPUT:     security-control-output;
  24 >       SYNONYM:    scout;
  25 >       DESCRIPTION;
  26 >                 The system will produce outputs of several
  27 >            different types: approvals to data access or modification
  28 >            requests, audit trails on security features, a
  29 >            record of outputs produced, etc.  ;
  30 >
  31 >  INTERFACE:  security-control-interface;
  32 >       SYNONYM:    scint;
  33 >       DESCRIPTION;
  34 >                 There will be several different types of users
  35 >            generating requests on the system and retrieving
```

Security-control-example

A S - I S S O U R C E L I S I I N G

```
LINE  S T M T                                                    ID FIELD

  36 >              data from it.  The security controls of the system
  37 >              must be capable of allowing users of different
  38 >              authorizations to process concurrently while preventing
  39 >              the release of information to unauthorized users.  ;
  40 >
  41 >  SET:   security-control-data-base;
  42 >       SYNONYM: scdb;
  43 >       DESCRIPTION;
  44 >                    The information in this set consists of all
  45 >              data stored and maintained by the security control
  46 >              system.   ;
  47 >
  48 >
  49 >  DEFINE:      level-1  KEYWORD;
  50 >       DESCRIPTION;
  51 >                    This keyword is given to the highest level
  52 >              objects in the scs description.  ;
  53 >       APPLIES:    scs,scinp,scout,scint,scdb;
  54 >
  55 >  MEMO:        system-philosophy-memo;
  56 >       DESCRIPTION;
  57 >                    The philosophy of the secure computer system will
  58 >              be such that the system will control the various shared
  59 >              resources.  Hence the user will only be able to influence
  60 >              allocation decisions in a secondary way.  Specifically,
  61 >              he can ask for a resource but not control the absolute
  62 >              time or address of the resource.  It is essential that any
  63 >              other paths which might allow the user to access
  64 >              information (from any device) without the access controls
  65 >              of the system be eliminated.     ;
  66 >      APPLIES:     scs,scinp,scout,scint,scdb;
  67 >
  68 >  DEFINE       specification-derivation  ATTRIBUTE;
  69 >       SYNONYM:    specder;
  70 >       DESCRIPTION;
  71 >                    This attribute specifies whether a complete and
  72 >              explicit description of the object can be found in
  73 >              current documentation of the system or whether it
  74 >              must be derived from this documentation.  ;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  75 >
  76 >  PROCESS:    scs;
  77 >       ATTRIBUTE:  specder  explicit;
  78 >
  79 >  INPUT:      scinp;
  80 >       ATTRIBUTE:  specder  implicit;
  81 >
  82 >  OUTPUT:     scout;
  83 >       ATTRIBUTE:  specder  implicit;
  84 >
  85 >  INTERFACE:  scint;
  86 >       ATTRIBUTE:  specder  explicit;
  87 >
  88 >  SET:        scdb;
  89 >       ATTRIBUTE:  specder  implicit;
  90 >
  91 >  EOF
```

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ALL' ORDER=BYTYPE

1	specification-derivation	ATTRIBUTE
2	explicit	ATTRIBUTE-VALUE
3	implicit	ATTRIBUTE-VALUE
4	security-control-input	INPUT
5	security-control-interface	INTERFACE
6	level-1	KEYWORD
7	system-philosophy-memo	MEMO
8	security-control-output	OUTPUT
9	security-control-system	PROCESS
10	security-control-data-base	SET

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=79 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 DEFINE                                  specification-derivation
 2      AS A ATTRIBUTE;
 3  /* VALUES ARE:
 4       explicit FOR                      security-control-system,
 5       implicit FOR                      security-control-input,
 6       implicit FOR                      security-control-output,
 7       explicit FOR                      security-control-interface,
 8       implicit FOR                      security-control-data-base,
 9      */
10     SYNONYMS ARE:                       specder;
11     DESCRIPTION;
12                    This attribute specifies whether a complete and
13               explicit description of the object can be found in
14               current documentation of the system or whether it
15               must be derived from this documentation.;
16
17 DEFINE                                  explicit
18      AS A ATTRIBUTE-VALUE;
19
20 DEFINE                                  implicit
21      AS A ATTRIBUTE-VALUE;
22
23 INPUT                                   security-control-input;
24     SYNONYMS ARE:                       scinp;
25     DESCRIPTION;
26                    The input to the security control system
27               consists of requests by users to access and
28               modify information in the system and of commands
29               by security personnel to monitor the system.;
30     SEE-MEMO:                           system-philosophy-memo;
31     KEYWORDS:                           level-1;
32     ATTRIBUTES ARE:
33       specification-derivation          implicit;
34     GENERATED BY:                       security-control-interface;
35     RECEIVED BY:                        security-control-system;
36
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37 INTERFACE                              security-control-interface;
38     SYNONYMS ARE:                      scint;
39     DESCRIPTION;
40                     There will be several different types of users
41               generating requests on the system and retrieving
42               data from it.  The security controls of the system
43               must be capable of allowing users of different
44               authorizations to process concurrently while preventing
45               the release of information to unauthorized users.;
46     SEE-MEMO:                          system-philosophy-memo;
47     KEYWORDS:                          level-1;
48     ATTRIBUTES ARE:
49       specification-derivation         explicit;
50     GENERATES:                         security-control-input;
51     RECEIVES:                          security-control-output;
52     RESPONSIBLE FOR:                   security-control-data-base;
53
54 DEFINE                                level-1
55      AS A KEYWORD;
56     DESCRIPTION;
57                     This keyword is given to the highest level
58               objects in the scs description.;
59     APPLIES TO:                        security-control-system,
60                                        security-control-input,
61                                        security-control-output,
62                                        security-control-interface,
63                                        security-control-data-base;
64
65 MEMO                                   system-philosophy-memo;
66     DESCRIPTION;
67                     The philosophy of the secure computer system will
68               be such that the system will control the various shared
69               resources.  Hence the user will only be able to influence
70               allocation decisions in a secondary way.  Specifically,
71               he can ask for a resource but not control the absolute
72               time or address of the resource.  It is essential that any
73               other paths which might allow the user to access
74               information (from any device) without the access controls
75               of the system be eliminated.;
76     APPLIES TO:                        security-control-system,
77                                        security-control-input,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
                                        security-control-output,
                                        security-control-interface,
                                        security-control-data-base;

OUTPUT                                   security-control-output;
    SYNONYMS ARE:                       scout;
    DESCRIPTION;
                The system will produce outputs of several
            different types: approvals to data access or modification
            requests, audit trails on security features, a
            record of outputs produced, etc.;
    SEE-MEMO:                           system-philosophy-memo;
    KEYWORDS:                           level-1;
    ATTRIBUTES ARE:
      specification-derivation          implicit;
    GENERATED BY:                       security-control-system;
    RECEIVED BY:                        security-control-interface;

PROCESS                                  security-control-system;
    SYNONYMS ARE:                       scs,
                                        scsys;
    DESCRIPTION;
                The system will provide a means to allow users to
            process information concurrently while providing
            reasonable assurance that no unauthorized release of
            information shall take place.  The security features must
            be an integral part of the operating system.  The
            contractor can assume that the physical installation
            will be secured to the highest level of information in
            the system.;
    SEE-MEMO:                           system-philosophy-memo;
    KEYWORDS:                           level-1;
    ATTRIBUTES ARE:
      specification-derivation          explicit;
    RECEIVES:                           security-control-input;
    GENERATES:                          security-control-output;

SET                                      security-control-data-base;
    SYNONYMS ARE:                       scdb;
    DESCRIPTION;
                The information in this set consists of all
```

security-control-example

FORMATTED PROBLEM STATEMENT

```
119                data stored and maintained by the security control
120                system.;
121       SEE-MEMO:                          system-philosophy-memo;
122       KEYWORDS:                          level-1;
123       ATTRIBUTES ARE:
124         specification-derivation         implicit;
125       RESPONSIBLE-INTERFACE IS:          security-control-interface;
126
127 EOF EOF EOF EOF EOF
```

Security-control-example

NAME LIST

PARAMETERS FOR: NL

ORDER=ALPHA

	NAME	TYPE	SYNONYM	
1	explicit	ATTRIBUTE-VALUE		-
2	implicit	ATTRIBUTE-VALUE		-
3	level-1	KEYWORD		-
4	security-control-data-base	SET	scdb	
5	security-control-input	INPUT	scinp	
6	security-control-interface	INTERFACE	scint	
7	security-control-output	OUTPUT	scout	
8	security-control-system	PROCESS	scs	
			scsys	
9	specification-derivation	ATTRIBUTE	specder	
10	system-philosophy-memo	MEMO		-

Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS system structure */
   2 >
   3 >  PROCESS:    scs;
   4 >       SUBPARTS:   reference-monitor,
   5 >                   administrative-security-system,
   6 >                   auditing-system;
   7 >
   8 >  PROCESS:    reference-monitor;
   9 >       SYNONYM:    access-control-system, rmon;
  10 >       DESCRIPTION;
  11 >                   The system will provide controls which will allow
  12 >             users to operate concurrently while preventing the
  13 >             release of information to unauthorized users.  The
  14 >             system will also prevent inadvertent violation of need
  15 >             to know access to data. In addition to providing the
  16 >             primary access controls for this environment, the
  17 >             system will provide programs which perform subsidiary
  18 >             security control functions.
  19 >                  The capability must be provided for the system
  20 >             hardware to check the validity of all arguements
  21 >             utilized in calling the operating system.  ;
  22 >       RECEIVES:   reference-monitor-request;
  23 >       GENERATES:  reference-monitor-decision;
  24 >
  25 >  PROCESS:    administrative-security-system;
  26 >       SYNONYM:    admssys;
  27 >       DESCRIPTION;
  28 >                   The system will define the administrative
  29 >             functions of the system security administrator, and will
  30 >             support his responsibility for maintaining control of
  31 >             users id's, passwords, and user classification level and
  32 >             category set.  ;
  33 >       RECEIVES:   administrative-security-comd;
  34 >       GENERATES:  administrative-security-resp;
  35 >
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  36 >  PROCESS:    auditing-system;
  37 >       SYNONYM:    audsys;
  38 >       DESCRIPTION;
  39 >                   The system will provide an automatic capabilty to
  40 >             collect and record data regarding security related
  41 >             actions.  ;
  42 >       RECEIVES:   auditing-request;
  43 >       GENERATES:  audit-trail;
  44 >
  45 >  INPUT:          reference-monitor-request;
  46 >       SYNONYM:    rmonreq;
  47 >       DESCRIPTION;
  48 >                   These are requests to access or modify information
  49 >             in the system and may include output options.  ;
  50 >       ATTRIBUTE:  occurrences   unschedulel;
  51 >       PART OF:    security-control-input;
  52 >
  53 >  OUTPUT:         reference-monitor-decision;
  54 >       SYNONYM:    rmondec;
  55 >       DESCRIPTION;
  56 >                   These are decisions in answer  to the reference
  57 >             monitor subject's request and allow for read, write, or
  58 >             execute access to system information.  ;
  59 >       PART OF:    security-control-output;
  60 >
  61 >  INTERFACE:   reference-monitor-subject;
  62 >       SYNONYM:    rmonsub;
  63 >       DESCRIPTION;
  64 >                   A reference monitor subject may be a user, a
  65 >             process, or a job which generates requests on the
  66 >             reference monitor.  ;
  67 >       PART OF:    security-control-interface;
  68 >       RECEIVES:   reference-monitor-decision;
  69 >       GENERATES:  reference-monitor-request;
  70 >
  71 >  INPUT:          administrative-security-comd;
  72 >       SYNONYM:    admscom;
  73 >       DESCRIPTION;
  74 >                   These are commands necessary to the performance
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  75 >              of administrative security functions and will allow for
  76 >              the maintenance of the reference monitor data base.  ;
  77 >        ATTRIBUTE:  occurrences   unscheduled;
  78 >        PART OF:    security-control-input;
  79 >
  80 >  OUTPUT:           administrative-security-resp;
  81 >        SYNONYM:    admsres;
  82 >        DESCRIPTION;
  83 >                    These are responses to administrative security
  84 >              commands and will consist of validations as to
  85 >              the execution of these commands.  ;
  86 >        PART OF:    security-control-output;
  87 >
  88 >  INTERFACE:        system-security-administrator;
  89 >        SYNONYM:    ssadm,ssa;
  90 >        DESCRIPTION;
  91 >                    The system security administrator will have the
  92 >              responsibility of receiving and reviewing audit data
  93 >              contained in the auditing system data base and
  94 >              performing administrative functions dealing with the
  95 >              initiation and maintenance of system subject and object
  96 >              information contained in the reference monitor data
  97 >              base.          ;
  98 >        PART OF:    security-control-interface;
  99 >        GENERATES:  administrative-security-cond;
 100 >        RECEIVES:   administrative-security-resp;
 101 >        GENERATES:  auditing-request;
 102 >        RECEIVES:   audit-trail;
 103 >
 104 >  INPUT:            auditing-request;
 105 >        SYNONYM:    audreq;
 106 >        DESCRIPTION;
 107 >                    These are requests to view audit data stored in
 108 >              the auditing system data base by the reference
 109 >              monitor.  ;
 110 >        ATTRIBUTE:  occurrences   scheduled;
 111 >        PART OF:    security-control-input;
 112 >
 113 >  OUTPUT:           audit-trail;
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 114 >        SYNONYM:    audtra;
 115 >        DESCRIPTION;
 116 >                    Security audit trails should contain records of
 117 >               each security incident, and may contain other data
 118 >               as well.  ;
 119 >        PART OF:    security-control-output;
 120 >
 121 >  SET:              scdb;
 122 >        SUBSETS ARE:    reference-monitor-data-base,
 123 >                    auditing-system-data-base;
 124 >
 125 >  SET:               reference-monitor-data-base;
 126 >        SYNONYM:    rmondb;
 127 >        DESCRIPTION;
 128 >                    The information in this set consists of user access
 129 >               data, object sensitivity, need-to-know, etc.  This
 130 >               information is generated by the system security
 131 >               administrator and users given permission.  ;
 132 >        RESPONSIBLE-INTERFACE:    system-security-administrator;
 133 >
 134 >  SET:              auditing-system-data-base;
 135 >        SYNONYM:    audsysdb;
 136 >        DESCRIPTION;
 137 >                    The system audit functions should provide a
 138 >               history of normal and abnormal system use, or
 139 >               operation, to permit regular security review of
 140 >               system activity.  ;
 141 >        RESPONSIBLE-INTERFACE:  system-security-administrator;
 142 >
 143 >  DEFINE:           level-2  KEYWORD;
 144 >        DESCRIPTION;
 145 >                    This keyword is given to the second highest
 146 >               level in the scs description.  ;
 147 >        APPLIES: rmonsub,rmonreq,rmon,rmondec,
 148 >                    ssadm,admscom,admssys,admsres,
 149 >                    audreq,audsys,audtra,rmondb,audsysdb;
 150 >
 151 >  EOF
```

Security-control-example

DATA BASE SUMMARY

	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE	2	1	50.00	1	50.00
ATTRIBUTE-VALUE	4	0		0	
INPUT	4	4	100.00	4	100.00
KEYWORD	2	0		2	100.00
MEMO	1	0		1	100.00
OUTPUT	4	4	100.00	4	100.00
PROCESS	4	4	100.00	4	100.00
INTERFACE	3	3	100.00	3	100.00
SET	3	3	100.00	3	100.00
** TOTAL **	27	19	70.37	22	81.48

Security-control-example

PROCESS STRUCTURE

PARAMETERS FOR: STR

PROCESS INDENT=3 NOINDEX

COUNT	LEVEL	NAME
1	1	security-control-system
2	2	reference-monitor
3	2	administrative-security-system
4	2	auditing-system

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	3						

Security-control-example

INTERFACE STRUCTURE

PARAMETERS FOR: STR

INTERFACE INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 security-control-interface
    2      2   reference-monitor-subject
    3      2   system-security-administrator
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	2						

Security-control-example

INPUT STRUCTURE

PARAMETERS FOR: STR

INPUT INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 security-control-input
    2      2   reference-monitor-request
    3      2   administrative-security-comd
    4      2   auditing-request
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	3						

Security-control-example

OUTPUT STRUCTURE

PARAMETERS FOR: STR

OUTPUT INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 security-control-output
    2      2   reference-monitor-decision
    3      2   administrative-security-resp
    4      2   audit-trail
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	3						

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='SET' ORDER=BYTYPE

1	auditing-system-data-base	SET
2	reference-monitor-data-base	SET
3	security-control-data-base	SET

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: PPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=70 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 SET                                    auditing-system-data-base;
 2     SYNONYMS ARE:                      audsysdb;
 3     DESCRIPTION;
 4                 The system audit functions should provide a
 5           history of normal and abnormal system use, or
 6           operation, to permit regular security review of
 7           system activity.;
 8     KEYWORDS:                          level-2;
 9     SUBSET OF:                         security-control-data-base;
10     RESPONSIBLE-INTERFACE IS:          system-security-administrator;
11
12 SET                                    reference-monitor-data-base;
13     SYNONYMS ARE:                      rmondb;
14     DESCRIPTION;
15                 The information in this set consists of user access
16           data, object sensitivity, need-to-know, etc.  This
17           information is generated by the system security
18           administrator and users given permission.;
19     KEYWORDS:                          level-2;
20     SUBSET OF:                         security-control-data-base;
21     RESPONSIBLE-INTERFACE IS:          system-security-administrator;
22
23 SET                                    security-control-data-base;
24     SYNONYMS ARE:                      scdb;
25     DESCRIPTION;
26                 The information in this set consists of all
27           data stored and maintained by the security control
28           system.;
29     SEE-MEMO:                          system-philosophy-memo;
30     KEYWORDS:                          level-1;
31     ATTRIBUTES ARE:
32       specification-derivation         implicit;
33     SUBSETS ARE:                       reference-monitor-data-base,
34                                        auditing-system-data-base;
35     RESPONSIBLE-INTERFACE IS:          security-control-interface;
36
```

Security-control-example

FORMATTED PROBLEM STATEMENT

37 EOF EOF EOF EOF EOF

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='PROCESS' ORDER=BYTYPE

1	administrative-security-system	PROCESS
2	auditing-system	PROCESS
3	reference-monitor	PROCESS
4	security-control-system	PROCESS

PICTURE

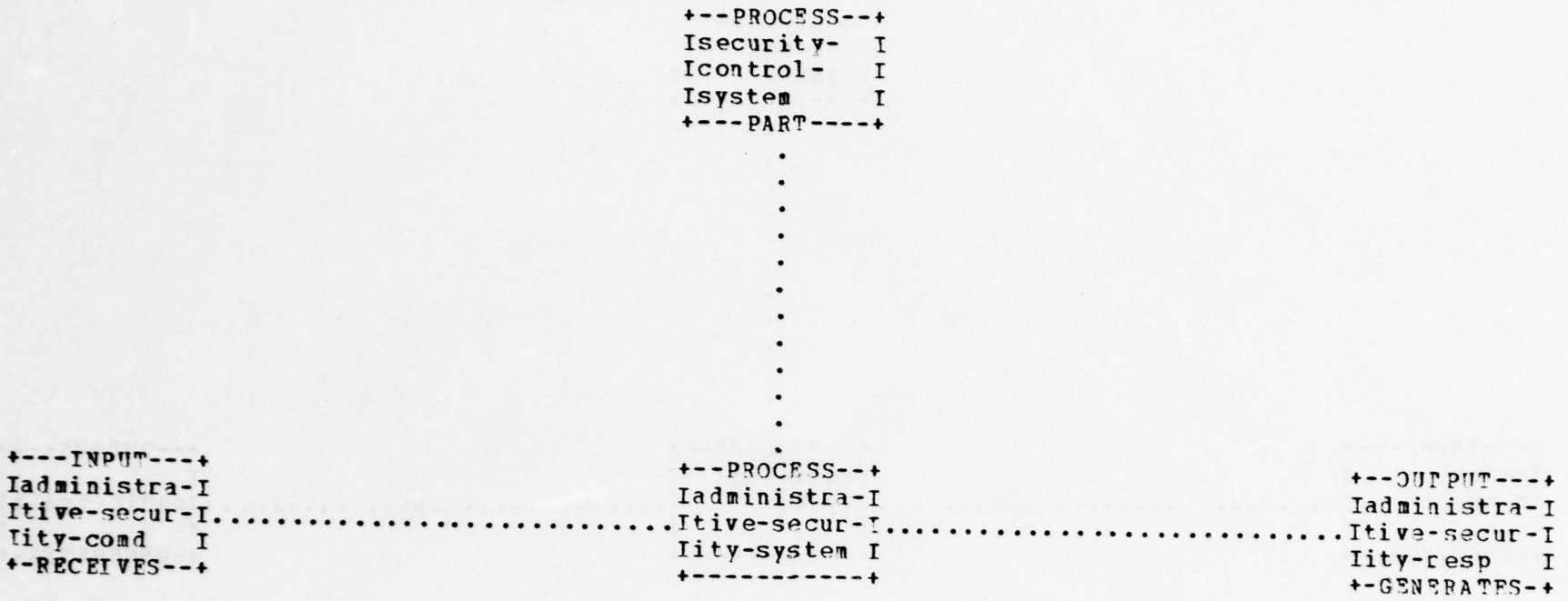
PARAMETERS FOR: PIC

FILE NOINDEX DATA STRUCTURE FLOW

Security-control-example

PROCESS PICTURE

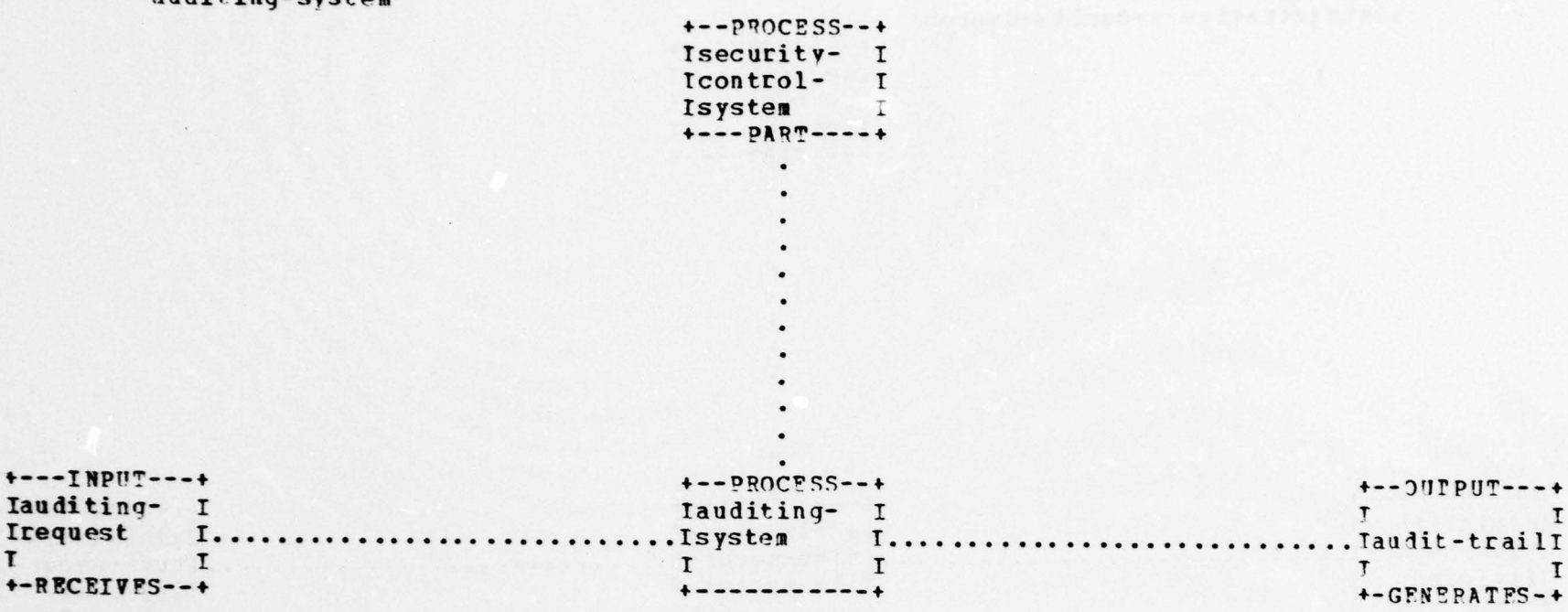
administrative-security-system



Security-control-example

PROCESS PICTURE

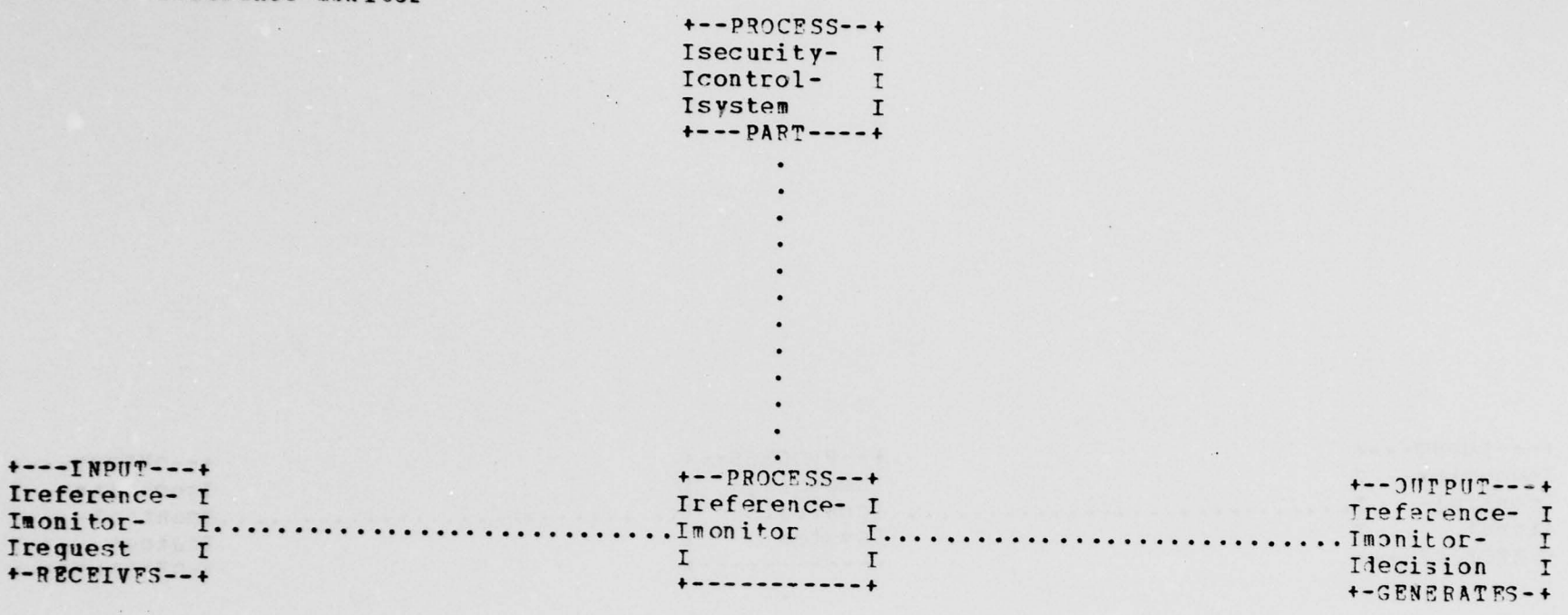
auditing-system



Security-control-example

PROCESS PICTURE

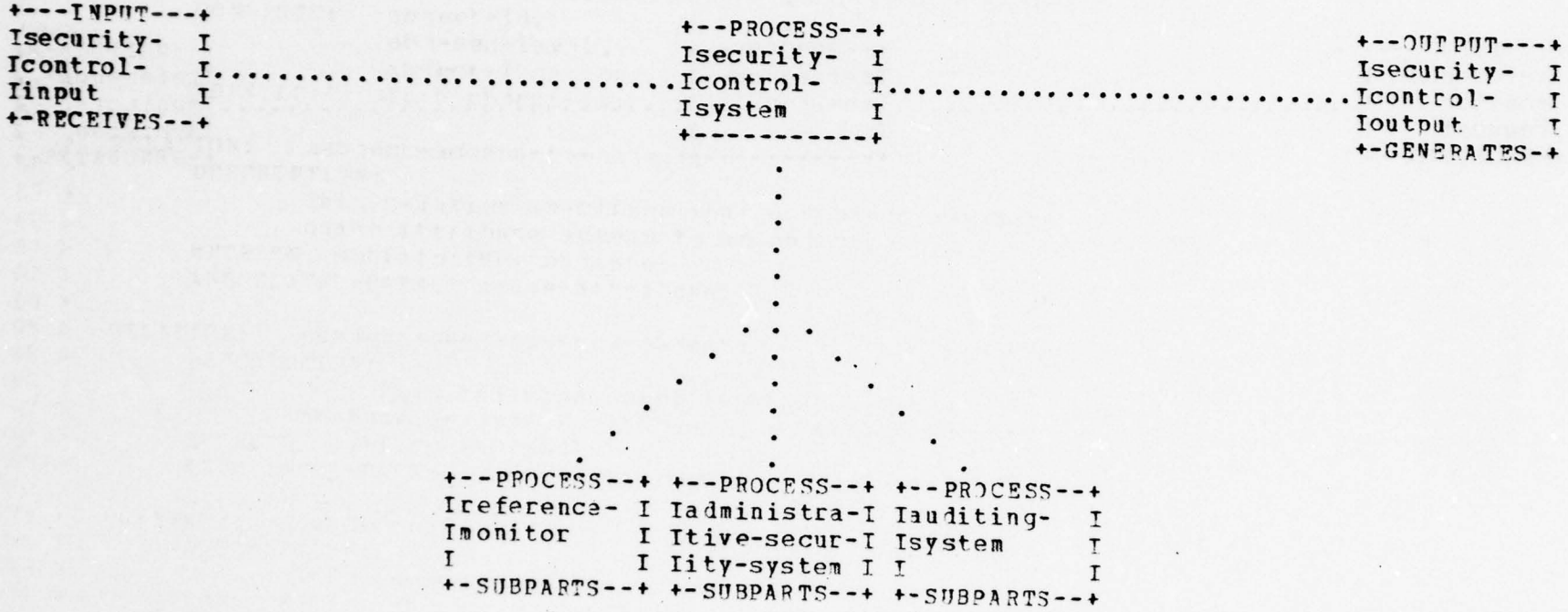
reference-monitor



Security-control-example

PROCESS PICTURE

security-control-system



Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS data structure */
   2 >
   3 >  /* Reference Monitor Data Base */
   4 >
   5 >  SET:        reference-monitor-data-base;
   6 >       SUBSETS:    top-secret-file,secret-file,confidential-file,
   7 >                   unclassified-file;
   8 >       SUBSETTING-CRITERIA:   sub-curr-sec-level,obj-sec-level;
   9 >
  10 >  SET:        top-secret-file;
  11 >       SYNONYM:    topsecfile;
  12 >       DESCRIPTION;
  13 >                   This file contains occurrences of subject and object
  14 >             information which have top secret security levels.  ;
  15 >       CONSISTS:   subject-information, object-information;
  16 >
  17 >  SET:        secret-file;
  18 >       SYNONYM:    secfile;
  19 >       DESCRIPTION;
  20 >                   This file contains occurrences of subject and object
  21 >             information which have secret security levels.  ;
  22 >       CONSISTS:   subject-information, object-information;
  23 >
  24 >  SET:        confidential-file;
  25 >       SYNONYM:    confile;
  26 >       DESCRIPTION;
  27 >                   This file contains occurrences of subject and object
  28 >             information which have confidential security levels. ;
  29 >       CONSISTS:   subject-information, object-information;
  30 >
  31 >  SET:        unclassified-file;
  32 >       SYNONYM:    uncfile;
  33 >       DESCRIPTION;
  34 >                   This file contains occurrences of subject and object
  35 >             information which have unclassified security levels. ;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  36 >       CONSISTS:   subject-information, object-information;
  37 >
  38 >  ENTITY:     subject-information;
  39 >       SYNONYM:    subinfo;
  40 >       DESCRIPTION;
  41 >                   This information holds identification and
  42 >             security data about a reference monitor subject. ;
  43 >       CONSISTS:   subject-id,
  44 >                   sub-max-sec-level,
  45 >                   sub-curr-sec-level;
  46 >
  47 >  ENTITY:     object-information;
  48 >       SYNONYM:    objinfo;
  49 >       DESCRIPTION;
  50 >                   This information holds identification, security,
  51 >             and location information for a particular object.  ;
  52 >       CONSISTS:   object-id,
  53 >                   obj-sec-level,
  54 >                   object-location;
  55 >       IDENTIFIED BY:   object-id;
  56 >
  57 >  RELATION:   subject-access-to-object;
  58 >       DESCRIPTION;
  59 >             This relation specifies that a subject may have
  60 >             usage attribute access to an object.  ;
  61 >       BETWEEN  subinfo AND  objinfo;
  62 >       ASSOCIATED-DATA:  usage-attribute;
  63 >
  64 >  RELATION:   subject-need-to-know-object;
  65 >       DESCRIPTION;
  66 >                   This relation specifies that a subject has a need
  67 >             to know an object with usage attribute access.  ;
  68 >       BETWEEN  subinfo AND objinfo;
  69 >       ASSOCIATED-DATA:   usage-attribute;
  70 >
  71 >  ELEMENT:    subject-id;
  72 >       DESCRIPTION;
  73 >             This is a unique identifier for a subject.  ;
  74 >       IDENTIFIES:  subject-information;
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  75 >
  76 >  ELEMENT:    object-id;
  77 >       DESCRIPTION;
  78 >                 This is a unique identifier for an object.  ;
  79 >
  80 >
  81 >  ELEMENT:    usage-attribute;
  82 >       DESCRIPTION;
  83 >                 This specifies the type of usage, that is
  84 >            read, write, or execute, that a subject may have of an
  85 >            object.  ;
  86 >
  87 >  ELEMENT:    decision-type;
  88 >       DESCRIPTION;
  89 >                 This is the affirmative or negative decision to
  90 >            a subject's request.  ;
  91 >
  92 >
  93 >  ELEMENT:         requesting-subject-id,
  94 >                   receiving-subject-id,
  95 >                   error-code;
  96 >
  97 >  GROUP:      sub-max-sec-level;
  98 >       DESCRIPTION;
  99 >                 This is the maximum security level for a subject. ;
 100 >       CONSISTS:   classification-level,
 101 >                   category-set;
 102 >
 103 >  GROUP:      sub-curr-sec-level;
 104 >       DESCRIPTION;
 105 >                 This is the current security level for a subject. ;
 106 >       CONSISTS:   classification-level,
 107 >                   category-set;
 108 >
 109 >  GROUP:      obj-sec-level;
 110 >       DESCRIPTION;
 111 >                 This is the security level for an object. ;
 112 >       CONSISTS:   classification-level,
 113 >                   category-set;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 114 >
 115 >  ELEMENT:    object-location;
 116 >       DESCRIPTION;
 117 >                    This is a pointer to the actual object which
 118 >              contains the information of interest to a subject and
 119 >              which exists outside the security control system.   ;
 120 >
 121 >  ELEMENT:    classification-level;
 122 >       DESCRIPTION;
 123 >                    This is a level of classification which may
 124 >              range up from unclassified to top secret and may be
 125 >              owned by a subject or an object.   ;
 126 >
 127 >  ELEMENT:    category-set;
 128 >       DESCRIPTION;
 129 >                     This is a set of categories of information which
 130 >            may be owned by a subject  or an object.  ;
 131 >
 132 >  /* Auditing System Data Base */
 133 >
 134 >  ENTITY:     incident-information;
 135 >       SYNONYM:    incinfo;
 136 >       DESCRIPTION;
 137 >                    This information holds data about where and
 138 >              when an incident has occurred.  ;
 139 >       CONTAINED IN:   audsysdb;
 140 >       CONSISTS:   date-time,
 141 >                   consol-nr,
 142 >                   incident-type;
 143 >
 144 >  RELATION:   sub-inc-audit-relation;
 145 >       DESCRIPTION;
 146 >                    This relates a subject to an audit incident
 147 >              which he has caused by trying to access objects via the .
 148 >              reference monitor.   ;
 149 >       BETWEEN  subinfo  AND  incinfo;
 150 >
 151 >  RELATION:   sub-obj-audit-relation;
 152 >       DESCRIPTION;
```

A S - T S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 153 >                    This relates a subject to an object with which
 154 >               he has caused audit incidents by trying to access
 155 >               the object via the reference monitor.  ;
 156 >         BETWEEN  subinfo  AND objinfo;
 157 >
 158 >  RELATION:   obj-inc-audit-relation;
 159 >         DESCRIPTION;
 160 >                    This relates an object to an incident in which
 161 >               subjects tried to access this object via the reference
 162 >               monitor.  ;
 163 >         BETWEEN:   objinfo  AND  incinfo;
 164 >
 165 >  ELEMENT:    incident-type;
 166 >         DESCRIPTION;
 167 >                    This specifies the type of audit incident which
 168 >               has occurred.   ;
 169 >
 170 >  ELEMENT:    date-time;
 171 >         DESCRIPTION;
 172 >                    This is the date and time an audit incident
 173 >               occurred.     ;
 174 >
 175 >  ELEMENT:    consol-nr;
 176 >         DESCRIPTION;
 177 >                    This is the number of the console at which the audit
 178 >                incident occurred.   ;
 179 >
 180 >
 181 >  ELEMENT:    security-id;
 182 >         DESCRIPTION;
 183 >                    This uniquely identifies the system security
 184 >               administrator.  ;
 185 >
 186 >  ELEMENT:    validation-code;
 187 >         DESCRIPTION;
 188 >                    This is a validation of a command issued by
 189 >               the system security administrator.   ;
 190 >
 191 >
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 192 >  /* Reference Monitor Input/Output */
 193 >
 194 >  INPUT:       get-read-request;
 195 >       SYNONYM:     kf1req;
 196 >       PART OF:     reference-monitor-request;
 197 >       CONSISTS:    subject-id,
 198 >                    object-id,
 199 >                    usage-attribute;
 200 >
 201 >  OUTPUT:      get-read-decision;
 202 >       SYNONYM:     kf1dec;
 203 >       PART OF:     reference-monitor-decision;
 204 >       CONSISTS:    decision-type;
 205 >
 206 >  INPUT:       get-write-request;
 207 >       SYNONYM:     kf2req;
 208 >       PART OF:     reference-monitor-request;
 209 >       CONSISTS:    subject-id,
 210 >                    object-id,
 211 >                    usage-attribute;
 212 >
 213 >  OUTPUT:      get-write-decision;
 214 >       SYNONYM:     kf2dec;
 215 >       PART OF:     reference-monitor-decision;
 216 >       CONSISTS:    decision-type;
 217 >
 218 >  INPUT:       get-execute-request;
 219 >       SYNONYM:     kf3req;
 220 >       PART OF:     reference-monitor-request;
 221 >       CONSISTS:    subject-id,
 222 >                    object-id,
 223 >                    usage-attribute;
 224 >
 225 >  OUTPUT:      get-execute-decision;
 226 >       SYNONYM:     kf3dec;
 227 >       PART OF:     reference-monitor-decision;
 228 >       CONSISTS:    decision-type;
 229 >
 230 >  INPUT:       get-read-write-request;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 231 >        SYNONYM:    kf4req;
 232 >        PART OF:    reference-monitor-request;
 233 >        CONSISTS:   subject-id,
 234 >                    object-id,
 235 >                    usage-attribute;
 236 >
 237 >  OUTPUT:     get-read-write-decision;
 238 >        SYNONYM:    kf4dec;
 239 >        PART OF:    reference-monitor-decision;
 240 >        CONSISTS:   decision-type;
 241 >
 242 >  INPUT:      release-usage-attr-request;
 243 >        SYNONYM:    kf5req;
 244 >        PART OF:    reference-monitor-request;
 245 >        CONSISTS:   subject-id,
 246 >                    object-id,
 247 >                    usage-attribute;
 248 >
 249 >  OUTPUT:     release-usage-attr-decision;
 250 >        SYNONYM:    kf5dec;
 251 >        PART OF:    reference-monitor-decision;
 252 >        CONSISTS:   decision-type;
 253 >
 254 >  INPUT:      give-usage-attr-request;
 255 >        SYNONYM:    kf6req;
 256 >        PART OF:    reference-monitor-request;
 257 >        CONSISTS:   requesting-subject-id,
 258 >                    receiving-subject-id,
 259 >                    object-id,
 260 >                    usage-attribute;
 261 >
 262 >  OUTPUT:     give-usage-attr-decision;
 263 >        SYNONYM:    kf6dec;
 264 >        PART OF:    reference-monitor-decision;
 265 >        CONSISTS:   decision-type;
 266 >
 267 >  INPUT:      rescind-usage-attr-request;
 268 >        SYNONYM:    kf7req;
 269 >        PART OF:    reference-monitor-request;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 270 >       CONSISTS:   requesting-subject-id,
 271 >                   receiving-subject-id,
 272 >                   object-id,
 273 >                   usage-attribute;
 274 >
 275 >  OUTPUT:     rescind-usage-attr-decision;
 276 >       SYNONYM:    kf7dec;
 277 >       PART OF:    reference-monitor-decision;
 278 >       CONSISTS:   decision-type;
 279 >
 280 >  INPUT:      create-object-request;
 281 >       SYNONYM:    kf8req;
 282 >       PART OF:    reference-monitor-request;
 283 >       CONSISTS:   subject-id,
 284 >                   object-id,
 285 >                   obj-sec-level;
 286 >
 287 >  OUTPUT:     create-object-decision;
 288 >       SYNONYM:    kf8dec;
 289 >       PART OF:    reference-monitor-decision;
 290 >       CONSISTS:   decision-type;
 291 >
 292 >  INPUT:      delete-object-request;
 293 >       SYNONYM:    kf9req;
 294 >       PART OF:    reference-monitor-request;
 295 >       CONSISTS:   subject-id,
 296 >                   object-id;
 297 >
 298 >  OUTPUT:     delete-object-decision;
 299 >       SYNONYM:    kf9dec;
 300 >       PART OF:    reference-monitor-decision;
 301 >       CONSISTS:   decision-type;
 302 >
 303 >  INPUT:      change-sub-curr-sec-level-req;
 304 >       SYNONYM:    kf10req;
 305 >       PART OF:    reference-monitor-request;
 306 >       CONSISTS:   subject-id,
 307 >                   sub-curr-sec-level;
 308 >
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 309 >  OUTPUT:     change-sub-curr-sec-level-dec;
 310 >       SYNONYM:    kf10dec;
 311 >       PART OF:    reference-monitor-decision;
 312 >       CONSISTS:   decision-type;
 313 >
 314 >  INPUT:      change-obj-sec-level-request;
 315 >       SYNONYM:    kf11req;
 316 >       PART OF:    reference-monitor-request;
 317 >       CONSISTS:   subject-id,
 318 >                   object-id,
 319 >                   obj-sec-level;
 320 >
 321 >  OUTPUT:     change-obj-sec-level-decision;
 322 >       SYNONYM:    kf11dec;
 323 >       PART OF:    reference-monitor-decision;
 324 >       CONSISTS:   decision-type;
 325 >
 326 >  /* Administrative Security System Input/Output */
 327 >
 328 >  INPUT:      create-subject-command;
 329 >       SYNONYM:    cresubcom;
 330 >       PART OF:    admscom;
 331 >       CONSISTS:   security-id,
 332 >                   subject-id,
 333 >                   sub-max-sec-level,
 334 >                   sub-curr-sec-level;
 335 >
 336 >  OUTPUT:     create-subject-response;
 337 >       SYNONYM:    cresubres;
 338 >       PART OF:    admsres;
 339 >       CONSISTS:   validation-code;
 340 >
 341 >  INPUT:      delete-subject-command;
 342 >       SYNONYM:    delsubcom;
 343 >       PART OF:    admscom;
 344 >       CONSISTS:   security-id,
 345 >                   subject-id;
 346 >
 347 >  OUTPUT:     delete-subject-response;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 348 >        SYNONYM:    delsubres;
 349 >        PART OF:    admsres;
 350 >        CONSISTS:   validation-code;
 351 >
 352 >  INPUT:       change-sub-max-sec-level-comd;
 353 >        SYNONYM:    chasubmaxseclevcom;
 354 >        PART OF:    admscom;
 355 >        CONSISTS:   security-id,
 356 >                    subject-id,
 357 >                    sub-max-sec-level;
 358 >
 359 >  OUTPUT:      change-sub-max-sec-level-resp;
 360 >        SYNONYM:    chasubmaxseclevres;
 361 >        PART OF:    admsres;
 362 >        CONSISTS:   validation-code;
 363 >
 364 >  INPUT:       link-reference-monitor-comd;
 365 >        SYNONYM:    linrmoncom;
 366 >        PART OF:    admscom;
 367 >        CONSISTS:   security-id;
 368 >
 369 >  OUTPUT:      link-reference-monitor-resp;
 370 >        SYNONYM:    linrmonres;
 371 >        PART OF:    admsres;
 372 >        CONSISTS:   validation-code;
 373 >
 374 >  /* Auditing System Input/Output */
 375 >
 376 >  INPUT:       sub-obj-audit-request;
 377 >        SYNONYM:    subobjaudreq;
 378 >        PART OF:    audreq;
 379 >        CONSISTS:   subject-id,
 380 >                    object-id;
 381 >
 382 >  OUTPUT:            sub-obj-audit-trail;
 383 >        SYNONYM:    subobjaudtra;
 384 >        PART OF:    audtra;
 385 >        CONSISTS:   inc-audit-information;
 386 >
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 387 >  GROUP:       inc-audit-information;
 388 >       SYNONYM:    incaudinfo;
 389 >       CONSISTS:   incident-type,
 390 >                   date-time,
 391 >                   consol-nr;
 392 >
 393 >  INPUT:       sub-inc-audit-request;
 394 >       SYNONYM:    subincaudreq;
 395 >       PART OF:    audreq;
 396 >       CONSISTS:   subject-id,
 397 >                   incident-type;
 398 >
 399 >  OUTPUT:      sub-inc-audit-trail;
 400 >       SYNONYM:    subincaudtra;
 401 >       PART OF:    audtra;
 402 >       CONSISTS:   obj-audit-information;
 403 >
 404 >  GROUP:       obj-audit-information;
 405 >       SYNONYM:    objaudinfo;
 406 >       CONSISTS:   object-id,
 407 >                   date-time,
 408 >                   consol-nr;
 409 >
 410 >  INPUT:       sub-obj-inc-audit-request;
 411 >       SYNONYM:    subobjincaudreq;
 412 >       PART OF:    audreq;
 413 >       CONSISTS:   subject-id,
 414 >                   object-id,
 415 >                   incident-type;
 416 >
 417 >  OUTPUT:      sub-obj-inc-audit-trail;
 418 >       SYNONYM:    subobjincaudtra;
 419 >       PART OF:    audtra;
 420 >       CONSISTS:   audit-information;
 421 >
 422 >  GROUP        audit-information;
 423 >       SYNONYM:    audinfo;
 424 >       CONSISTS:   date-time,
 425 >                   consol-nr;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 426 >
 427 >  INPUT:      sub-audit-request;
 428 >       SYNONYM:    subaudreq;
 429 >       PART OF:    audreq;
 430 >       CONSISTS:   subject-id;
 431 >
 432 >  OUTPUT:     sub-audit-trail;
 433 >       SYNONYM:    subaudtra;
 434 >       PART OF:    audtra;
 435 >       CONSISTS:   obj-inc-audit-information;
 436 >
 437 >  GROUP:      obj-inc-audit-information;
 438 >       SYNONYM:    objincaudinfo;
 439 >       CONSISTS:   object-id,
 440 >                   incident-type,
 441 >                   date-time,
 442 >                   consol-nr;
 443 >
 444 >  INPUT:      obj-inc-audit-request;
 445 >       SYNONYM:    objincaudreq;
 446 >       PART OF:    audreq;
 447 >       CONSISTS:   object-id,
 448 >                   incident-type;
 449 >
 450 >  OUTPUT:     obj-inc-audit-trail;
 451 >       SYNONYM:    objincaudtra;
 452 >       PART OF:    audtra;
 453 >       CONSISTS:   sub-audit-information;
 454 >
 455 >  GROUP:      sub-audit-information;
 456 >       SYNONYM:    subaudinfo;
 457 >       CONSISTS:   subject-id,
 458 >                   date-time,
 459 >                   consol-nr;
 460 >
 461 >  INPUT:      obj-audit-request;
 462 >       SYNONYM:    objaudreq;
 463 >       PART OF:    audreq;
 464 >       CONSISTS:   object-id;
```

A S - I S S O U R C E L I S T I N G

ID FIELD

```
>
>  OUTPUT:     obj-audit-trail;
>       SYNONYM:    objaudtra;
>       PART OF:    audtra;
>       CONSISTS:   sub-inc-audit-information;
>
>  GROUP:      sub-inc-audit-information;
>       SYNONYM:    subincaudinfo;
>       CONSISTS:   subject-id,
>                   incident-type,
>                   date-time,
>                   consol-nr;
>
>  INPUT:      inc-audit-request;
>       SYNONYM:    incaudreq;
>       PART OF:    audreq;
>       CONSISTS:   incident-type;
>
>  OUTPUT:     inc-audit-trail;
>       SYNONYM:    incaudtra;
>       PART OF:    audtra;
>       CONSISTS:   sub-obj-audit-information;
>
>  GROUP:      sub-obj-audit-information;
>       SYNONYM:    subobjaudinfo;
>       CONSISTS:   subject-id,
>                   object-id,
>                   date-time,
>                   consol-nr;
>
>  INPUT:      dump-audit-request;
>       SYNONYM:    dumaudreq;
>       PART OF:    audreq;
>
>  OUTPUT:     dump-audit-trail;
>       SYNONYM:    dumaudtra;
>       PART OF:    audtra;
>       CONSISTS:   sub-obj-inc-audit-information;
>
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 504 >  GROUP:       sub-obj-inc-audit-information;
 505 >       SYNONYM:     sibobjincaudinfo;
 506 >       CONSISTS:    subject-id,
 507 >                    object-id,
 508 >                    incident-type,
 509 >                    date-time,
 510 >                    consol-nr;
 511 >
 512 >  EOF
```

Security-control-example

DATA BASE SUMMARY

	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE	2	1	50.00	1	50.00
ATTRIBUTE-VALUE	4	0		0	
ELEMENT	15	0		12	80.00
ENTITY	3	3	100.00	3	100.00
GROUP	11	8	72.73	3	27.27
INPUT	27	27	100.00	4	14.81
KEYWORD	2	0		2	100.00
MEMO	1	0		1	100.00
OUTPUT	27	27	100.00	4	14.81
PROCESS	4	4	100.00	4	100.00
INTERFACE	3	3	100.00	3	100.00
RELATION	5	0		5	100.00
SET	7	7	100.00	7	100.00
** TOTAL **	111	80	72.07	49	44.14

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='OUT' ORDER=BYTYPE

1	administrative-security-resp	OUTPUT
2	audit-trail	OUTPUT
3	change-obj-sec-level-decision	OUTPUT
4	change-sub-curr-sec-level-dec	OUTPUT
5	change-sub-max-sec-level-resp	OUTPUT
6	create-object-decision	OUTPUT
7	create-subject-response	OUTPUT
8	delete-object-decision	OUTPUT
9	delete-subject-response	OUTPUT
10	dump-audit-trail	OUTPUT
11	get-execute-decision	OUTPUT
12	get-read-decision	OUTPUT
13	get-read-write-decision	OUTPUT
14	get-write-decision	OUTPUT
15	give-usage-attr-decision	OUTPUT
16	inc-audit-trail	OUTPUT
17	link-reference-monitor-resp	OUTPUT
18	obj-audit-trail	OUTPUT
19	obj-inc-audit-trail	OUTPUT
20	reference-monitor-decision	OUTPUT
21	release-usage-attr-decision	OUTPUT
22	rescind-usage-attr-decision	OUTPUT
23	security-control-output	OUTPUT
24	sub-audit-trail	OUTPUT
25	sub-inc-audit-trail	OUTPUT
26	sub-obj-audit-trail	OUTPUT
27	sub-obj-inc-audit-trail	OUTPUT

Security-control-example

CONTENTS REPORT

PARAMETERS FOR: CONT

FILE NONCFLAG INDEX LEVELS=ALL

```
 1*    1 administrative-security-resp (OUTPUT)

 2*    1 audit-trail (OUTPUT)

 3*    1 change-obj-sec-level-decision (OUTPUT)
  1     2   decision-type (ELEMENT)

 4*    1 change-sub-curr-sec-level-dec (OUTPUT)
  1     2   decision-type (ELEMENT)

 5*    1 change-sub-max-sec-level-resp (OUTPUT)
  1     2   validation-code (ELEMENT)

 6*    1 create-object-decision (OUTPUT)
  1     2   decision-type (ELEMENT)

 7*    1 create-subject-response (OUTPUT)
  1     2   validation-code (ELEMENT)

 8*    1 delete-object-decision (OUTPUT)
  1     2   decision-type (ELEMENT)

 9*    1 delete-subject-response (OUTPUT)
  1     2   validation-code (ELEMENT)

10*    1 dump-audit-trail (OUTPUT)
  1     2   sub-obj-inc-audit-information (GROUP)
  2      3     subject-id (ELEMENT)
  3      3     object-id (ELEMENT)
  4      3     incident-type (ELEMENT)
  5      3     date-time (ELEMENT)
  6      3     consol-nr (ELEMENT)

11*    1 get-execute-decision (OUTPUT)
  1     2   decision-type (ELEMENT)
```

Security-control-example

CONTENTS REPORT

```
12*   1 get-read-decision (OUTPUT)
  1    2   decision-type (ELEMENT)

13*   1 get-read-write-decision (OUTPUT)
  1    2   decision-type (ELEMENT)

14*   1 get-write-decision (OUTPUT)
  1    2   decision-type (ELEMENT)

15*   1 give-usage-attr-decision (OUTPUT)
  1    2   decision-type (ELEMENT)

16*   1 inc-audit-trail (OUTPUT)
  1    2   sub-obj-audit-information (GROUP)
  2     3     subject-id (ELEMENT)
  3     3     object-id (ELEMENT)
  4     3     date-time (ELEMENT)
  5     3     consol-nr (ELEMENT)

17*   1 link-reference-monitor-resp (OUTPUT)
  1    2   validation-code (ELEMENT)

18*   1 obj-audit-trail (OUTPUT)
  1    2   sub-inc-audit-information (GROUP)
  2     3     subject-id (ELEMENT)
  3     3     incident-type (ELEMENT)
  4     3     date-time (ELEMENT)
  5     3     consol-nr (ELEMENT)

19*   1 obj-inc-audit-trail (OUTPUT)
  1    2   sub-audit-information (GROUP)
  2     3     subject-id (ELEMENT)
  3     3     date-time (ELEMENT)
  4     3     consol-nr (ELEMENT)

20*   1 reference-monitor-decision (OUTPUT)

21*   1 release-usage-attr-decision (OUTPUT)
  1    2   decision-type (ELEMENT)

22*   1 rescind-usage-attr-decision (OUTPUT)
```

Security-control-example

CONTENTS REPORT

```
 1      2   decision-type (ELEMENT)

23*     1 security-control-output (OUTPUT)

24*     1 sub-audit-trail (OUTPUT)
 1       2   obj-inc-audit-information (GROUP)
 2         3     object-id (ELEMENT)
 3         3     incident-type (ELEMENT)
 4         3     date-time (ELEMENT)
 5         3     consol-nr (ELEMENT)

25*     1 sub-inc-audit-trail (OUTPUT)
 1       2   obj-audit-information (GROUP)
 2         3     object-id (ELEMENT)
 3         3     date-time (ELEMENT)
 4         3     consol-nr (ELEMENT)

26*     1 sub-obj-audit-trail (OUTPUT)
 1       2   inc-audit-information (GROUP)
 2         3     incident-type (ELEMENT)
 3         3     date-time (ELEMENT)
 4         3     consol-nr (ELEMENT)

27*     1 sub-obj-inc-audit-trail (OUTPUT)
 1       2   audit-information (GROUP)
 2         3     date-time (ELEMENT)
 3         3     consol-nr (ELEMENT)
```

Security-control-example

INDEX

1 administrative-security-resp 57

2 audit-information 59

3 audit-trail 57

4 change-obj-sec-level-decision 57

5 change-sub-curr-sec-level-dec 57

6 change-sub-max-sec-level-resp 57

7 consol-nr 57, 58(3), 59(4)

8 create-object-decision 57

9 create-subject-response 57

10 date-time 57, 58(3), 59(4)

11 decision-type 57(5), 58(5), 59

12 delete-object-decision 57

13 delete-subject-response 57

14 dump-audit-trail 57

15 get-execute-decision 57

16 get-read-decision 58

17 get-read-write-decision 58

18 get-write-decision 58

19 give-usage-attr-decision 58

20 inc-audit-information 59

21 inc-audit-trail 58

Security-control-example

INDEX

22 incident-type 57, 58, 59(2)

23 link-reference-monitor-resp 58

24 obj-audit-information 59

25 obj-audit-trail 58

26 obj-inc-audit-information 59

27 obj-inc-audit-trail 58

28 object-id 57, 58, 59(2)

29 reference-monitor-decision 58

30 release-usage-attr-decision 58

31 rescind-usage-attr-decision 58

32 security-control-output 59

33 sub-audit-information 58

34 sub-audit-trail 59

35 sub-inc-audit-information 58

36 sub-inc-audit-trail 59

37 sub-obj-audit-information 58

38 sub-obj-audit-trail 59

39 sub-obj-inc-audit-information 57

40 sub-obj-inc-audit-trail 59

41 subject-id 57, 58(3)

42 validation-code 57(3), 58

Security-control-example

Name Generation

PARAMETERS FOR: NG

```
   PRINT PUNCH EMPTY SELECTION='INP' ORDER=BYTYPE

    1    administrative-security-comd        INPUT
    2    auditing-request                    INPUT
    3    change-obj-sec-level-request        INPUT
    4    change-sub-curr-sec-level-req       INPUT
    5    change-sub-max-sec-level-comd       INPUT
    6    create-object-request               INPUT
    7    create-subject-command              INPUT
    8    delete-object-request               INPUT
    9    delete-subject-command              INPUT
   10    dump-audit-request                  INPUT
   11    get-execute-request                 INPUT
   12    get-read-request                    INPUT
   13    get-read-write-request              INPUT
   14    get-write-request                   INPUT
   15    give-usage-attr-request             INPUT
   16    inc-audit-request                   INPUT
   17    link-reference-monitor-comd         INPUT
   18    obj-audit-request                   INPUT
   19    obj-inc-audit-request               INPUT
   20    reference-monitor-request           INPUT
   21    release-usage-attr-request          INPUT
   22    rescind-usage-attr-request          INPUT
   23    security-control-input              INPUT
   24    sub-audit-request                   INPUT
   25    sub-inc-audit-request               INPUT
   26    sub-obj-audit-request               INPUT
   27    sub-obj-inc-audit-request           INPUT
```

Security-control-example

CONSISTS COMPARISON REPORT

PARAMETERS FOR: CNC

FILE

URA273:CNCBLD : NAME DOESNT CONSIST OF ANYTHING - administrative-security-cond
URA273:CNCBLD : NAME DOESNT CONSIST OF ANYTHING - auditing-request
URA273:CNCBLD : NAME DOESNT CONSIST OF ANYTHING - dump-audit-request
URA273:CNCBLD : NAME DOESNT CONSIST OF ANYTHING - reference-monitor-request
URA273:CNCBLD : NAME DOESNT CONSIST OF ANYTHING - security-control-input

Security-control-example

CONSISTS COMPARISON REPORT

BASIC CONTENTS MATRIX

The rows are the given input names.

The columns are the lowest level objects which are contained in the rows, with intermediate groups ignored.

If any columns are group names, then the definition is incomplete.

If any columns are ambiguous names, they are possible elements.

	ROW NAMES	
1	change-obj-sec-level-request	INPUT
2	change-sub-curr-sec-level-req	INPUT
3	change-sub-max-sec-level-comd	INPUT
4	create-object-request	INPUT
5	create-subject-command	INPUT
6	delete-object-request	INPUT
7	delete-subject-command	INPUT
8	get-execute-request	INPUT
9	get-read-request	INPUT
10	get-read-write-request	INPUT
11	get-write-request	INPUT
12	give-usage-attr-request	INPUT
13	inc-audit-request	INPUT
14	link-reference-monitor-comd	INPUT
15	obj-audit-request	INPUT
16	obj-inc-audit-request	INPUT
17	release-usage-attr-request	INPUT
18	rescind-usage-attr-request	INPUT
19	sub-audit-request	INPUT
20	sub-inc-audit-request	INPUT
21	sub-obj-audit-request	INPUT
22	sub-obj-inc-audit-request	INPUT

	COLUMN NAMES	
1	subject-id	ELEMENT
2	object-id	ELEMENT
3	classification-level	ELEMENT
4	category-set	ELEMENT
5	security-id	ELEMENT
6	usage-attribute	ELEMENT
7	requesting-subject-id	ELEMENT
8	receiving-subject-id	ELEMENT
9	incident-type	ELEMENT

Security-control-example

CONSISTS COMPARISON REPORT

BASIC CONTENTS MATRIX

An * in (i,j) means that column j is contained directly or indirectly in row i. The columns do not consist of anything further. Intermediate groups are ignored.

```
    123456789
   +---------+
 1 I****     I
 2 I* **     I
 3 I* ***    I
 4 I****     I
 5 I* ***    I
   +---------+
 6 I**       I
 7 I*   *    I
 8 I**   *   I
 9 I**   *   I
10 I**   *   I
   +---------+
11 I**   *   I
12 I *   *** I
13 I        *I
14 I    *    I
15 I *       I
   +---------+
16 I *      *I
17 I**   *  I
18 I *   *** I
19 I*        I
20 I*       *I
   +---------+
21 I**       I
22 I**      *I
   +---------+
```

Security-control-example

CONSISTS COMPARISON REPORT

CONTENTS SIMILARITY SUMMARY

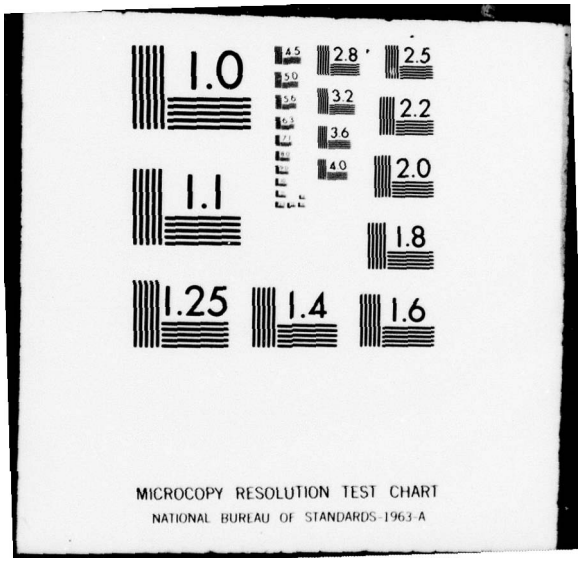
ROW#	NAME		ROW#	NAME
2	change-sub-curr-sec-level-req	IS A SUBSET OF	1	change-obj-sec-level-request
1	change-obj-sec-level-request	IS EQUIVALENT TO	4	create-object-request
6	delete-object-request	IS A SUBSET OF	1	change-obj-sec-level-request
15	obj-audit-request	IS A SUBSET OF	1	change-obj-sec-level-request
19	sub-audit-request	IS A SUBSET OF	1	change-obj-sec-level-request
21	sub-obj-audit-request	IS A SUBSET OF	1	change-obj-sec-level-request
2	change-sub-curr-sec-level-req	IS A SUBSET OF	3	change-sub-max-sec-level-cond
2	change-sub-curr-sec-level-req	IS A SUBSET OF	4	create-object-request
2	change-sub-curr-sec-level-req	IS A SUBSET OF	5	create-subject-command
19	sub-audit-request	IS A SUBSET OF	2	change-sub-curr-sec-level-req
3	change-sub-max-sec-level-cond	IS EQUIVALENT TO	5	create-subject-command
7	delete-subject-command	IS A SUBSET OF	3	change-sub-max-sec-level-cond
14	link-reference-monitor-comd	IS A SUBSET OF	3	change-sub-max-sec-level-cond
19	sub-audit-request	IS A SUBSET OF	3	change-sub-max-sec-level-cond
6	delete-object-request	IS A SUBSET OF	4	create-object-request
15	obj-audit-request	IS A SUBSET OF	4	create-object-request
19	sub-audit-request	IS A SUBSET OF	4	create-object-request
21	sub-obj-audit-request	IS A SUBSET OF	4	create-object-request
7	delete-subject-command	IS A SUBSET OF	5	create-subject-command
14	link-reference-monitor-comd	IS A SUBSET OF	5	create-subject-command
19	sub-audit-request	IS A SUBSET OF	5	create-subject-command
6	delete-object-request	IS A SUBSET OF	8	get-execute-request
6	delete-object-request	IS A SUBSET OF	9	get-read-request
6	delete-object-request	IS A SUBSET OF	10	get-read-write-request
6	delete-object-request	IS A SUBSET OF	11	get-write-request
15	obj-audit-request	IS A SUBSET OF	6	delete-object-request
6	delete-object-request	IS A SUBSET OF	17	release-usage-attr-request
19	sub-audit-request	IS A SUBSET OF	6	delete-object-request
6	delete-object-request	IS EQUIVALENT TO	21	sub-obj-audit-request
6	delete-object-request	IS A SUBSET OF	22	sub-obj-inc-audit-request
14	link-reference-monitor-comd	IS A SUBSET OF	7	delete-subject-command
19	sub-audit-request	IS A SUBSET OF	7	delete-subject-command
8	get-execute-request	IS EQUIVALENT TO	9	get-read-request
8	get-execute-request	IS EQUIVALENT TO	10	get-read-write-request
8	get-execute-request	IS EQUIVALENT TO	11	get-write-request
15	obj-audit-request	IS A SUBSET OF	8	get-execute-request
8	get-execute-request	IS EQUIVALENT TO	17	release-usage-attr-request

PRECEDING PAGE NOT FILMED BLANK

AD-A065 948 MICHIGAN UNIV ANN ARBOR DEPT OF INDUSTRIAL AND OPERA--ETC F/G 5/9
URL/URA TRAINING EXAMPLE.(U)
DEC 78 F19628-76-C-0197

UNCLASSIFIED ESD-TR-78-126 NL

2 OF 3
AD
A065948


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Security-control-example

CONSISTS COMPARISON REPORT

CONTENTS SIMILARITY SUMMARY

ROW#	NAME		ROW#	NAME
19	sub-audit-request	IS A SUBSET OF	8	get-execute-request
21	sub-obj-audit-request	IS A SUBSET OF	8	get-execute-request
9	get-read-request	IS EQUIVALENT TO	10	get-read-write-request
9	get-read-request	IS EQUIVALENT TO	11	get-write-request
15	obj-audit-request	IS A SUBSET OF	9	get-read-request
9	get-read-request	IS EQUIVALENT TO	17	release-usage-attr-request
19	sub-audit-request	IS A SUBSET OF	9	get-read-request
21	sub-obj-audit-request	IS A SUBSET OF	9	get-read-request
10	get-read-write-request	IS EQUIVALENT TO	11	get-write-request
15	obj-audit-request	IS A SUBSET OF	10	get-read-write-request
10	get-read-write-request	IS EQUIVALENT TO	17	release-usage-attr-request
19	sub-audit-request	IS A SUBSET OF	10	get-read-write-request
21	sub-obj-audit-request	IS A SUBSET OF	10	get-read-write-request
15	obj-audit-request	IS A SUBSET OF	11	get-write-request
11	get-write-request	IS EQUIVALENT TO	17	release-usage-attr-request
19	sub-audit-request	IS A SUBSET OF	11	get-write-request
21	sub-obj-audit-request	IS A SUBSET OF	11	get-write-request
15	obj-audit-request	IS A SUBSET OF	12	give-usage-attr-request
12	give-usage-attr-request	IS EQUIVALENT TO	18	rescind-usage-attr-request
13	inc-audit-request	IS A SUBSET OF	16	obj-inc-audit-request
13	inc-audit-request	IS A SUBSET OF	20	sub-inc-audit-request
13	inc-audit-request	IS A SUBSET OF	22	sub-obj-inc-audit-request
15	obj-audit-request	IS A SUBSET OF	16	obj-inc-audit-request
15	obj-audit-request	IS A SUBSET OF	17	release-usage-attr-request
15	obj-audit-request	IS A SUBSET OF	18	rescind-usage-attr-request
15	obj-audit-request	IS A SUBSET OF	21	sub-obj-audit-request
15	obj-audit-request	IS A SUBSET OF	22	sub-obj-inc-audit-request
16	obj-inc-audit-request	IS A SUBSET OF	22	sub-obj-inc-audit-request
19	sub-audit-request	IS A SUBSET OF	17	release-usage-attr-request
21	sub-obj-audit-request	IS A SUBSET OF	17	release-usage-attr-request
19	sub-audit-request	IS A SUBSET OF	20	sub-inc-audit-request
19	sub-audit-request	IS A SUBSET OF	21	sub-obj-audit-request
19	sub-audit-request	IS A SUBSET OF	22	sub-obj-inc-audit-request
20	sub-inc-audit-request	IS A SUBSET OF	22	sub-obj-inc-audit-request
21	sub-obj-audit-request	IS A SUBSET OF	22	sub-obj-inc-audit-request

Security-control-example

Name Generation

'ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ENTITY' ORDER=BYTYPE

1	incident-information	ENTITY
2	object-information	ENTITY
3	subject-information	ENTITY

Security-control-example

IDENTIFIER INFORMATION REPORT

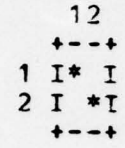
PARAMETERS FOR: EI

FILE ENTITY

URA308:IDENTC : THE FOLLOWING NAMES ARE NOT IDENTIFIED BY ANYTHING:
incident-information

ROW NAMES		COLUMN NAMES	
1 object-id	ELEMENT	1 object-information	ENTITY
2 subject-id	ELEMENT	2 subject-information	ENTITY

THE ROWS ARE IDENTIFIERS OF THE COLUMNS WITH *S



Security-control-example

IDENTIFIER INFORMATION REPORT

THE NUMBER OF COLUMNS IDENTIFIED BY THE ROWS

	ROW	TYPE	COUNT
1	object-id	ELEMENT	1
2	subject-id	ELEMENT	1

THE NUMBER OF ROWS THAT IDENTIFY THE COLUMNS

	COLUMN	TYPE	COUNT
1	object-information	ENTITY	1
2	subject-information	ENTITY	1

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='RELATION' ORDER=BYTYPE

1	obj-inc-audit-relation	RELATION
2	sub-inc-audit-relation	RELATION
3	sub-obj-audit-relation	RELATION
4	subject-access-to-object	RELATION
5	subject-need-to-know-object	RELATION

Security-control-example

FORMATTED PROBLEM STATEMENT

'ARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 BNMARG=72 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 RELATION                                  obj-inc-audit-relation;
 2     DESCRIPTION;
 3                     This relates an object to an incident in which
 4               subjects tried to access this object via the reference
 5               monitor.;
 6     BETWEEN:
 7       object-information AND          incident-information;
 8
 9 RELATION                                   sub-inc-audit-relation;
10     DESCRIPTION;
11                     This relates a subject to an audit incident
12               which he has caused by trying to access objects via the .
13               reference monitor.;
14     BETWEEN:
15       subject-information AND         incident-information;
16
17 RELATION                                   sub-obj-audit-relation;
18     DESCRIPTION;
19                     This relates a subject to an object with which
20               he has caused audit incidents by trying to access
21               the object via the reference monitor.;
22     BETWEEN:
23       subject-information AND         object-information;
24
25 RELATION                                   subject-access-to-object;
26     DESCRIPTION;
27               This relation specifies that a subject may have
28               usage attribute access to an object.;
29     ASSOCIATED-DATA IS:                 usage-attribute;
30     BETWEEN:
31       subject-information AND         object-information;
32
33 RELATION                                   subject-need-to-know-object;
34     DESCRIPTION;
35                     This relation specifies that a subject has a need
36               to know an object with usage attribute access.;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37      ASSOCIATED-DATA IS:                usage-attribute;
38      BETWEEN:
39        subject-information AND          object-information;
40
41 EOP EOP EOP EOP EOP
```

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD
   1 >  /* SCS data derivation */
   2 >
   3 >  PROCESS:    reference-monitor;
   4 >       USES:        reference-monitor-request;
   5 >       DERIVES:     reference-monitor-decision;
   6 >       USES:        reference-monitor-data-base;
   7 >       UPDATES:     auditing-system-data-base;
   8 >
   9 >  PROCESS:    administrative-security-system;
  10 >       USES:        administrative-security-cond;
  11 >       DERIVES:     administrative-security-resp;
  12 >       UPDATES:     reference-monitor-data-base;
  13 >
  14 >  PROCESS:    auditing-system;
  15 >       USES:        auditing-request;
  16 >       DERIVES:     audit-trail;
  17 >       USES:        auditing-system-data-base;
  18 >
  19 >  /* Reference Monitor Functions */
  20 >
  21 >  PROCESS:    get-read;
  22 >       SYNONYM:     kf1;
  23 >       DESCRIPTION;
  24 >                    This process decides whether or not to enable
  25 >              subject with subject-id read only access to object with
  26 >              object-id.          ;
  27 >       PART OF:     reference-monitor;
  28 >       USES:    get-read-request;
  29 >       DERIVES:  get-read-decision;
  30 >
  31 >  PROCESS:    get-write;
  32 >       SYNONYM:     kf2;
  33 >       DESCRIPTION;
  34 >                    This process decides whether or not to enable
  35 >              subject with subject-id write only access to object
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  36 >              with object-id.      ;
  37 >        PART OF:    reference-monitor;
  38 >        USES:   get-write-request;
  39 >        DERIVES:  get-write-decision;
  40 >
  41 >  PROCESS:    get-execute;
  42 >        SYNONYM:    kf3;
  43 >        DESCRIPTION;
  44 >                    This process decides whether or not to enable
  45 >              subject with subject-id execute access to object with
  46 >              object-id.  This process is only useful if the
  47 >              object-id requested is a procedure.  ;
  48 >        PART OF:    reference-monitor;
  49 >        USES:   get-execute-request;
  50 >        DERIVES:  get-execute-decision;
  51 >
  52 >  PROCESS:    get-read-write;
  53 >        SYNONYM:    kf4;
  54 >        DESCRIPTION;
  55 >                    This process decides whether or not to enable
  56 >              subject with subject-id read and write access to object
  57 >              with object-id.   ;
  58 >        PART OF:    reference-monitor;
  59 >        USES:   get-read-write-request;
  60 >        DERIVES:  get-read-write-decision;
  61 >
  62 >  PROCESS:    release-usage-attr;
  63 >        SYNONYM:    kf5;
  64 >        DESCRIPTION;
  65 >                    This process releases usage attribute access
  66 >              to object with object-id from subject with subject-id.;
  67 >        PART OF:    reference-monitor;
  68 >        USES:   release-usage-attr-request;
  69 >        DERIVES:  release-usage-attr-decision;
  70 >
  71 >  PROCESS:    give-usage-attr;
  72 >        SYNONYM:    kf6;
  73 >        DESCRIPTION;
  74 >                    This process decides whether or not subject with
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  75 >              requesting-subject-id may give subject with
  76 >              receiving-subject-id usage attribute access to object
  77 >              with object-id.    ;
  78 >        PART OF:    reference-monitor;
  79 >        USES:   give-usage-attr-request;
  80 >        DERIVES:  give-usage-attr-decision;
  81 >
  82 >  PROCESS:    rescind-usage-attr;
  83 >        SYNONYM:    kf7;
  84 >        DESCRIPTION;
  85 >                    This process decides whether or not subject
  86 >              with requesting-subject-id may take usage attribute
  87 >              access of object with object-id from subject with
  88 >              receiving-subject-id.    ;
  89 >        PART OF:    reference-monitor;
  90 >        USES:   rescind-usage-attr-request;
  91 >        DERIVES:  rescind-usage-attr-decision;
  92 >
  93 >  PROCESS:    create-object;
  94 >        SYNONYM:    kf8;
  95 >        DESCRIPTION;
  96 >                    This process decides whether or not subject with
  97 >              subject-id may add an object to the directory
  98 >              hierarchy directly below directory object with
  99 >              object-id.  This added object is requested to have
 100 >              security level obj-sec-level.   ;
 101 >        PART OF:    reference-monitor;
 102 >        USES:   create-object-request;
 103 >        DERIVES:  create-object-decision;
 104 >
 105 >  PROCESS:    delete-object;
 106 >        SYNONYM:    kf9;
 107 >        DESCRIPTION;
 108 >                    This process decides whether or not subject with
 109 >              subject-id may delete an object with object-id from the
 110 >              appropriate set in the reference monitor data base.  ;
 111 >        PART OF:    reference-monitor;
 112 >        USES:   delete-object-request;
 113 >        DERIVES:  delete-object-decision;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 114 >
 115 >  PROCESS:    change-sub-curr-sec-level;
 116 >       SYNONYM:    kf10;
 117 >       DESCRIPTION;
 118 >                   This process decides whether or not subject with
 119 >             subject-id may change his current security level to
 120 >             sub-curr-sec-level.          ;
 121 >       PART OF:    reference-monitor;
 122 >       USES:   change-sub-curr-sec-level-req;
 123 >       DERIVES:  change-sub-curr-sec-level-dec;
 124 >
 125 >  PROCESS:    change-obj-sec-level;
 126 >       SYNONYM:    kf11;
 127 >       DESCRIPTION;
 128 >                   This process decides whether or not subject with
 129 >             subject-id may revise the security level of object
 130 >             with object-id to the value of obj-sec-level.   ;
 131 >       PART OF:    reference-monitor;
 132 >       USES:   change-obj-sec-level-request;
 133 >       DERIVES:  change-obj-sec-level-decision;
 134 >
 135 >  /* Administrative Security System Functions */
 136 >
 137 >  PROCESS:    create-subject;
 138 >       SYNONYM:    cresub;
 139 >       DESCRIPTION;
 140 >                   This process allows the system security
 141 >             administrator with security-id to create the record
 142 >             of a subject with subject-id.  This subject will
 143 >             be assigned maximum security level sub-max-sec-level and
 144 >             current security level obj-sec-level.     ;
 145 >       PART OF:    admssys;
 146 >       USES:   create-subject-command;
 147 >       DERIVES:  create-subject-response;
 148 >
 149 >  PROCESS:    delete-subject;
 150 >       SYNONYM:    delsub;
 151 >       DESCRIPTION;
 152 >                   This process allows the system security
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 153 >              administrator with security-id to delete the record
 154 >              of a subject with subject-id.          ;
 155 >         PART OF:    admssys;
 156 >         USES:   delete-subject-command;
 157 >         DERIVES:  delete-subject-response;
 158 >
 159 >   PROCESS:    change-sub-max-sec-level;
 160 >         SYNONYM:    chasubmaxseclev;
 161 >         DESCRIPTION;
 162 >                    This process allows the system security
 163 >              administrator with security-id to change the maximum
 164 >              security level of subject with subject-id to
 165 >              sub-max-sec-level.                     ;
 166 >         PART OF:    admssys;
 167 >         USES:   change-sub-max-sec-level-coml;
 168 >         DERIVES:  change-sub-max-sec-level-resp;
 169 >
 170 >   PROCESS:    link-reference-monitor;
 171 >         SYNONYM:    linrmon;
 172 >         DESCRIPTION;
 173 >                    This process allows the system security
 174 >              administrator with security-id to perform all
 175 >              reference monitor functions without security checks
 176 >              by the reference monitor.  He may perform these
 177 >              functions for any subject-id registered in the system.
 178 >              This process will effectively link the administrative
 179 >              security system to the reference monitor with the only
 180 >              security check being that of the system security
 181 >              administrator's security-id.  ;
 182 >         PART OF:    admssys;
 183 >         USES:   link-reference-monitor-coml;
 184 >         DERIVES:  link-reference-monitor-resp;
 185 >
 186 >   /* Auditing System Functions */
 187 >
 188 >   PROCESS:    sub-obj-audit;
 189 >         SYNONYM:    subobjaud;
 190 >         DESCRIPTION;
 191 >                    This process allows the system security
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 192 >              administrator obtain all sets of inc-audit-information
 193 >              for a particular subject with subject-id and object
 194 >              with object-id.          ;
 195 >        PART OF:    audsys;
 196 >        USES:   sub-obj-audit-request;
 197 >        DERIVES:  sub-obj-audit-trail;
 198 >
 199 >  PROCESS:    sub-inc-audit;
 200 >        SYNONYM:    subincaud;
 201 >        DESCRIPTION;
 202 >                   This process allows the system security
 203 >              administrator obtain all sets of obj-audit-information
 204 >              for a particular subject with subject-id and incident
 205 >              with incident-type.          ;
 206 >        PART OF:    audsys;
 207 >        USES:   sub-inc-audit-request;
 208 >        DERIVES:  sub-inc-audit-trail;
 209 >
 210 >  PROCESS:    sub-obj-inc-audit;
 211 >        SYNONYM:    subobjincaud;
 212 >        DESCRIPTION;
 213 >                   This process allows the system security
 214 >              administrator obtain all sets of audit-information
 215 >              for a particular subject with subject-id, object with
 216 >               object-id, and incident with incident-type.   ;
 217 >       PART OF:    audsys;
 218 >        USES:   sub-obj-inc-audit-request;
 219 >        DERIVES:  sub-obj-inc-audit-trail;
 220 >
 221 >  PROCESS:    sub-audit;
 222 >        SYNONYM:    subaud;
 223 >        DESCRIPTION;
 224 >                   This process allows the system security
 225 >              administrator obtain all sets of obj-inc-audit-
 226 >              information for a particular subject with subject-id.   ;
 227 >        PART OF:    audsys;
 228 >        USES:   sub-audit-request;
 229 >        DERIVES:  sub-audit-trail;
 230 >
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 231 >  PROCESS:    obj-inc-audit;
 232 >       SYNONYM:    objincaud;
 233 >       DESCRIPTION;
 234 >                   This process allows the system security
 235 >             administrator obtain all sets of sub-audit-information
 236 >             for a particular object with object-id and incident
 237 >             with incident-id.        ;
 238 >       PART OF:    audsys;
 239 >       USES:   obj-inc-audit-request;
 240 >       DERIVES:  obj-inc-audit-trail;
 241 >
 242 >  PROCESS:    obj-audit;
 243 >       SYNONYM:    objaud;
 244 >       DESCRIPTION;
 245 >                   This process allows the system security
 246 >             administrator obtain all sets of sub-inc-audit-
 247 >             information for a particular object with object-id.  ;
 248 >       PART OF:    audsys;
 249 >       USES:   obj-audit-request;
 250 >       DERIVES:  obj-audit-trail;
 251 >
 252 >  PROCESS:    inc-audit;
 253 >       SYNONYM:    incaud;
 254 >       DESCRIPTION;
 255 >                   This process allows the system security
 256 >             administrator obtain all sets of sub-obj-audit-
 257 >             information for a particular incident with incident-
 258 >             type.     ;
 259 >       PART OF:    audsys;
 260 >       USES:   inc-audit-request;
 261 >       DERIVES:  inc-audit-trail;
 262 >
 263 >
 264 >  PROCESS:    dump-audit;
 265 >       SYNONYM:    dumaud;
 266 >       DESCRIPTION;
 267 >                   This process allows the system security
 268 >             administrator obtain all sets of sub-obj-audit-
 269 >             information available in the auditing-system-data-
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 270 >              base.    ;
 271 >        PART OF:    audsys;
 272 >        USES:    dump-audit-request;
 273 >        DERIVES:  dump-audit-trail;
 274 >
 275 >   /* Reference Monitor Subfunctions */
 276 >   /* The following statements demonstrate how low level */
 277 >   /* functions may be defined.                          */
 278 >
 279 >   PROCESS:    check-need-to-know-usage;
 280 >        DESCRIPTION;
 281 >                   This process checks if a subject-need-to-know-
 282 >              object relation with usage-attribute  exists
 283 >              between subject with subject-id and object with
 284 >              object-id.   ;
 285 >        KEYWORD:    low-level;
 286 >        USES:       subject-id,object-id,usage-attribute  TO
 287 >        DERIVE:     error-code;
 288 >
 289 >   PROCESS:    check-sub-obj-sec-levels;
 290 >        DESCRIPTION;
 291 >                   This process checks if sub-curr-sec-level
 292 >              exceeds obj-sec-level.  For example, security level 1
 293 >              exceeds security level 2 if the classification level
 294 >              of security level 1 is higher than the classification
 295 >              level of security level 2 and the category set of
 296 >              security level 2 is a subset of the category set of
 297 >              security level 1.   ;
 298 >        KEYWORD:    low-level;
 299 >        USES:       sub-curr-sec-level,obj-sec-level  TO
 300 >        DERIVE:     error-code;
 301 >
 302 >   PROCESS:    create-access-relation;
 303 >        DESCRIPTION;
 304 >                   This process creates a subject-access-to-object
 305 >              relation between subject with subject-id and object with
 306 >              object-id.   ;
 307 >        KEYWORD:    low-level;
 308 >        USES:       subject-id,object-id  TO
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 309 >       UPDATE:     usage-attribute;
 310 >       MAINTAINS:  subject-access-to-object;
 311 >
 312 >  PROCESS:    produce-audit-incident;
 313 >       DESCRIPTION;
 314 >                   This process produces an occurrence of incident-
 315 >             information in the auditing system data base based on
 316 >             the value of error-code.   ;
 317 >       KEYWORD:    low-level;
 318 >       USES:       error-code   TO
 319 >       DERIVE:     incident-information;
 320 >
 321 >  PROCESS:    generate-decision;
 322 >       DESCRIPTION;
 323 >                   This process derives a decision type based on
 324 >             the value of error-code.    ;
 325 >       KEYWORD:    low-level;
 326 >       USES:       error-code  TO
 327 >       DERIVE:     decision-type;
 328 >
 329 >  PROCESS:    check-access-usage;
 330 >       DESCRIPTION;
 331 >                   This process checks if a subject-access-to-
 332 >             object relation with usage attribute exist between
 333 >             subject with subject-id and object with object-id.  ;
 334 >       KEYWORD:    low-level;
 335 >       USES:       subject-id,object-id,usage-attribute  TO
 336 >       DERIVE:     error-code;
 337 >
 338 >  PROCESS:    delete-access-relation;
 339 >       DESCRIPTION;
 340 >                   This process deletes a subject-access-to-object
 341 >             relation with usage attribute between subject with
 342 >             subject-id and object with object-id.   ;
 343 >       KEYWORD:    low-level;
 344 >       USES:       subject-id,object-id  TO
 345 >       DERIVE:     error-code;
 346 >
 347 >  PROCESS:    create-object-information;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 348 >       DESCRIPTION;
 349 >                   This process creates an occurrence of object-
 350 >             information in the appropriate set according to the value
 351 >             of obj-sec-level and sets the value of object-location.;
 352 >       KEYWORD:    low-level;
 353 >       USES:       object-id,obj-sec-level  TO
 354 >       DERIVE:     object-information;
 355 >
 356 >  PROCESS:    delete-object-information;
 357 >       DESCRIPTION;
 358 >                   This process deletes an occurrence of object-
 359 >             information from the appropriate set based on the values
 360 >             of object-id and obj-sec-level.   ;
 361 >       KEYWORD:    low-level;
 362 >       USES:       object-id,obj-sec-level  TO
 363 >       DERIVE:     error-code;
 364 >
 365 >  /* Procedures for Reference Monitor Functions */
 366 >
 367 >  PROCESS:    get-read;
 368 >       UTILIZES:   check-need-to-know-usage,
 369 >                   check-sub-obj-sec-levels,
 370 >                   create-access-relation,
 371 >                   produce-audit-incident,
 372 >                   generate-decision;
 373 >       PROCEDURE;
 374 >            1. Check if subject-need-to-know-object relation exists
 375 >               with usage-attribute value of read between subject with
 376 >               subject-id and object with object-id.  If answer is
 377 >               no, go to step 4.
 378 >            2. Otherwise, check if subject's sub-curr-sec-level
 379 >               exceeds object's obj-sec-level.  If answer is no,
 380 >               go to step 4.
 381 >            3. Otherwise, create a subject-access-to-object relation
 382 >               with usage-attribute between subject with subject-id
 383 >               and object with object-id.
 384 >            4. Produce an audit incident and generate a decision
 385 >               based on the value of error-code and then terminate. ;
 386 >
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 387 >  PROCESS:    release-usage-attr;
 388 >       UTILIZES:   check-access-usage,
 389 >                   delete-access-relation,
 390 >                   produce-audit-incident,
 391 >                   generate-decision;
 392 >       PROCEDURE;
 393 >            1. Check if subject-access-to-object relation exists
 394 >               with usage-attribute between subject with subject-id
 395 >               and object with object-id.  If answer is no, go to
 396 >               step 3.
 397 >            2. Otherwise, delete the relation.
 398 >            3. Produce an audit incident and generate a decision based
 399 >               on the value of error-code and then terminate.  ;
 400 >
 401 >  PROCESS:    create-object;
 402 >       UTILIZES:   check-sub-obj-sec-levels,
 403 >                   create-object-information,
 404 >                   produce-audit-incident,
 405 >                   generate-decision;
 406 >       PROCEDURE;
 407 >            1. Check if subject's sub-curr-sec-level exceeds object's
 408 >               obj-sec-level.  If answer is no, go to step 3.
 409 >            2. Create an occurrence of object-information with
 410 >               object-id in the appropriate file based on the value
 411 >               of obj-sec-level.
 412 >            3. Produce an audit incident and generate a decision
 413 >               based on the value of error-code and then terminate. ;
 414 >
 415 >
 416 >  RELATION:   subject-access-to-object;
 417 >       DERIVATION;
 418 >                   Create-access-relation adds connections and
 419 >              delete-access-relation deletes connections.  ;
 420 >       MAINTAINED BY:  delete-access-relation;
 421 >
 422 >  SET:        topsecfile,secfile,confile,uncfile;
 423 >       DERIVATION;
 424 >                   Create-object-information adds objects to these sets
 425 >              and delete-object-information deletes objects from
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 426 >                these sets.  ;
 427 >
 428 >  EOF
```

Security-control-example

DATA BASE SUMMARY

	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE	2	1	50.00	1	50.00
ATTRIBUTE-VALUE	4	0		0	
ELEMENT	15	0		12	80.00
ENTITY	3	3	100.00	3	100.00
GROUP	11	8	72.73	3	27.27
INPUT	27	27	100.00	4	14.81
KEYWORD	3	0		2	66.67
MEMO	1	0		1	100.00
OUTPUT	27	27	100.00	4	14.81
PROCESS	36	27	75.00	36	100.00
INTERFACE	3	3	100.00	3	100.00
RELATION	5	0		5	100.00
SET	7	7	100.00	7	100.00
** TOTAL **	144	103	71.53	81	56.25

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ELE' ORDER=BYTYPE

1	category-set	ELEMENT
2	classification-level	ELEMENT
3	consol-nr	ELEMENT
4	date-time	ELEMENT
5	decision-type	ELEMENT
6	error-code	ELEMENT
7	incident-type	ELEMENT
8	object-id	ELEMENT
9	object-location	ELEMENT
10	receiving-subject-id	ELEMENT
11	requesting-subject-id	ELEMENT
12	security-id	ELEMENT
13	subject-id	ELEMENT
14	usage-attribute	ELEMENT
15	validation-code	ELEMENT

Security-control-example

DATA PROCESS REPORT

'ARAMETERS FOR: DP

FILE DATA DPMAT DPANL PMAT PANL

THE ROWS ARE DATA NAMES, THE COLUMNS ARE PROCESS NAMES.

	ROW NAMES			COLUMN NAMES	
1	category-set	ELEMENT	1	generate-decision	PROCESS
2	classification-level	ELEMENT	2	check-need-to-know-usage	PROCESS
3	consol-nr	ELEMENT	3	check-sub-obj-sec-levels	PROCESS
4	date-time	ELEMENT	4	check-access-usage	PROCESS
5	decision-type	ELEMENT	5	delete-access-relation	PROCESS
6	error-code	ELEMENT	6	delete-object-information	PROCESS
7	incident-type	ELEMENT	7	produce-audit-incident	PROCESS
8	object-id	ELEMENT	8	create-object-information	PROCESS
9	object-location	ELEMENT	9	create-access-relation	PROCESS
10	receiving-subject-id	ELEMENT			
11	requesting-subject-id	ELEMENT			
12	security-id	ELEMENT			
13	subject-id	ELEMENT			
14	usage-attribute	ELEMENT			
15	validation-code	ELEMENT			

Security-control-example

DATA PROCESS REPORT

DATA PROCESS INTERACTION MATRIX

(i,j) value	meaning
R	Row i is received or used by column j (input)
U	Row i is updated by column j
D	Row i is derived or generated by column j (output)
A	Row i is input to, updated by, and output of column j (all)
P	Row i is input to and output of column j (flow)
1	Row i is input to and updated by column j
2	Row i is updated by and output of column j

	1	2	3	4	5	6	7	8	9
1	I				I				I
2	I				I				I
3	I				I				I
4	I				I				I
5	I	D			I				I
6	I	R	D	D	D	DI	D	R	I
7	I				I				I
8	I		R		R	RI	R		R RI
9	I				I				I
10	I				I				I
11	I				I				I
12	I				I				I
13	I		R		R	RI			RI
14	I		R		R	I			UI
15	I				I				I

Security-control-example

DATA PROCESS REPORT

DATA PROCESS INTERACTION MATRIX ANALYSIS

DATA

category-set	(ELEMENT)	(ROW 1)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
classification-level	(ELEMENT)	(ROW 2)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
consol-nr	(ELEMENT)	(ROW 3)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
date-time	(ELEMENT)	(ROW 4)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
incident-type	(ELEMENT)	(ROW 7)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
object-location	(ELEMENT)	(ROW 9)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
receiving-subject-id	(ELEMENT)	(ROW 10)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
requesting-subject-id	(ELEMENT)	(ROW 11)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
security-id	(ELEMENT)	(ROW 12)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS
validation-code	(ELEMENT)	(ROW 16)	NOT DERIVED, UPDATED, OR USED BY ANY PROCESS

PROCESSES

check-sub-obj-sec-levels	(COLUMN 3)	DERIVES SOMETHING, BUT DOES NOT USE ANYTHING
produce-audit-incident	(COLUMN 7)	USES DATA, BUT DOES NOT DERIVE OR UPDATE ANYTHING
create-object-information	(COLUMN 8)	USES DATA, BUT DOES NOT DERIVE OR UPDATE ANYTHING

Security-control-example

DATA PROCESS REPORT

PROCESS INTERACTION MATRIX (INCIDENCE)

The rows and columns are process names from above.
An asterisk in (i,j) means that something derived
or updated by process i is used by process j.

```
   123456789
  +---------+
1 I         I
2 I*      * I
3 I*      * I
4 I*      * I
5 I*      * I
  +---------+
6 I*      * I
7 I         I
8 I         I
9 I * *     I
  +---------+
```

Security-control-example

DATA PROCESS REPORT

PROCESS INTERACTION MATRIX ANALYSIS

generate-decision	(ROW/COL 1)	NO SUCCESSORS FOR THIS PROCESS
check-sub-obj-sec-levels	(ROW/COL 3)	NO PREDECESSORS FOR THIS PROCESS
delete-access-relation	(ROW/COL 5)	NO PREDECESSORS FOR THIS PROCESS
delete-object-information	(ROW/COL 6)	NO PREDECESSORS FOR THIS PROCESS
produce-audit-incident	(ROW/COL 7)	NO SUCCESSORS FOR THIS PROCESS
create-object-information	(ROW/COL 8)	NO INTERACTION WITH OTHER PROCESSES
create-access-relation	(ROW/COL 9)	NO PREDECESSORS FOR THIS PROCESS

Security-control-example

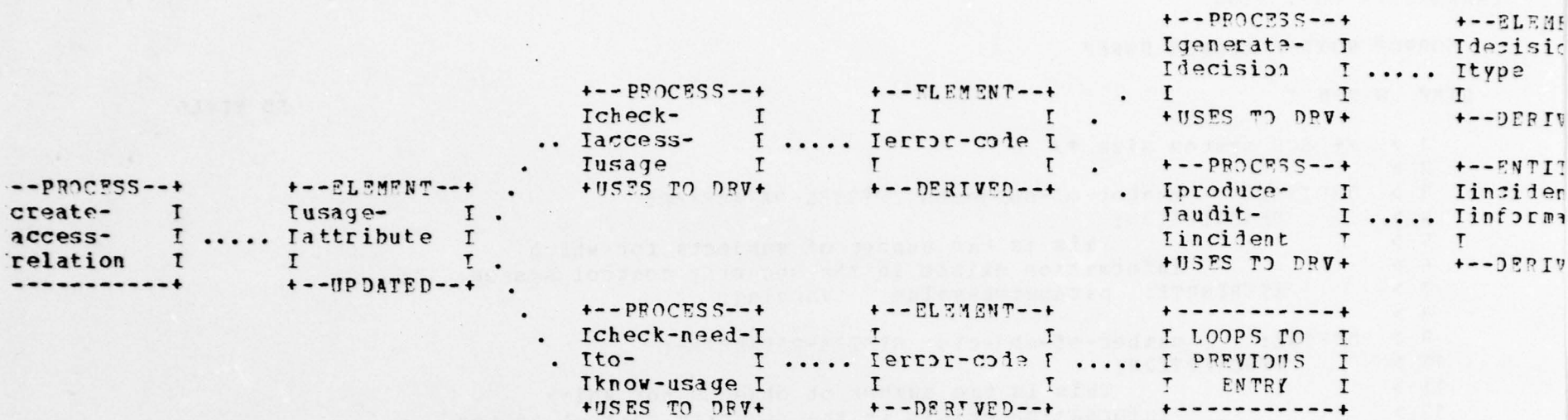
EXTENDED PICTURE

PARAMETERS FOR: EP

NAME=create-access-relation DATA-FLOW NOSTRUCTURE FORWARD NOBACKWARD LINKS=1000 NOINDEX
COLUMNS=119 ROWS=39 HORIZONTAL-BOXES=6 VERTICAL-BOXES=6

Security-control-example

EXTENDED PICTURE



Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS system size */
   2 >
   3 >  DEFINE:     number-of-subjects  SYSTEM-PARAMETER;
   4 >       DESCRIPTION;
   5 >                    This is the number of subjects for which
   6 >               information exists in the security control system.   ;
   7 >       ATTRIBUTE:  parameter-value    varying;
   8 >
   9 >  DEFINE:     number-of-objects  SYSTEM-PARAMETER;
  10 >       DESCRIPTION;
  11 >                    This is the number of objects for which
  12 >                information exists in the security control system.  ;
  13 >       ATTRIBUTE:  parameter-value    varying;
  14 >
  15 >  DEFINE:     number-of-incidents  SYSTEM-PARAMETER;
  16 >       DESCRIPTION;
  17 >                     This is the number of incidents for which
  18 >              information exists in the security control system.  ;
  19 >       ATTRIBUTE   parameter-value    varying;
  20 >
  21 >  DEFINE:     number-of-levels  SYSTEM-PARAMETER;
  22 >       DESCRIPTION;
  23 >                    This is the number of different classification
  24 >               levels which may be specified as a part of a subject
  25 >               and object security level.   ;
  26 >       ATTRIBUTE:  parameter-value    fixed;
  27 >       VALUE:   7;
  28 >
  29 >  DEFINE:     number-of-categories  SYSTEM-PARAMETER;
  30 >       DESCRIPTION;
  31 >                    This is the number of categories which are
  32 >               available for inclusion in a category set which may
  33 >               be specified as a part of a subject and object security
  34 >               level.   ;
  35 >       ATTRIBUTE:  parameter-value    fixed;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                          ID FIELD

  36 >       VALUE:    16;
  37 >
  38 >  DEFINE:     total-objects-and-subjects  SYSTEM-PARAMETER;
  39 >       DESCRIPTION;
  40 >                  This is the sum of number-of-objects and number-
  41 >            of-subjects.   ;
  42 >       ATTRIBUTE:  parameter-value    varying;
  43 >
  44 >  DEFINE:     number-of-dump-audit  SYSTEM-PARAMETER;
  45 >       ATTRIBUTE:  parameter-value    subject-to-change;
  46 >       VALUE IS:  1;
  47 >
  48 >  DEFINE:     number-of-obj-audit  SYSTEM-PARAMETER;
  49 >       ATTRIBUTE:  parameter-value    subject-to-change;
  50 >       VALUE IS:  1;
  51 >
  52 >  DEFINE:     number-of-sub-audit  SYSTEM-PARAMETER;
  53 >       ATTRIBUTE:  parameter-value    subject-to-change;
  54 >       VALUE IS:  1;
  55 >
  56 >  ENTITY:     subject-information;
  57 >       CARDINALITY:    number-of-subjects;
  58 >
  59 >  ENTITY:     object-information;
  60 >       CARDINALITY:    number-of-objects;
  61 >
  62 >  ENTITY:     incident-information;
  63 >       CARDINALITY:    number-of-incidents;
  64 >
  65 >  ELEMENT:    consol-nr;
  66 >       VALUES ARE:     0  THRU   25;
  67 >
  68 >  SET:        reference-monitor-data-base;
  69 >       CARDINALITY:    total-objects-and-subjects;
  70 >
  71 >  RELATION:   subject-need-to-know-object;
  72 >       CONNECTIVITY:   many  TO   many;
  73 >
  74 >  RELATION:   subject-access-to-object;
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  75 >       CONNECTIVITY:   many  TO  many;
  76 >
  77 >  RELATION:   sub-obj-audit-relation;
  78 >       CONNECTIVITY:   many  TO  many;
  79 >
  80 >  RELATION:   sub-inc-audit-relation;
  81 >       CONNECTIVITY:   1  TO  many;
  82 >       CARDINALITY:    number-of-incidents;
  83 >
  84 >  RELATION:   obj-inc-audit-relation;
  85 >       CONNECTIVITY:   1 TO many;
  86 >
  87 >  OUTPUT:     dump-audit-trail;
  88 >       CONSISTS:   number-of-incidents sub-obj-inc-audit-information;
  89 >
  90 >  INTERVAL:   year;
  91 >       CONSISTS:   12 month;
  92 >       CONSISTS:   52 week;
  93 >       CONSISTS:   365 day;
  94 >
  95 >  INTERVAL:   day;
  96 >       CONSISTS:   24 hour;
  97 >
  98 >  INTERVAL:   hour;
  99 >       CONSISTS:   60 minute;
 100 >
 101 >  PROCESS:    dump-audit;
 102 >       HAPPENS:    number-of-dump-audit  TIMES-PER  month;
 103 >
 104 >  INPUT:      dump-audit-request;
 105 >       HAPPENS:    number-of-dump-audit  TIMES-PER  month;
 106 >
 107 >  OUTPUT:     dump-audit-trail;
 108 >       HAPPENS:    number-of-dump-audit  TIMES-PER  month;
 109 >
 110 >  PROCESS:    obj-audit;
 111 >       HAPPENS:    number-of-obj-audit  TIMES-PER  month;
 112 >
 113 >  INPUT:      obj-audit-request;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

 114 >       HAPPENS:    number-of-obj-audit  TIMES-PER  month;
 115 >
 116 >  OUTPUT:     obj-audit-trail;
 117 >       HAPPENS:    number-of-obj-audit  TIMES-PER  month;
 118 >
 119 >  PROCESS:    sub-audit;
 120 >        HAPPENS:    number-of-sub-audit  TIMES-PER month;
 121 >
 122 >  INPUT:      sub-audit-request;
 123 >       HAPPENS:    number-of-sub-audit  TIMES-PER  month;
 124 >
 125 >  OUTPUT:     sub-audit-trail;
 126 >       HAPPENS:    number-of-sub-audit  TIMES-PER  month;
 127 >
 128 >  EOF
```

Security-control-example

DATA BASE SUMMARY

	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE	3	1	33.33	1	33.33
ATTRIBUTE-VALUE	7	0		0	
ELEMENT	15	0		12	80.00
ENTITY	3	3	100.00	3	100.00
GROUP	11	8	72.73	3	27.27
INPUT	27	27	100.00	4	14.81
INTERVAL	6	0		0	
KEYWORD	3	0		2	66.67
MEMO	1	0		1	100.00
OUTPUT	27	27	100.00	4	14.81
PROCESS	36	27	75.00	36	100.00
INTERFACE	3	3	100.00	3	100.00
RELATION	5	0		5	100.00
SET	7	7	100.00	7	100.00
SYSTEM-PARAMETER	10	0		6	60.00
** TOTAL **	164	103	62.80	87	53.05

Security-control-example

Name Generation

'ARAMETERS FOR: NG

```
PRINT PUNCH EMPTY SELECTION='SYSP' ORDER=BYTYPE

 1    many                          SYSTEM-PARAMETER
 2    number-of-categories          SYSTEM-PARAMETER
 3    number-of-dump-audit          SYSTEM-PARAMETER
 4    number-of-incidents           SYSTEM-PARAMETER
 5    number-of-levels              SYSTEM-PARAMETER
 6    number-of-obj-audit           SYSTEM-PARAMETER
 7    number-of-objects             SYSTEM-PARAMETER
 8    number-of-sub-audit           SYSTEM-PARAMETER
 9    number-of-subjects            SYSTEM-PARAMETER
10    total-objects-and-subjects    SYSTEM-PARAMETER
```

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

```
   FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=70 CMARG=1 HMARG=40 DESG
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 DEFINE                                  many
    2      AS A SYSTEM-PARAMETER;
    3   /* LEFT CONNECTIVITY OF:              subject-need-to-know-object,
    4                                         subject-access-to-object,
    5                                         sub-obj-audit-relation */
    6   /* RIGHT CONNECTIVITY OF:             subject-need-to-know-object,
    7                                         subject-access-to-object,
    8                                         sub-obj-audit-relation,
    9                                         sub-inc-audit-relation,
   10                                         obj-inc-audit-relation */
   11
   12 DEFINE                                  number-of-categories
   13      AS A SYSTEM-PARAMETER;
   14     DESCRIPTION;
   15                    This is the number of categories which are
   16               available for inclusion in a category set which may
   17               be specified as a part of a subject and object security
   18               level.;
   19     ATTRIBUTES ARE:
   20       parameter-value                  fixed;
   21     VALUE IS:                          16;
   22
   23 DEFINE                                  number-of-dump-audit
   24      AS A SYSTEM-PARAMETER;
   25     ATTRIBUTES ARE:
   26       parameter-value                  subject-to-change;
   27   /* dump-audit HAPPENS
   28        number-of-dump-audit TIMES-PER  month */
   29   /* dump-audit-request HAPPENS
   30        number-of-dump-audit TIMES-PER  month */
   31   /* dump-audit-trail HAPPENS
   32        number-of-dump-audit TIMES-PER  month */
   33     VALUE IS:                          1;
   34
   35 DEFINE                                  number-of-incidents
   36      AS A SYSTEM-PARAMETER;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37      DESCRIPTION;
38                      This is the number of incidents for which
39                information exists in the security control system.;
40      ATTRIBUTES ARE:
41        parameter-value                    varying;
42   /* dump-audit-trail CONTAINS
43        number-of-incidents                sub-obj-inc-audit-information
44    */
45   /* CARDINALITY OF:                     incident-information,
46                                           sub-inc-audit-relation */
47
48 DEFINE                                    number-of-levels
49       AS A SYSTEM-PARAMETER;
50      DESCRIPTION;
51                      This is the number of different classification
52                levels which may be specified as a part of a subject
53                and object security level.;
54      ATTRIBUTES ARE:
55        parameter-value                    fixed;
56      VALUE IS:                            7;
57
58 DEFINE                                    number-of-obj-audit
59       AS A SYSTEM-PARAMETER;
60      ATTRIBUTES ARE:
61        parameter-value                    subject-to-change;
62   /* obj-audit HAPPENS
63        number-of-obj-audit TIMES-PER      month */
64   /* obj-audit-request HAPPENS
65        number-of-obj-audit TIMES-PER      month */
66   /* obj-audit-trail HAPPENS
67        number-of-obj-audit TIMES-PER      month */
68      VALUE IS:                            1;
69
70 DEFINE                                    number-of-objects
71       AS A SYSTEM-PARAMETER;
72      DESCRIPTION;
73                      This is the number of objects for which
74                 information exists in the security control system.;
75      ATTRIBUTES ARE:
76        parameter-value                    varying;
77   /* CARDINALITY OF:                     object-information */
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
78
79 DEFINE                                  number-of-sub-audit
80      AS A SYSTEM-PARAMETER;
81     ATTRIBUTES ARE:
82       parameter-value                   subject-to-change;
83  /* sub-audit HAPPENS
84       number-of-sub-audit TIMES-PER     month */
85  /* sub-audit-request HAPPENS
86       number-of-sub-audit TIMES-PER     month */
87  /* sub-audit-trail HAPPENS
88       number-of-sub-audit TIMES-PER     month */
89     VALUE IS:                          1;
90
91 DEFINE                                  number-of-subjects
92      AS A SYSTEM-PARAMETER;
93     DESCRIPTION;
94                    This is the number of subjects for which
95               information exists in the security control system.;
96     ATTRIBUTES ARE:
97       parameter-value                   varying;
98  /* CARDINALITY OF:                    subject-information */
99
100 DEFINE                                 total-objects-and-subjects
101     AS A SYSTEM-PARAMETER;
102    DESCRIPTION;
103                   This is the sum of number-of-objects and number-
104             of-subjects.;
105    ATTRIBUTES ARE:
106      parameter-value                   varying;
107 /* CARDINALITY OF:                    reference-monitor-data-base */
108
109 EOF EOF EOF EOF EOF
```

Security-control-example

Name Generation

ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='INTERVAL' ORDER=BYTYPE

1	day	INTERVAL
2	hour	INTERVAL
3	minute	INTERVAL
4	month	INTERVAL
5	week	INTERVAL
6	year	INTERVAL

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 BNMARG=70 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 INTERVAL                                day;
 2     CONSISTS OF:
 3       24                                hour;
 4  /* year CONSISTS OF 365                day */
 5
 6 INTERVAL                                 hour;
 7     CONSISTS OF:
 8       60                                minute;
 9  /* day CONSISTS OF 24                  hour */
10
11 INTERVAL                                minute;
12  /* hour CONSISTS OF 60                minute */
13
14 INTERVAL                                month;
15  /* year CONSISTS OF 12                month */
16  /* dump-audit HAPPENS
17       number-of-dump-audit TIMES-PER    month */
18  /* dump-audit-request HAPPENS
19       number-of-dump-audit TIMES-PER    month */
20  /* dump-audit-trail HAPPENS
21       number-of-dump-audit TIMES-PER    month */
22  /* obj-audit HAPPENS
23       number-of-obj-audit TIMES-PER     month */
24  /* obj-audit-request HAPPENS
25       number-of-obj-audit TIMES-PER     month */
26  /* obj-audit-trail HAPPENS
27       number-of-obj-audit TIMES-PER     month */
28  /* sub-audit HAPPENS
29       number-of-sub-audit TIMES-PER     month */
30  /* sub-audit-request HAPPENS
31       number-of-sub-audit TIMES-PER     month */
32  /* sub-audit-trail HAPPENS
33       number-of-sub-audit TIMES-PER     month */
34
35 INTERVAL                                 week;
36  /* year CONSISTS OF 52                 week */
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37
38 INTERVAL                          year;
39     CONSISTS OF:
40       12                          month,
41       52                          week,
42       365                         day;
43
44 EOF EOF EOF EOF EOF
```

Security-control-example

FREQUENCY REPORT

I N T E R V A L : month

N A M E	T Y P E	T I M E S H A P P E N S
dump-audit	PROCESS	number-of-dump-audit
dump-audit-request	INPUT	number-of-dump-audit
dump-audit-trail	OUTPUT	number-of-dump-audit
obj-audit	PROCESS	number-of-obj-audit
obj-audit-request	INPUT	number-of-obj-audit
obj-audit-trail	OUTPUT	number-of-obj-audit
sub-audit	PROCESS	number-of-sub-audit
sub-audit-request	INPUT	number-of-sub-audit
sub-audit-trail	OUTPUT	number-of-sub-audit

Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS system dynamics */
   2 >
   3 >  ENTITY:     subject-information;
   4 >       VOLATILITY;
   5 >                    The sub-max-sec-level can only be changed by a
   6 >            system security administrator and only on decision
   7 >            of the administrator.  The sub-curr-sec-level may
   8 >            change several times within the course of one session
   9 >            on the system.   ;
  10 >
  11 >  ENTITY:     object-information;
  12 >       VOLATILITY;
  13 >                    The obj-sec-level may be changed by either the
  14 >            owner of the object or the system security administrator.
  15 >            Changing the object-location is done based on need by
  16 >            the operating system.    ;
  17 >
  18 >  ENTITY:     incident-information;
  19 >       VOLATILITY;
  20 >                    The contents of this type of entity are never
  21 >            changed after creation.    ;
  22 >
  23 >  SET:        reference-monitor-data-base;
  24 >       VOLATILITY-SET;
  25 >                    The set is changed whenever a subject or object
  26 >            is added to, or deleted from, the system.   ;
  27 >       VOLATILITY-MEMBER;
  28 >                    Volatility of the set's members can be found
  29 >            under description for subject-information and object-
  30 >            information.   ;
  31 >
  32 >  SET:        auditing-system-data-base;
  33 >       VOLATILITY-SET;
  34 >                    The set is changed whenever an auditing incident
  35 >            occurs.   ;
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  36 >       VOLATILITY-MEMBER;
  37 >                  An occurrence of incident-information is created
  38 >             whenever an object is improperly accessed, a subject
  39 >             logs in the system, or a subject id is improperly used. ;
  40 >
  41 >  EVENT:      occurrence-get-read-request;
  42 >       TRIGGERS:   get-read;
  43 >       HAPPENS:    get-read-distribution   TIMES-PER      hour;
  44 >
  45 >  EVENT:      initiate-get-read-procedure;
  46 >       ON INCEPTION:   get-read;
  47 >       TRIGGERS:       check-need-to-know-usage;
  48 >
  49 >  PROCESS:    check-need-to-know-usage;
  50 >       TERMINATION-CAUSES:  need-to-know-check-fails,
  51 >                            need-to-know-check-succeeds;
  52 >
  53 >  PROCESS:    produce-audit-incident,generate-decision;
  54 >       TRIGGERED BY:   need-to-know-check-fails,
  55 >                       sub-obj-sec-level-check-fails;
  56 >
  57 >  PROCESS:    check-sub-obj-sec-levels;
  58 >       TRIGGERED BY:   need-to-know-check-succeeds;
  59 >       TERMINATION-CAUSES:  sub-obj-sec-level-check-fails,
  60 >                            sub-obj-sec-level-check-succ;
  61 >
  62 >  PROCESS:    create-access-relation;
  63 >       TRIGGERED BY:   sub-obj-sec-level-check-succ;
  64 >
  65 >  EVENT:      create-access-relation-succ;
  66 >       ON TERMINATION: create-access-relation;
  67 >       TRIGGERS:       generate-decision;
  68 >
  69 >  EVENT:      need-to-know-check-fails;
  70 >       WHEN   need-to-know-check-passes    BECOMES FALSE;
  71 >
  72 >  EVENT:      need-to-know-check-succeeds;
  73 >       WHEN   need-to-know-check-passes    BECOMES TRUE;
  74 >
```

Security-control-example

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  75 >  CONDITION:  sub-obj-sec-level-check-passes;
  76 >       BECOMING TRUE IS CALLED sub-obj-sec-level-check-succ;
  77 >       BECOMING FALSE IS CALLED  sub-obj-sec-level-check-fails;
  78 >
  79 >  CONDITION:  get-read-request-made;
  80 >       BECOMING TRUE CALLED occurrence-get-read-request;
  81 >       FALSE WHILE;
  82 >                 Requests on the get-read procedure occur on
  83 >            demand of subjects.  These occurrences are unscheduled
  84 >            and considered random events.    ;
  85 >       TRUE WHILE;
  86 >                 This event exists during the period in which the
  87 >            get-read-request is being processed up until the
  88 >            decision has been given to the subject.  ;
  89 >
  90 >  CONDITION:  create-access-relation-fin;
  91 >       BECOMING TRUE CALLED  create-access-relation-succ;
  92 >       FALSE WHILE;
  93 >                 This event exists during the period in which
  94 >            the access relation is being created.  This condition
  95 >            must resolve to a TRUE state unless there is an error
  96 >            in the software.  ;
  97 >
  98 >  EVENT:       occur-release-usage-attr-req;
  99 >       TRIGGERS:       release-usage-attr;
 100 >       HAPPENS:    release-usage-attr-req-distr  TIMES-PER  hour;
 101 >
 102 >  EVENT:       init-release-usage-attr-proc;
 103 >       ON INCEPTION    release-usage-attr;
 104 >       TRIGGERS:       check-access-usage;
 105 >
 106 >  PROCESS:    check-access-usage;
 107 >       TERMINATION-CAUSES:  access-usage-check-fails,
 108 >                            access-usage-check-succeeds;
 109 >
 110 >  PROCESS:    delete-access-relation;
 111 >       TRIGGERED BY:   access-usage-check-succeeds;
 112 >
 113 >  EVENT:       delete-access-relation-succ;
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                          ID FIELD

 114 >       ON TERMINATION:  delete-access-relation;
 115 >       TRIGGERS:        generate-decision;
 116 >
 117 >  EVENT:       access-usage-check-fails;
 118 >       TRIGGERS:  produce-audit-incident,
 119 >                  generate-decision;
 120 >
 121 >  EVENT:       occur-create-object-request;
 122 >       TRIGGERS:   create-object;
 123 >       HAPPENS:    create-object-distribution   TIMES-PER   hour;
 124 >
 125 >  EVENT:       init-create-object-procedure;
 126 >       ON INCEPTION:   create-object;
 127 >       TRIGGERS:       check-sub-obj-sec-levels;
 128 >
 129 >  PROCESS:     create-object-information;
 130 >       TRIGGERED BY:   sub-obj-sec-level-check-succ;
 131 >
 132 >  EVENT:       create-object-information-succ;
 133 >       ON TERMINATION  create-object-information;
 134 >       TRIGGERS:       generate-decision;
 135 >
 136 >  EOF
```

Security-control-example

DATA BASE SUMMARY

	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE	3	1	33.33	1	33.33
ATTRIBUTE-VALUE	7	0		0	
CONDITION	4	0		0	
ELEMENT	15	0		12	80.00
ENTITY	3	3	100.00	3	100.00
EVENT	15	0		0	
GROUP	11	8	72.73	3	27.27
INPUT	27	27	100.00	4	14.81
INTERVAL	6	0		0	
KEYWORD	3	0		2	66.67
MEMO	1	0		1	100.00
OUTPUT	27	27	100.00	4	14.81
PROCESS	36	27	75.00	36	100.00
INTERFACE	3	3	100.00	3	100.00
RELATION	5	0		5	100.00
SET	7	7	100.00	7	100.00
SYSTEM-PARAMETER	13	0		6	46.15
** TOTAL **	186	103	55.38	87	46.77

Security-control-example

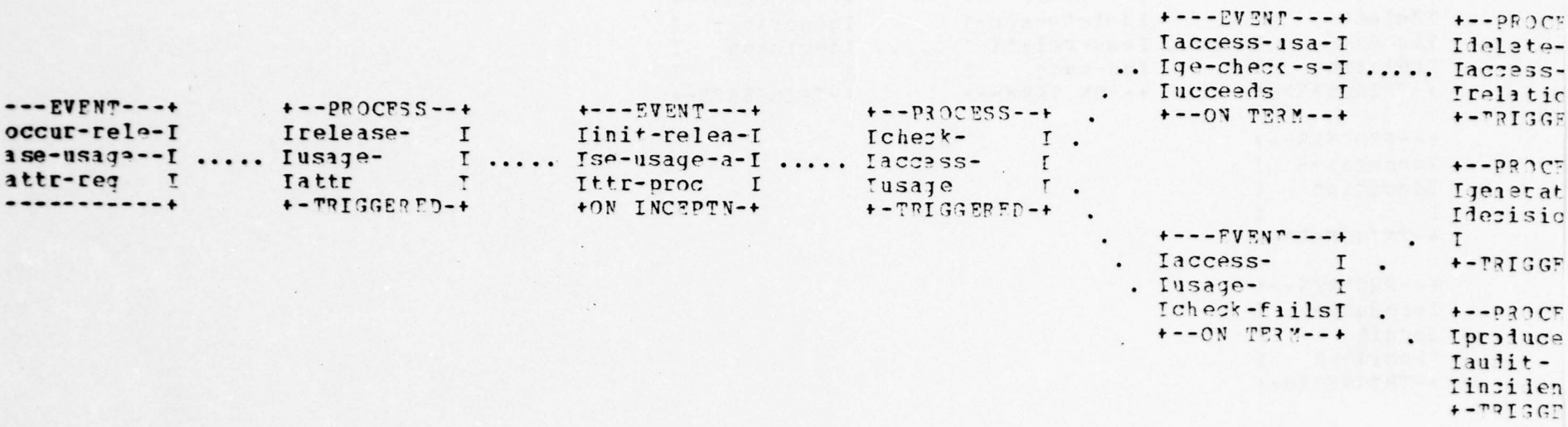
Process Chain

PARAMETERS FOR: PC

NAME=occur-release-usage-attr-req LINKS=1000 NOINDEX COLUMNS=119 ROWS=39 HORIZONTAL-BOXES=6
VERTICAL-BOXES=6

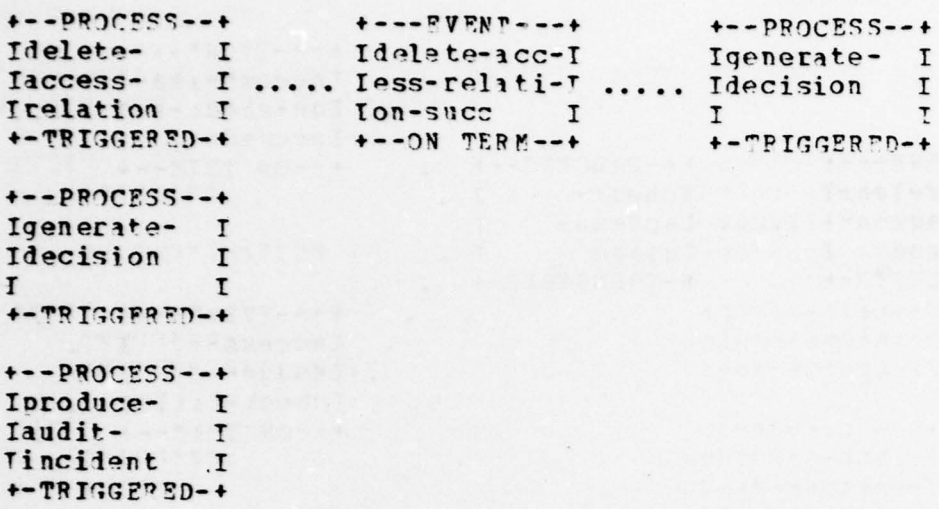
Security-control-example

Process Chain



Security-control-example

Process Chain



Security-control-example

Name Generation

ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='EVENT' ORDER=BYTYPE

1	access-usage-check-fails	EVENT
2	access-usage-check-succeeds	EVENT
3	create-access-relation-succ	EVENT
4	create-object-information-succ	EVENT
5	delete-access-relation-succ	EVENT
6	init-create-object-procedure	EVENT
7	init-release-usage-attr-proc	EVENT
8	initiate-get-read-procedure	EVENT
9	need-to-know-check-fails	EVENT
10	need-to-know-check-succeeds	EVENT
11	occur-create-object-request	EVENT
12	occur-release-usage-attr-req	EVENT
13	occurrence-get-read-request	EVENT
14	sub-obj-sec-level-check-fails	EVENT
15	sub-obj-sec-level-check-succ	EVENT

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: PPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 BNMARG=70 CMARG=1 HMARG=40 DESC
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 EVENT                                 access-usage-check-fails;
 2     TRIGGERS:                        produce-audit-incident,
 3                                      generate-decision;
 4     ON TERMINATION OF:               check-access-usage;
 5
 6 EVENT                                 access-usage-check-succeeds;
 7     TRIGGERS:                        delete-access-relation;
 8     ON TERMINATION OF:               check-access-usage;
 9
10 EVENT                                 create-access-relation-succ;
11     TRIGGERS:                        generate-decision;
12     WHEN:                            create-access-relation-fin
13                                       BECOMES TRUE;
14     ON TERMINATION OF:               create-access-relation;
15
16 EVENT                                 create-object-information-succ;
17     TRIGGERS:                        generate-decision;
18     ON TERMINATION OF:               create-object-information;
19
20 EVENT                                 delete-access-relation-succ;
21     TRIGGERS:                        generate-decision;
22     ON TERMINATION OF:               delete-access-relation;
23
24 EVENT                                 init-create-object-procedure;
25     TRIGGERS:                        check-sub-obj-sec-levels;
26     ON INCEPTION OF:                 create-object;
27
28 EVENT                                 init-release-usage-attr-proc;
29     TRIGGERS:                        check-access-usage;
30     ON INCEPTION OF:                 release-usage-attr;
31
32 EVENT                                 initiate-get-read-procedure;
33     TRIGGERS:                        check-need-to-know-usage;
34     ON INCEPTION OF:                 get-read;
35
36 EVENT                                 need-to-know-check-fails;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37      TRIGGERS:                          produce-audit-incident,
38                                         generate-decision;
39      WHEN:                              need-to-know-check-passes
40                                          BECOMES FALSE;
41      ON TERMINATION OF:                 check-need-to-know-usage;
42
43  EVENT                                   need-to-know-check-succeeds;
44      TRIGGERS:                          check-sub-obj-sec-levels;
45      WHEN:                              need-to-know-check-passes
46                                          BECOMES TRUE;
47      ON TERMINATION OF:                 check-need-to-know-usage;
48
49  EVENT                                   occur-create-object-request;
50      TRIGGERS:                          create-object;
51      HAPPENS:
52        create-object-distribution
53         TIMES-PER                       hour;
54
55  EVENT                                   occur-release-usage-attr-req;
56      TRIGGERS:                          release-usage-attr;
57      HAPPENS:
58        release-usage-attr-req-distr
59         TIMES-PER                       hour;
60
61  EVENT                                   occurrence-get-read-request;
62      TRIGGERS:                          get-read;
63      WHEN:                              get-read-request-made
64                                          BECOMES TRUE;
65      HAPPENS:
66        get-read-distribution TIMES-PER  hour;
67
68  EVENT                                   sub-obj-sec-level-check-fails;
69      TRIGGERS:                          produce-audit-incident,
70                                         generate-decision;
71      WHEN:                              sub-obj-sec-level-check-passes
72                                          BECOMES FALSE;
73      ON TERMINATION OF:                 check-sub-obj-sec-levels;
74
75  EVENT                                   sub-obj-sec-level-check-succ;
76      TRIGGERS:                          create-access-relation,
77                                         create-object-information;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
78      WHEN:                          sub-obj-sec-level-check-passes
79                                      BECOMES TRUE;
80      ON TERMINATION OF:             check-sub-obj-sec-levels;
81
82 EOF EOF EOF EOF EOF
```

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='COND' ORDER=BYTYPE

1	create-access-relation-fin	CONDITION
2	get-read-request-made	CONDITION
3	need-to-know-check-passes	CONDITION
4	sub-obj-sec-level-check-passes	CONDITION

Security-control-example

FORMATTED PROBLEM STATEMENT

```
PARAMETERS FOR: PPS

   FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=70 CMARG=1 HMARG=40 DESC
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 CONDITION                                create-access-relation-fin;
    2     BECOMING TRUE IS CALLED:            create-access-relation-succ;
    3     FALSE WHILE;
    4                     This event exists during the period in which
    5               the access relation is being created.  This condition
    6               must resolve to a TRUE state unless there is an error
    7               in the software.;
    8
    9 CONDITION                                get-read-request-made;
   10     BECOMING TRUE IS CALLED:            occurrence-get-read-request;
   11     TRUE WHILE;
   12                     This event exists during the period in which the
   13               get-read-request is being processed up until the
   14               decision has been given to the subject.;
   15     FALSE WHILE;
   16                     Requests on the get-read procedure occur on
   17               demand of subjects.  These occurrences are unscheduled
   18               and considered random events.;
   19
   20 CONDITION                                need-to-know-check-passes;
   21     BECOMING TRUE IS CALLED:            need-to-know-check-succeeds;
   22     BECOMING FALSE IS CALLED:           need-to-know-check-fails;
   23
   24 CONDITION                                sub-obj-sec-level-check-passes;
   25     BECOMING TRUE IS CALLED:            sub-obj-sec-level-check-succ;
   26     BECOMING FALSE IS CALLED:           sub-obj-sec-level-check-fails;
   27
   28 EOF EOF EOF EOF EOF
```

Security-control-example

A S - I S S O U R C E L I S T I N G

PARAMETERS FOR: SYNU

SOURCE NOXREF UPDATE DBREF

```
LINE  S T M T                                                    ID FIELD

   1 >  /* SCS project management */
   2 >
   3 >  PROBLEM-DEFINER:      michel-j-bastarache;
   4 >       MAILBOX:         isdos-project-ann-arbor;
   5 >       RESPONSIBLE:     auditing-system,
   6 >                        administrative-security-system,
   7 >                        reference-monitor,
   8 >                        system-security-administrator;
   9 >
  10 >  PROBLEM-DEFINER:      james-m-amster;
  11 >       MAILBOX:         isdos-project-ann-arbor;
  12 >       RESPONSIBLE:     object-information,
  13 >                        subject-information,
  14 >                        incident-information,
  15 >                        reference-monitor-subject;
  16 >
  17 >  DEFINE:       unclassified   SECURITY;
  18 >       DESCRIPTION;
  19 >                     Any parts of the problem statement
  20 >                designated as unclassified may be viewed
  21 >                by unclassified personnel.  ;
  22 >       APPLIES:    scs,scinp,scout,scint,scdb;
  23 >
  24 >  DEFINE:       scs-statement-of-need SOURCE;
  25 >       DESCRIPTION;
  26 >                     This document is the statement of need for the
  27 >                Security Control System.
  28 >                Distribution Data:  22 August 1975.
  29 >                It is directed towards the MACIMS
  30 >                Multilevel Computer Security System.  ;
  31 >       APPLIES:    scs;
  32 >
  33 >  DEFINE:      scs-specification  SOURCE;
  34 >       DESCRIPTION;
  35 >                     This document specifies the major functions of
```

A S - I S S O U R C E L I S T I N G

```
LINE  S T M T                                                    ID FIELD

  36 >              the security control system.  The access controls or
  37 >              reference monitor, the auditing system, and the
  38 >              administrative security system are mentioned.  ;
  39 >        APPLIES:    scs;
  40 >
  41 >  MEMO:       clearance-memo;
  42 >        DESCRIPTION;
  43 >                   In this specification, clearance is defined as the
  44 >              eligibility of a person (or process or job) to access
  45 >              information of a certain classification level (or
  46 >              lower).  For example, a person with a Secret clearance
  47 >              is eligible to access information with classification
  48 >              levels Unclassified to Secret, but may not have access
  49 >              to Top Secret information.  When compartmented security
  50 >              is used, a clearance also includes the categories a
  51 >              person is eligible to access.  In addition to the
  52 >              eligibility afforded a person by his clearance, he
  53 >              must also have the need to know the classified
  54 >              information before he is given access.     ;
  55 >        APPLIES:    classification-level;
  56 >
  57 >  MEMO:       category-set-memo;
  58 >        DESCRIPTION;
  59 >                   In reference to a person (or process), a category
  60 >              set refers to the set of compartments a person is
  61 >              eligible to access.  A compartment in this context is
  62 >              an orthogonal subdivision of the classification
  63 >              levels.  A compartment is like a FORMAL NEED TO KNOW
  64 >              authorization to information of a certain topic
  65 >              without consideration of classification level.
  66 >                   In reference to documents, files, or other objects
  67 >              a category set refers to the possible information
  68 >              sources used to create the object.  Thus, a category set
  69 >              with several categories or compartments would indicate
  70 >              that the object should be handled with extra caution
  71 >              o objects which would intersect the sensitive areas
  72 >              of each of the categories in the set.   ;
  73 >        APPLIES:    category-set;
  74 >
```

Security-control-example

A S - I S S O U R C E L I S T I N G

LINE	S T M T	ID FIELD
75 >	EOF	

Security-control-example

DATA BASE SUMMARY

	COUNT	#W/SYN	PERCENT	#W/DESC	PERCENT
ATTRIBUTE	3	1	33.33	1	33.33
ATTRIBUTE-VALUE	7	0		0	
CONDITION	4	0		0	
ELEMENT	15	0		12	80.00
ENTITY	3	3	100.00	3	100.00
EVENT	15	0		0	
GROUP	11	8	72.73	3	27.27
INPUT	27	27	100.00	4	14.81
INTERVAL	6	0		0	
KEYWORD	3	0		2	66.67
MAILBOX	1	0		0	
MEMO	3	0		3	100.00
OUTPUT	27	27	100.00	4	14.81
PROBLEM-DEFINER	2	0		0	
PROCESS	36	27	75.00	36	100.00
INTERFACE	3	3	100.00	3	100.00
RELATION	5	0		5	100.00
SECURITY	1	0		1	100.00
SET	7	7	100.00	7	100.00
SOURCE	2	0		2	100.00
SYSTEM-PARAMETER	13	0		6	46.15
** TOTAL **	194	103	53.09	92	47.42

Security-control-example

Name Generation

ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='MAILBOX OR MEMO OR PD' ORDER=BYTYPE

1	isdos-project-ann-arbor	MAILBOX
2	category-set-memo	MEMO
3	clearance-memo	MEMO
4	system-philosophy-memo	MEMO
5	james-m-amster	PROBLEM-DEFINER
6	michel-j-bastarache	PROBLEM-DEFINER

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

```
   FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 BNMARG=72 CMARG=1 HMARG=40 DFSG
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 DEFINE                                    isdos-project-ann-arbor
    2      AS A MAILBOX;
    3     APPLIES TO:                          michel-j-bastarache,
    4                                          james-m-amster;
    5
    6 MEMO                                      category-set-memo;
    7     DESCRIPTION;
    8                 In reference to a person (or process), a category
    9               set refers to the set of compartments a person is
   10               eligible to access.  A compartment in this context is
   11               an orthogonal subdivision of the classification
   12               levels.  A compartment is like a FORMAL NEED TO KNOW
   13               authorization to information of a certain topic
   14               without consideration of classification level.
   15                    In reference to documents, files, or other objects
   16               a category set refers to the possible information
   17               sources used to create the object.  Thus, a category set
   18               with several categories or compartments would indicate
   19               that the object should be handled with extra caution
   20               o objects which would intersect the sensitive areas
   21               of each of the categories in the set.;
   22     APPLIES TO:                          category-set;
   23
   24 MEMO                                      clearance-memo;
   25     DESCRIPTION;
   26                 In this specification, clearance is defined as the
   27               eligibility of a person (or process or job) to access
   28               information of a certain classification level (or
   29               lower).  For example, a person with a Secret clearance
   30               is eligible to access information with classification
   31               levels Unclassified to Secret, but may not have access
   32               to Top Secret information.  When compartmented security
   33               is used, a clearance also includes the categories a
   34               person is eligible to access.  In addition to the
   35               eligibility afforded a person by his clearance, he
   36               must also have the need to know the classified
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37                information before he is given access.;
38      APPLIES TO:                          classification-level;
39
40  MEMO                                      system-philosophy-memo;
41      DESCRIPTION;
42                      The philosophy of the secure computer system will
43                be such that the system will control the various shared
44                resources.  Hence the user will only be able to influence
45                allocation decisions in a secondary way.  Specifically,
46                he can ask for a resource but not control the absolute
47                time or address of the resource.  It is essential that any
48                other paths which might allow the user to access
49                information (from any device) without the access controls
50                of the system be eliminated.;
51      APPLIES TO:                          security-control-system,
52                                           security-control-input,
53                                           security-control-output,
54                                           security-control-interface,
55                                           security-control-data-base;
56
57  PROBLEM-DEFINER                           james-m-amster;
58      MAILBOX:                             isdos-project-ann-arbor;
59      RESPONSIBLE FOR:                     object-information,
60                                           subject-information,
61                                           incident-information,
62                                           reference-monitor-subject;
63
64  PROBLEM-DEFINER                           michel-j-bastarache;
65      MAILBOX:                             isdos-project-ann-arbor;
66      RESPONSIBLE FOR:                     auditing-system,
67                                           administrative-security-system,
68                                           reference-monitor,
69                                           system-security-administrator;
70
71  EOF EOF EOF EOF EOF
```

Security-control-example

Name Generation

PARAMETERS FOR: NG

```
PRINT PUNCH EMPTY SELECTION='PD=james-m-amster' ORDER=BYTYPE
```

1	incident-information	ENTITY
2	object-information	ENTITY
3	subject-information	ENTITY
4	reference-monitor-subject	INTERFACE

Security-control-example

DICTIONARY REPORT

PARAMETERS FOR: DICT

FILE NOINDEX DESCRIPTION SYNONYMS KEYWORDS RESPONSIBLE-PD NUM-SPACE=2

1 incident-information ENTITY

DESCRIPTION:
This information holds data about where and when an incident has occurred.

SYNONYMS: incinfo

RESP PD: james-m-amster

2 object-information ENTITY

DESCRIPTION:
This information holds identification, security, and location information for a particular object.

SYNONYMS: objinfo

RESP PD: james-m-amster

3 subject-information ENTITY

DESCRIPTION:
This information holds identification and security data about a reference monitor subject.

SYNONYMS: subinfo

RESP PD: james-m-amster

4 reference-monitor-subject INTERFACE

Security-control-example

DICTIONARY REPORT

DESCRIPTION:

A reference monitor subject may be a user, a process, or a job which generates requests on the reference monitor.

SYNONYMS: rmonsub

KEYWORDS: level-2

RESP PD: james-m-amster

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='MEMO' ORDER=BYTYPE

1	category-set-memo	MEMO
2	clearance-memo	MEMO
3	system-philosophy-memo	MEMO

Security-control-example

PUNCHED COMMENT ENTRIES

PARAMETERS FOR: PCOM

FILE DESCRIPTION NOPROCEDURE NOVOLATILITY NOVOLATILITY-MEMBER NOVOLATILITY-SET NODERIVATION NOTRUE-WHILE NOFALSE-WHILE PRINT PUNCH

```
1*   category-set-memo
     DESCRIPTION;
          1
          2                  In reference to a person (or process), a category
          3             set refers to the set of compartments a person is
          4             eligible to access.  A compartment in this context is
          5             an orthogonal subdivision of the classification
          6             levels.  A compartment is like a FORMAL NEED TO KNOW
          7             authorization to information of a certain topic
          8             without consideration of classification level.
          9                  In reference to documents, files, or other objects
         10             a category set refers to the possible information
         11             sources used to create the object.  Thus, a category set
         12             with several categories or compartments would indicate
         13             that the object should be handled with extra caution
         14             o objects which would intersect the sensitive areas
                        of each of the categories in the set.;

2*   clearance-memo
     DESCRIPTION;
          1                  In this specification, clearance is defined as the
          2             eligibility of a person (or process or job) to access
          3             information of a certain classification level (or
          4             lower).  For example, a person with a Secret clearance
          5             is eligible to access information with classification
          6             levels Unclassified to Secret, but may not have access
          7             to Top Secret information.  When compartmented security
          8             is used, a clearance also includes the categories a
          9             person is eligible to access.  In addition to the
         10             eligibility afforded a person by his clearance, he
         11             must also have the need to know the classified
         12             information before he is given access.;

3*   system-philosophy-memo
     DESCRIPTION;
          1                  The philosophy of the secure computer system will
```

PUNCHED COMMENT ENTRIES

```
2                be such that the system will control the various shared
3                resources.  Hence the user will only be able to influence
4                allocation decisions in a secondary way.  Specifically,
5                he can ask for a resource but not control the absolute
6                time or address of the resource.  It is essential that any
7                other paths which might allow the user to access
8                information (from any device) without the access controls
9                of the system be eliminated.;
```

Security-control-example

NAME LIST

PARAMETERS FOR: NL

ORDER=BYTYPE

	NAME	TYPE	SYNONYM	
1	occurrences	ATTRIBUTE		-
2	parameter-value	ATTRIBUTE		-
3	specification-derivation	ATTRIBUTE	speder	
4	explicit	ATTRIBUTE-VALUE		-
5	fixed	ATTRIBUTE-VALUE		-
6	implicit	ATTRIBUTE-VALUE		-
7	scheduled	ATTRIBUTE-VALUE		-
8	subject-to-change	ATTRIBUTE-VALUE		-
9	unscheduled	ATTRIBUTE-VALUE		-
10	varying	ATTRIBUTE-VALUE		-
11	create-access-relation-fin	CONDITION		-
12	get-read-request-made	CONDITION		-
13	need-to-know-check-passes	CONDITION		-
14	sub-obj-sec-level-check-passes	CONDITION		-
15	category-set	ELEMENT		-
16	classification-level	ELEMENT		-
17	consol-nr	ELEMENT		-
18	date-time	ELEMENT		-
19	decision-type	ELEMENT		-
20	error-code	ELEMENT		-
21	incident-type	ELEMENT		-
22	object-id	ELEMENT		-
23	object-location	ELEMENT		-
24	receiving-subject-id	ELEMENT		-
25	requesting-subject-id	ELEMENT		-
26	security-id	ELEMENT		-
27	subject-id	ELEMENT		-
28	usage-attribute	ELEMENT		-
29	validation-code	ELEMENT		-
30	incident-information	ENTITY	incinfo	
31	object-information	ENTITY	objinfo	
32	subject-information	ENTITY	subinfo	
33	access-usage-check-fails	EVENT		-
34	access-usage-check-succeeds	EVENT		-

Security-control-example

NAME LIST

	NAME	TYPE	SYNONYM
35	create-access-relation-succ	EVENT	-
36	create-object-information-succ	EVENT	-
37	delete-access-relation-succ	EVENT	-
38	init-create-object-procedure	EVENT	-
39	init-release-usage-attr-proc	EVENT	-
40	initiate-get-read-procedure	EVENT	-
41	need-to-know-check-fails	EVENT	-
42	need-to-know-check-succeeds	EVENT	-
43	occur-create-object-request	EVENT	-
44	occur-release-usage-attr-req	EVENT	-
45	occurrence-get-read-request	EVENT	-
46	sub-obj-sec-level-check-fails	EVENT	-
47	sub-obj-sec-level-check-succ	EVENT	-
48	audit-information	GROUP	audinfo
49	inc-audit-information	GROUP	incaudinfo
50	obj-audit-information	GROUP	objaudinfo
51	obj-inc-audit-information	GROUP	objincaudinfo
52	obj-sec-level	GROUP	-
53	sub-audit-information	GROUP	subaudinfo
54	sub-curr-sec-level	GROUP	-
55	sub-inc-audit-information	GROUP	subincaudinfo
56	sub-max-sec-level	GROUP	-
57	sub-obj-audit-information	GROUP	subobjaudinfo
58	sub-obj-inc-audit-information	GROUP	subobjincaudinfo
59	administrative-security-comd	INPUT	admscom
60	auditing-request	INPUT	audreq
61	change-obj-sec-level-request	INPUT	kf11req
62	change-sub-curr-sec-level-req	INPUT	kf10req
63	change-sub-max-sec-level-comd	INPUT	chasubmaxseclevcom
64	create-object-request	INPUT	kf8req
65	create-subject-command	INPUT	cresubcom
66	delete-object-request	INPUT	kf9req
67	delete-subject-command	INPUT	delsubcom
68	dump-audit-request	INPUT	dumaudreq
69	get-execute-request	INPUT	kf3req
70	get-read-request	INPUT	kf1req
71	get-read-write-request	INPUT	kf4req
72	get-write-request	INPUT	kf2req
73	give-usage-attr-request	INPUT	kf6req

Security-control-example

NAME LIST

	NAME	TYPE	SYNONYM
74	inc-audit-request	INPUT	incaudreq
75	link-reference-monitor-comd	INPUT	linrmoncom
76	obj-audit-request	INPUT	objaudreq
77	obj-inc-audit-request	INPUT	objincaudreq
78	reference-monitor-request	INPUT	rmonreq
79	release-usage-attr-request	INPUT	kf5req
80	rescind-usage-attr-request	INPUT	kf7req
81	security-control-input	INPUT	scinp
82	sub-audit-request	INPUT	subaudreq
83	sub-inc-audit-request	INPUT	subincaudreq
84	sub-obj-audit-request	INPUT	subobjaudreq
85	sub-obj-inc-audit-request	INPUT	subobjincaudreq
86	reference-monitor-subject	INTERFACE	rmonsub
87	security-control-interface	INTERFACE	scint
88	system-security-administrator	INTERFACE	ssa ssadm
89	day	INTERVAL	-
90	hour	INTERVAL	-
91	minute	INTERVAL	-
92	month	INTERVAL	-
93	week	INTERVAL	-
94	year	INTERVAL	-
95	level-1	KEYWORD	-
96	level-2	KEYWORD	-
97	low-level	KEYWORD	-
98	isios-project-ann-arbor	MAILBOX	-
99	category-set-memo	MEMO	-
100	clearance-memo	MEMO	-
101	system-philosophy-memo	MEMO	-
102	administrative-security-resp	OUTPUT	admsres
103	audit-trail	OUTPUT	audtra
104	change-obj-sec-level-decision	OUTPUT	kf11dec
105	change-sub-curr-sec-level-dec	OUTPUT	kf10dec
106	change-sub-max-sec-level-resp	OUTPUT	chasubmaxseclevres
107	create-object-decision	OUTPUT	kf8dec
108	create-subject-response	OUTPUT	cresubres
109	delete-object-decision	OUTPUT	kf9dec
110	delete-subject-response	OUTPUT	delsubres
111	dump-audit-trail	OUTPUT	dumaudtra

Security-control-example

NAME LIST

	NAME	TYPE	SYNONYM
112	get-execute-decision	OUTPUT	kf3dec
113	get-read-decision	OUTPUT	kf1dec
114	get-read-write-decision	OUTPUT	kf4dec
115	get-write-decision	OUTPUT	kf2dec
116	give-usage-attr-decision	OUTPUT	kf6dec
117	inc-audit-trail	OUTPUT	incaudtra
118	link-reference-monitor-resp	OUTPUT	linrmontes
119	obj-audit-trail	OUTPUT	objaudtra
120	obj-inc-audit-trail	OUTPUT	objincaudtra
121	reference-monitor-decision	OUTPUT	rmondec
122	release-usage-attr-decision	OUTPUT	kf5dec
123	rescind-usage-attr-decision	OUTPUT	kf7dec
124	security-control-output	OUTPUT	scout
125	sub-audit-trail	OUTPUT	subaudtra
126	sub-inc-audit-trail	OUTPUT	subincaudtra
127	sub-obj-audit-trail	OUTPUT	subobjaudtra
128	sub-obj-inc-audit-trail	OUTPUT	subobjincaudtra
129	james-m-amster	PROBLEM-DEFINER	-
130	michel-j-bastarache	PROBLEM-DEFINER	-
131	administrative-security-system	PROCESS	adssys
132	auditing-system	PROCESS	aulsys
133	change-obj-sec-level	PROCESS	kf11
134	change-sub-curr-sec-level	PROCESS	kf10
135	change-sub-max-sec-level	PROCESS	chasubmaxseclev
136	check-access-usage	PROCESS	-
137	check-need-to-know-usage	PROCESS	-
138	check-sub-obj-sec-levels	PROCESS	-
139	create-access-relation	PROCESS	-
140	create-object	PROCESS	kf8
141	create-object-information	PROCESS	-
142	create-subject	PROCESS	cresub
143	delete-access-relation	PROCESS	-
144	delete-object	PROCESS	kf9
145	delete-object-information	PROCESS	-
146	delete-subject	PROCESS	delsub
147	dump-audit	PROCESS	dumaud
148	generate-decision	PROCESS	-
149	get-execute	PROCESS	kf3
150	get-read	PROCESS	kf1

Security-control-example

NAME LIST

	NAME	TYPE	SYNONYM
151	get-read-write	PROCESS	kf4
152	get-write	PROCESS	kf2
153	give-usage-attr	PROCESS	kf6
154	inc-audit	PROCESS	incaud
155	link-reference-monitor	PROCESS	linrmon
156	obj-audit	PROCESS	objaud
157	obj-inc-audit	PROCESS	objincaud
158	produce-audit-incident	PROCESS	-
159	reference-monitor	PROCESS	access-control-system rmon
160	release-usage-attr	PROCESS	kf5
161	rescind-usage-attr	PROCESS	kf7
162	security-control-system	PROCESS	scs scsys
163	sub-audit	PROCESS	subaud
164	sub-inc-audit	PROCESS	subincaud
165	sub-obj-audit	PROCESS	subobjaud
166	sub-obj-inc-audit	PROCESS	subobjincaud
167	obj-inc-audit-relation	RELATION	-
168	sub-inc-audit-relation	RELATION	-
169	sub-obj-audit-relation	RELATION	-
170	subject-access-to-object	RELATION	-
171	subject-need-to-know-object	RELATION	-
172	unclassified	SECURITY	-
173	auditing-system-data-base	SET	audsysdb
174	confidential-file	SET	confile
175	reference-monitor-data-base	SET	rmondb
176	secret-file	SET	secfile
177	security-control-data-base	SET	scdb
178	top-secret-file	SET	topsecfile
179	unclassified-file	SET	uncfile
180	scs-specification	SOURCE	-
181	scs-statement-of-need	SOURCE	-
182	create-object-distribution	SYSTEM-PARAMETER	-
183	get-read-distribution	SYSTEM-PARAMETER	-
184	many	SYSTEM-PARAMETER	-
185	number-of-categories	SYSTEM-PARAMETER	-
186	number-of-dump-audit	SYSTEM-PARAMETER	-
187	number-of-incidents	SYSTEM-PARAMETER	-

Security-control-example

NAME LIST

	NAME	TYPE	SYNONYM
188	number-of-levels	SYSTEM-PARAMETER	-
189	number-of-obj-audit	SYSTEM-PARAMETER	-
190	number-of-objects	SYSTEM-PARAMETER	-
191	number-of-sub-audit	SYSTEM-PARAMETER	-
192	number-of-subjects	SYSTEM-PARAMETER	-
193	release-usage-attr-req-distr	SYSTEM-PARAMETER	-
194	total-objects-and-subjects	SYSTEM-PARAMETER	-

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ATTR' ORDER=BYTYPE

1	occurrences	ATTRIBUTE
2	parameter-value	ATTRIBUTE
3	specification-derivation	ATTRIBUTE

Security-control-example

ATTRIBUTE REPORT

PARAMETERS FOR: PAV

FILE

1* ATTRIBUTE: occurrences

	APPLIES TO:	VALUE:
1	reference-monitor-request	unscheduled
2	administrative-security-comd	unscheduled
3	auditing-request	scheduled

2* ATTRIBUTE: parameter-value

	APPLIES TO:	VALUE:
1	number-of-subjects	varying
2	number-of-objects	varying
3	number-of-incidents	varying
4	number-of-levels	fixed
5	number-of-categories	fixed
6	total-objects-and-subjects	varying
7	number-of-dump-audit	subject-to-change
8	number-of-obj-audit	subject-to-change
9	number-of-sub-audit	subject-to-change

3* ATTRIBUTE: specification-derivation

	APPLIES TO:	VALUE:
1	security-control-system	explicit
2	security-control-input	implicit
3	security-control-output	implicit
4	security-control-interface	explicit
5	security-control-data-base	implicit

Security-control-example

PROCESS STRUCTURE

PARAMETERS FOR: STR

PROCESS INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 check-access-usage
    2     1 check-need-to-know-usage
    3     1 check-sub-obj-sec-levels
    4     1 create-access-relation
    5     1 create-object-information
    6     1 delete-access-relation
    7     1 delete-object-information
    8     1 generate-decision
    9     1 produce-audit-incident
   10     1 security-control-system
   11      2   reference-monitor
   12       3     get-read
   13       3     get-write
   14       3     get-execute
   15       3     get-read-write
   16       3     release-usage-attr
   17       3     give-usage-attr
   18       3     rescind-usage-attr
   19       3     create-object
   20       3     delete-object
   21       3     change-sub-curr-sec-level
   22       3     change-obj-sec-level
   23      2   administrative-security-system
   24       3     create-subject
   25       3     delete-subject
```

Security-control-example

PROCESS STRUCTURE

```
COUNT LEVEL NAME
   26       3      change-sub-max-sec-level
   27       3      link-reference-monitor
   28     2    auditing-system
   29       3      sub-obj-audit
   30       3      sub-inc-audit
   31       3      sub-obj-inc-audit
   32       3      sub-audit
   33       3      obj-inc-audit
   34       3      obj-audit
   35       3      inc-audit
   36       3      dump-audit
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	12	2	3	3	23				

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='PROC' ORDER=BYTYPE

1	administrative-security-system	PROCESS
2	auditing-system	PROCESS
3	change-obj-sec-level	PROCESS
4	change-sub-curr-sec-level	PROCESS
5	change-sub-max-sec-level	PROCESS
6	check-access-usage	PROCESS
7	check-need-to-know-usage	PROCESS
8	check-sub-obj-sec-levels	PROCESS
9	create-access-relation	PROCESS
10	create-object	PROCESS
11	create-object-information	PROCESS
12	create-subject	PROCESS
13	delete-access-relation	PROCESS
14	delete-object	PROCESS
15	delete-object-information	PROCESS
16	delete-subject	PROCESS
17	dump-audit	PROCESS
18	generate-decision	PROCESS
19	get-execute	PROCESS
20	get-read	PROCESS
21	get-read-write	PROCESS
22	get-write	PROCESS
23	give-usage-attr	PROCESS
24	inc-audit	PROCESS
25	link-reference-monitor	PROCESS
26	obj-audit	PROCESS
27	obj-inc-audit	PROCESS
28	produce-audit-incident	PROCESS
29	reference-monitor	PROCESS
30	release-usage-attr	PROCESS
31	rescind-usage-attr	PROCESS
32	security-control-system	PROCESS
33	sub-audit	PROCESS
34	sub-inc-audit	PROCESS
35	sub-obj-audit	PROCESS
36	sub-obj-inc-audit	PROCESS

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: PPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=79 CMARG=1 HMARG=40 DESG ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 PROCESS                                  administrative-security-system;
 2     SYNONYMS ARE:                        admssys;
 3     DESCRIPTION;
 4                 The system will define the administrative
 5           functions of the system security administrator, and will
 6           support his responsibility for maintaining control of
 7           users id's, passwords, and user classification level and
 8           category set.;
 9     KEYWORDS:                            level-2;
10     PART OF:                             security-control-system;
11     SUBPARTS ARE:                        create-subject,
12                                          delete-subject,
13                                          change-sub-max-sec-level,
14                                          link-reference-monitor;
15     RECEIVES:                            administrative-security-comd;
16     GENERATES:                           administrative-security-resp;
17     DERIVES:                             administrative-security-resp;
18     UPDATES:                             reference-monitor-data-base;
19     USES:                                administrative-security-comd;
20     RESPONSIBLE-PROBLEM-DEFINER IS:      michel-j-bastarache;
21
22 PROCESS                                  auditing-system;
23     SYNONYMS ARE:                        audsys;
24     DESCRIPTION;
25                 The system will provide an automatic capabilty to
26           collect and record data regarding security related
27           actions.;
28     KEYWORDS:                            level-2;
29     PART OF:                             security-control-system;
30     SUBPARTS ARE:                        sub-obj-audit,
31                                          sub-inc-audit,
32                                          sub-obj-inc-audit,
33                                          sub-audit,
34                                          obj-inc-aulit,
35                                          obj-audit,
36                                          inc-audit,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37                                      dump-audit;
38      RECEIVES:                       auditing-request;
39      GENERATES:                      audit-trail;
40      DERIVES:                        audit-trail;
41      USES:                           auditing-request,
42                                      auditing-system-data-base;
43      RESPONSIBLE-PROBLEM-DEFINER IS: michel-j-bastarache;
44
45  PROCESS                              change-obj-sec-level;
46      SYNONYMS ARE:                   kf11;
47      DESCRIPTION;
48                      This process decides whether or not subject with
49                  subject-id may revise the security level of object
50                  with object-id to the value of obj-sec-level.;
51      PART OF:                        reference-monitor;
52      DERIVES:                        change-obj-sec-level-decision;
53      USES:                           change-obj-sec-level-request;
54
55  PROCESS                              change-sub-curr-sec-level;
56      SYNONYMS ARE:                   kf10;
57      DESCRIPTION;
58                      This process decides whether or not subject with
59                  subject-id may change his current security level to
60                  sub-curr-sec-level.;
61      PART OF:                        reference-monitor;
62      DERIVES:                        change-sub-curr-sec-level-dec;
63      USES:                           change-sub-curr-sec-level-req;
64
65  PROCESS                              change-sub-max-sec-level;
66      SYNONYMS ARE:                   chasubmaxseclev;
67      DESCRIPTION;
68                      This process allows the system security
69                  administrator with security-id to change the maximum
70                  security level of subject with subject-id to
71                  sub-max-sec-level.;
72      PART OF:                        administrative-security-system;
73      DERIVES:                        change-sub-max-sec-level-resp;
74      USES:                           change-sub-max-sec-level-comd;
75
76  PROCESS                              check-access-usage;
77      DESCRIPTION;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
                    This process checks if a subject-access-to-
               object relation with usage attribute exist between
               subject with subject-id and object with object-id.;
    KEYWORDS:                          low-level;
    UTILIZED BY:                       release-usage-attr;
    DERIVES:                           error-code
      USING:                           subject-id,
                                       object-id,
                                       usage-attribute;
    TERMINATION-CAUSES:                access-usage-check-fails,
                                       access-usage-check-succeeds;
    TRIGGERED BY:                      init-release-usage-attr-proc;

PROCESS                                 check-need-to-know-usage;
    DESCRIPTION;
                    This process checks if a subject-need-to-know-
               object relation with usage-attribute  exists
               between subject with subject-id and object with
               object-id.;
    KEYWORDS:                          low-level;
    UTILIZED BY:                       get-read;
    DERIVES:                           error-code
      USING:                           subject-id,
                                       object-id,
                                       usage-attribute;
    TERMINATION-CAUSES:                need-to-know-check-fails,
                                       need-to-know-check-succeeds;
    TRIGGERED BY:                      initiate-get-read-procedure;

PROCESS                                 check-sub-obj-sec-levels;
    DESCRIPTION;
                    This process checks if sub-curr-sec-level
               exceeds obj-sec-level.  For example, security level 1
               exceeds security level 2 if the classification level
               of security level 1 is higher than the classification
               level of security level 2 and the category set of
               security level 2 is a subset of the category set of
               security level 1.;
    KEYWORDS:                          low-level;
    UTILIZED BY:                       get-read,
                                       create-object;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
119     DERIVES:                        error-code
120       USING:                        sub-curr-sec-level,
121                                     obj-sec-level;
122     TERMINATION-CAUSES:             sub-obj-sec-level-check-fails,
123                                     sub-obj-sec-level-check-succ;
124     TRIGGERED BY:                   need-to-know-check-succeeds,
125                                     init-create-object-procedure;
126
127 PROCESS                             create-access-relation;
128     DESCRIPTION;
129                     This process creates a subject-access-to-object
130               relation between subject with subject-id and object with
131               object-id.;
132     KEYWORDS:                       low-level;
133     UTILIZED BY:                    get-read;
134     MAINTAINS:                      subject-access-to-object;
135     UPDATES:                        usage-attribute
136       USING:                        subject-id,
137                                     object-id;
138     TERMINATION-CAUSES:             create-access-relation-succ;
139     TRIGGERED BY:                   sub-obj-sec-level-check-succ;
140
141 PROCESS                             create-object;
142     SYNONYMS ARE:                   kf8;
143     DESCRIPTION;
144                     This process decides whether or not subject with
145               subject-id may add an object to the directory
146               hierarchy directly below directory object with
147               object-id.  This added object is requested to have
148               security level obj-sec-level.;
149     PART OF:                        reference-monitor;
150     UTILIZES:                       check-sub-obj-sec-levels,
151                                     create-object-information,
152                                     produce-audit-incident,
153                                     generate-decision;
154     DERIVES:                        create-object-decision;
155     USES:                           create-object-request;
156     PROCEDURE;
157             1. Check if subject's sub-curr-sec-level exceeds object's
158                obj-sec-level.  If answer is no, go to step 3.
159             2. Create an occurrence of object-information with
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
160                 object-id in the appropriate file based on the value
161                 of obj-sec-level.
162               3. Produce an audit incident and generate a decision
163                 based on the value of error-code and then terminate.;
164     INCEPTION-CAUSES:                   init-create-object-procedure;
165     TRIGGERED BY:                       occur-create-object-request;
166
167 PROCESS                                  create-object-information;
168     DESCRIPTION;
169                       This process creates an occurrence of object-
170                 information in the appropriate set according to the value
171                 of obj-sec-level and sets the value of object-location.;
172     KEYWORDS:                           low-level;
173     UTILIZED BY:                        create-object;
174     DERIVES:                            object-information
175       USING:                            object-id,
176                                         obj-sec-level;
177     TERMINATION-CAUSES:                 create-object-information-succ;
178     TRIGGERED BY:                       sub-obj-sec-level-check-succ;
179
180 PROCESS                                  create-subject;
181     SYNONYMS ARE:                       cresub;
182     DESCRIPTION;
183                       This process allows the system security
184                 administrator with security-id to create the record
185                 of a subject with subject-id.  This subject will
186                 be assigned maximum security level sub-max-sec-level and
187                 current security level obj-sec-level.;
188     PART OF:                            administrative-security-system;
189     DERIVES:                            create-subject-response;
190     USES:                               create-subject-command;
191
192 PROCESS                                  delete-access-relation;
193     DESCRIPTION;
194                       This process deletes a subject-access-to-object
195                 relation with usage attribute between subject with
196                 subject-id and object with object-id.;
197     KEYWORDS:                           low-level;
198     UTILIZED BY:                        release-usage-attr;
199     DERIVES:                            error-code
200       USING:                            subject-id,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
242                base.;
243     PART OF:                              auditing-system;
244     DERIVES:                              dump-audit-trail;
245     USES:                                 dump-audit-request;
246     HAPPENS:
247       number-of-dump-audit TIMES-PER      month;
248
249 PROCESS                                    generate-decision;
250     DESCRIPTION;
251                   This process derives a decision type based on
252               the value of error-code.;
253     KEYWORDS:                             low-level;
254     UTILIZED BY:                          get-read,
255                                           release-usage-attr,
256                                           create-object;
257     DERIVES:                              decision-type
258       USING:                              error-code;
259     TRIGGERED BY:                         need-to-know-check-fails,
260                                           sub-obj-sec-level-check-fails,
261                                           create-access-relation-succ,
262                                           delete-access-relation-succ,
263                                           access-usage-check-fails,
264                                           create-object-information-succ;
265
266 PROCESS                                    get-execute;
267     SYNONYMS ARE:                         kf3;
268     DESCRIPTION;
269                   This process decides whether or not to enable
270               subject with subject-id execute access to object with
271               object-id.  This process is only useful if the
272               object-id requested is a procedure.;
273     PART OF:                              reference-monitor;
274     DERIVES:                              get-execute-decision;
275     USES:                                 get-execute-request;
276
277 PROCESS                                    get-read;
278     SYNONYMS ARE:                         kf1;
279     DESCRIPTION;
280                   This process decides whether or not to enable
281               subject with subject-id read only access to object with
282               object-id.;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
283     PART OF:                              reference-monitor;
284     UTILIZES:                             check-need-to-know-usage,
285                                           check-sub-obj-sec-levels,
286                                           create-access-relation,
287                                           produce-audit-incident,
288                                           generate-decision;
289     DERIVES:                              get-read-decision;
290     USES:                                 get-read-request;
291     PROCEDURE;
292             1. Check if subject-need-to-know-object relation exists
293                with usage-attribute value of read between subject with
294                subject-id and object with object-id.  If answer is
295                no, go to step 4.
296             2. Otherwise, check if subject's sub-curr-sec-level
297                exceeds object's obj-sec-level.  If answer is no,
298                go to step 4.
299             3. Otherwise, create a subject-access-to-object relation
300                with usage-attribute between subject with subject-id
301                and object with object-id.
302             4. Produce an audit incident and generate a decision
303                based on the value of error-code and then terminate.;
304     INCEPTION-CAUSES:                     initiate-get-read-procedure;
305     TRIGGERED BY:                         occurrence-get-read-request;
306
307 PROCESS                                    get-read-write;
308     SYNONYMS ARE:                         kf4;
309     DESCRIPTION;
310                     This process decides whether or not to enable
311               subject with subject-id read and write access to object
312               with object-id.;
313     PART OF:                              reference-monitor;
314     DERIVES:                              get-read-write-decision;
315     USES:                                 get-read-write-request;
316
317 PROCESS                                    get-write;
318     SYNONYMS ARE:                         kf2;
319     DESCRIPTION;
320                     This process decides whether or not to enable
321               subject with subject-id write only access to object
322               with object-id.;
323     PART OF:                              reference-monitor;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
324     DERIVES:                        get-write-decision;
325     USES:                           get-write-request;
326
327 PROCESS                             give-usage-attr;
328     SYNONYMS ARE:                   kf6;
329     DESCRIPTION;
330                 This process decides whether or not subject with
331             requesting-subject-id may give subject with
332             receiving-subject-id usage attribute access to object
333             with object-id.;
334     PART OF:                        reference-monitor;
335     DERIVES:                        give-usage-attr-decision;
336     USES:                           give-usage-attr-request;
337
338 PROCESS                             inc-audit;
339     SYNONYMS ARE:                   incaud;
340     DESCRIPTION;
341                 This process allows the system security
342             administrator obtain all sets of sub-obj-audit-
343             information for a particular incident with incident-
344             type.;
345     PART OF:                        auditing-system;
346     DERIVES:                        inc-audit-trail;
347     USES:                           inc-audit-request;
348
349 PROCESS                             link-reference-monitor;
350     SYNONYMS ARE:                   linrmon;
351     DESCRIPTION;
352                 This process allows the system security
353             administrator with security-id to perform all
354             reference monitor functions without security checks
355             by the reference monitor.  He may perform these
356             functions for any subject-id registered in the system.
357             This process will effectively link the administrative
358             security system to the reference monitor with the only
359             security check being that of the system security
360             administrator's security-id.;
361     PART OF:                        administrative-security-system;
362     DERIVES:                        link-reference-monitor-resp;
363     USES:                           link-reference-monitor-cmd;
364
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
365 PROCESS                                  obj-audit;
366     SYNONYMS ARE:                       objaud;
367     DESCRIPTION;
368                     This process allows the system security
369               administrator obtain all sets of sub-inc-audit-
370               information for a particular object with object-id.;
371     PART OF:                            auditing-system;
372     DERIVES:                            obj-audit-trail;
373     USES:                               obj-audit-request;
374     HAPPENS:
375       number-of-obj-audit TIMES-PER     month;
376
377 PROCESS                                  obj-inc-audit;
378     SYNONYMS ARE:                       objincaud;
379     DESCRIPTION;
380                     This process allows the system security
381               administrator obtain all sets of sub-audit-information
382               for a particular object with object-id and incident
383               with incident-id.;
384     PART OF:                            auditing-system;
385     DERIVES:                            obj-inc-audit-trail;
386     USES:                               obj-inc-audit-request;
387
388 PROCESS                                  produce-audit-incident;
389     DESCRIPTION;
390                     This process produces an occurrence of incident-
391               information in the auditing system data base based on
392               the value of error-code.;
393     KEYWORDS:                           low-level;
394     UTILIZED BY:                        get-read,
395                                         release-usage-attr,
396                                         create-object;
397     DERIVES:                            incident-information
398       USING:                            error-code;
399     TRIGGERED BY:                       need-to-know-check-fails,
400                                         sub-obj-sec-level-check-fails,
401                                         access-usage-check-fails;
402
403 PROCESS                                  reference-monitor;
404     SYNONYMS ARE:                       access-control-system,
405                                         rmon;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
406     DESCRIPTION;
407                     The system will provide controls which will allow
408               users to operate concurrently while preventing the
409               release of information to unauthorized users.  The
410               system will also prevent inadvertent violation of need
411               to know access to data. In addition to providing the
412               primary access controls for this environment, the
413               system will provide programs which perform subsidiary
414               security control functions.
415                     The capability must be provided for the system
416               hardware to check the validity of all arguements
417               utilized in calling the operating system.;
418     KEYWORDS:                              level-2;
419     PART OF:                               security-control-system;
420     SUBPARTS ARE:                          get-read,
421                                            get-write,
422                                            get-execute,
423                                            get-read-write,
424                                            release-usage-attr,
425                                            give-usage-attr,
426                                            rescind-usage-attr,
427                                            create-object,
428                                            delete-object,
429                                            change-sub-curr-sec-level,
430                                            change-obj-sec-level;
431     RECEIVES:                              reference-monitor-request;
432     GENERATES:                             reference-monitor-decision;
433     DERIVES:                               reference-monitor-decision;
434     UPDATES:                               auditing-system-data-base;
435     USES:                                  reference-monitor-request,
436                                            reference-monitor-data-base;
437     RESPONSIBLE-PROBLEM-DEFINER IS:        michel-j-bastarache;
438
439 PROCESS                                     release-usage-attr;
440     SYNONYMS ARE:                          kf5;
441     DESCRIPTION;
442                     This process releases usage attribute access
443               to object with object-id from subject with subject-id.;
444     PART OF:                               reference-monitor;
445     UTILIZES:                              check-access-usage,
446                                            delete-access-relation,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
447                                     produce-audit-incident,
448                                     generate-decision;
449     DERIVES:                        release-usage-attr-decision;
450     USES:                           release-usage-attr-request;
451     PROCEDURE;
452             1. Check if subject-access-to-object relation exists
453                with usage-attribute between subject with subject-id
454                and object with object-id.  If answer is no, go to
455                step 3.
456             2. Otherwise, delete the relation.
457             3. Produce an audit incident and generate a decision based
458                on the value of error-code and then terminate.;
459     INCEPTION-CAUSES:               init-release-usage-attr-proc;
460     TRIGGERED BY:                   occur-release-usage-attr-req;
461
462 PROCESS                              rescind-usage-attr;
463     SYNONYMS ARE:                   kf7;
464     DESCRIPTION;
465                 This process decides whether or not subject
466               with requesting-subject-id may take usage attribute
467               access of object with object-id from subject with
468               receiving-subject-id.;
469     PART OF:                        reference-monitor;
470     DERIVES:                        rescind-usage-attr-decision;
471     USES:                           rescind-usage-attr-request;
472
473 PROCESS                              security-control-system;
474     SYNONYMS ARE:                   scs,
475                                     scsys;
476     DESCRIPTION;
477                 The system will provide a means to allow users to
478               process information concurrently while providing
479               reasonable assurance that no unauthorized release of
480               information shall take place.  The security features must
481               be an integral part of the operating system.  The
482               contractor can assume that the physical installation
483               will be secured to the highest level of information in
484               the system.;
485     SER-MEMO:                       system-philosophy-memo;
486     KEYWORDS:                       level-1;
487     ATTRIBUTES ARE:
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
488       specification-derivation:        explicit;
489     SUBPARTS ARE:                      reference-monitor,
490                                        administrative-security-system,
491                                        auditing-system;
492     RECEIVES:                          security-control-input;
493     GENERATES:                         security-control-output;
494     SECURITY IS:                       unclassified;
495     SOURCE IS:                         scs-statement-of-need,
496                                        scs-specification;
497
498 PROCESS                                sub-audit;
499     SYNONYMS ARE:                      subaud;
500     DESCRIPTION;
501                     This process allows the system security
502               administrator obtain all sets of obj-inc-audit-
503               information for a particular subject with subject-id.;
504     PART OF:                           auditing-system;
505     DERIVES:                           sub-audit-trail;
506     USES:                              sub-audit-request;
507     HAPPENS:
508       number-of-sub-audit TIMES-PER    month;
509
510 PROCESS                                sub-inc-audit;
511     SYNONYMS ARE:                      subincaud;
512     DESCRIPTION;
513                     This process allows the system security
514               administrator obtain all sets of obj-audit-information
515               for a particular subject with subject-id and incident
516               with incident-type.;
517     PART OF:                           auditing-system;
518     DERIVES:                           sub-inc-audit-trail;
519     USES:                              sub-inc-audit-request;
520
521 PROCESS                                sub-obj-audit;
522     SYNONYMS ARE:                      subobjaud;
523     DESCRIPTION;
524                     This process allows the system security
525               administrator obtain all sets of inc-audit-information
526               for a particular subject with subject-id and object
527               with object-id.;
528     PART OF:                           auditing-system;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
529     DERIVES:                          sub-obj-audit-trail;
530     USES:                             sub-obj-audit-request;
531
532 PROCESS                               sub-obj-inc-audit;
533     SYNONYMS ARE:                     subobjincaud;
534     DESCRIPTION;
535                   This process allows the system security
536              administrator obtain all sets of audit-information
537              for a particular subject with subject-id, object with
538               object-id, and incident with incident-type.;
539     PART OF:                          auditing-system;
540     DERIVES:                          sub-obj-inc-audit-trail;
541     USES:                             sub-obj-inc-audit-request;
542
543 EOF EOF EOF EOF EOF
```

Security-control-example

OUTPUT STRUCTURE

PARAMETERS FOR: STR

OUTPUT INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 security-control-output
    2      2   reference-monitor-decision
    3        3     get-read-decision
    4        3     get-write-decision
    5        3     get-execute-decision
    6        3     get-read-write-decision
    7        3     release-usage-attr-decision
    8        3     give-usage-attr-decision
    9        3     rescind-usage-attr-decision
   10        3     create-object-decision
   11        3     delete-object-decision
   12        3     change-sub-curr-sec-level-dec
   13        3     change-obj-sec-level-decision
   14      2   administrative-security-resp
   15        3     create-subject-response
   16        3     delete-subject-response
   17        3     change-sub-max-sec-level-resp
   18        3     link-reference-monitor-resp
   19      2   audit-trail
   20        3     sub-obj-audit-trail
   21        3     sub-inc-audit-trail
   22        3     sub-obj-inc-audit-trail
   23        3     sub-audit-trail
   24        3     obj-inc-audit-trail
   25        3     obj-audit-trail
   26        3     inc-audit-trail
   27        3     dump-audit-trail
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	3	3	23				

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='OUT' ORDER=BYTYPE

1	administrative-security-resp	OUTPUT
2	audit-trail	OUTPUT
3	change-obj-sec-level-decision	OUTPUT
4	change-sub-curr-sec-level-dec	OUTPUT
5	change-sub-max-sec-level-resp	OUTPUT
6	create-object-decision	OUTPUT
7	create-subject-response	OUTPUT
8	delete-object-decision	OUTPUT
9	delete-subject-response	OUTPUT
10	dump-audit-trail	OUTPUT
11	get-execute-decision	OUTPUT
12	get-read-decision	OUTPUT
13	get-read-write-decision	OUTPUT
14	get-write-decision	OUTPUT
15	give-usage-attr-decision	OUTPUT
16	inc-audit-trail	OUTPUT
17	link-reference-monitor-resp	OUTPUT
18	obj-audit-trail	OUTPUT
19	obj-inc-audit-trail	OUTPUT
20	reference-monitor-decision	OUTPUT
21	release-usage-attr-decision	OUTPUT
22	rescind-usage-attr-decision	OUTPUT
23	security-control-output	OUTPUT
24	sub-audit-trail	OUTPUT
25	sub-inc-audit-trail	OUTPUT
26	sub-obj-audit-trail	OUTPUT
27	sub-obj-inc-audit-trail	OUTPUT

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

```
FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=70 CMARG=1 HMARG=40 DPSG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

 1 OUTPUT                                  administrative-security-resp;
 2     SYNONYMS ARE:                      admsres;
 3     DESCRIPTION;
 4                  These are responses to administrative security
 5             commands and will consist of validations as to
 6             the execution of these commands.;
 7     KEYWORDS:                          level-2;
 8     PART OF:                           security-control-output;
 9     SUBPARTS ARE:                      create-subject-response,
10                                        delete-subject-response,
11                                        change-sub-max-sec-level-resp,
12                                        link-reference-monitor-resp;
13     DERIVED BY:                        administrative-security-system;
14     GENERATED BY:                      administrative-security-system;
15     RECEIVED BY:                       system-security-administrator;
16
17 OUTPUT                                  audit-trail;
18     SYNONYMS ARE:                      audtra;
19     DESCRIPTION;
20                  Security audit trails should contain records of
21             each security incident, and may contain other data
22             as well.;
23     KEYWORDS:                          level-2;
24     PART OF:                           security-control-output;
25     SUBPARTS ARE:                      sub-obj-audit-trail,
26                                        sub-inc-audit-trail,
27                                        sub-obj-inc-audit-trail,
28                                        sub-audit-trail,
29                                        obj-inc-audit-trail,
30                                        obj-audit-trail,
31                                        inc-audit-trail,
32                                        dump-audit-trail;
33     DERIVED BY:                        auditing-system;
34     GENERATED BY:                      auditing-system;
35     RECEIVED BY:                       system-security-administrator;
36
```

Security-control-example

FORMATTED PROBLEM STATEMENT

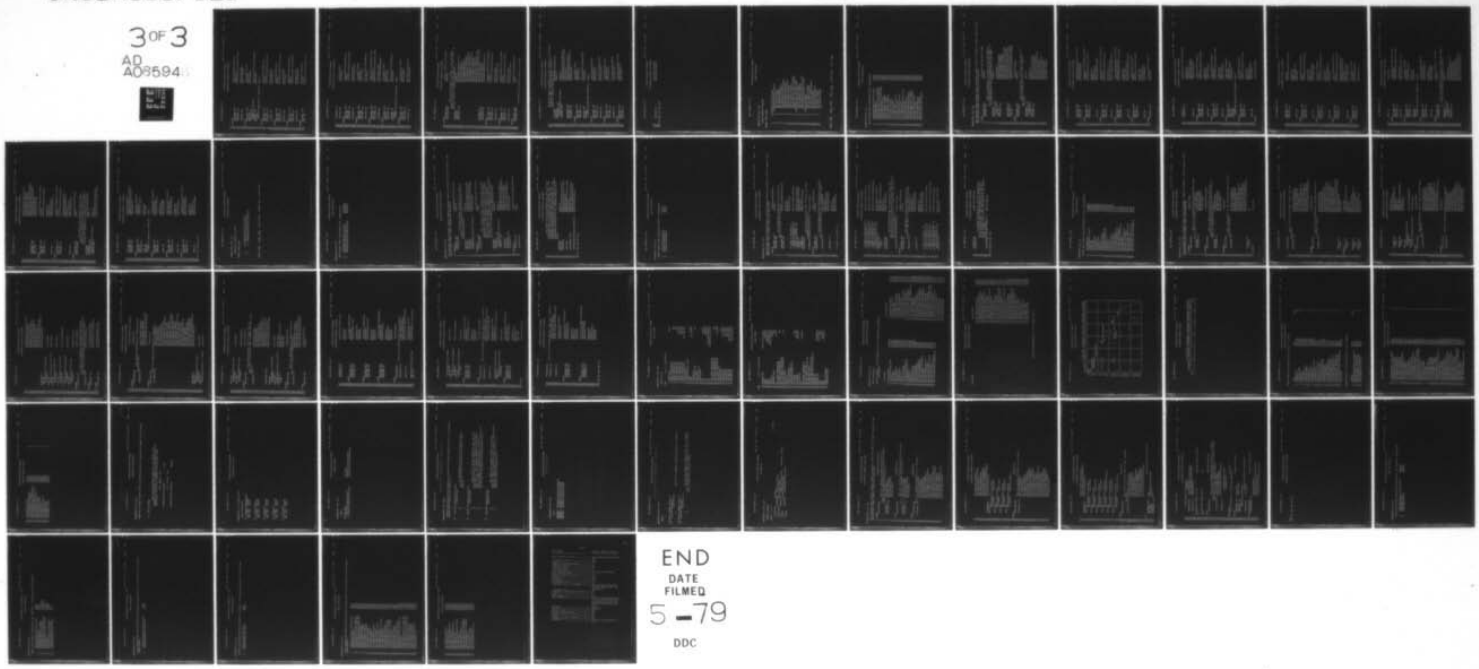
```
37 OUTPUT                          change-obj-sec-level-decision;
38     SYNONYMS ARE:               kf11dec;
39     PART OF:                    reference-monitor-decision;
40     CONSISTS OF:
41                                 decision-type;
42     DERIVED BY:                 change-obj-sec-level;
43
44 OUTPUT                          change-sub-curr-sec-level-dec;
45     SYNONYMS ARE:               kf10dec;
46     PART OF:                    reference-monitor-decision;
47     CONSISTS OF:
48                                 decision-type;
49     DERIVED BY:                 change-sub-curr-sec-level;
50
51 OUTPUT                          change-sub-max-sec-level-resp;
52     SYNONYMS ARE:               chasubmaxseclevres;
53     PART OF:                    administrative-security-resp;
54     CONSISTS OF:
55                                 validation-code;
56     DERIVED BY:                 change-sub-max-sec-level;
57
58 OUTPUT                          create-object-decision;
59     SYNONYMS ARE:               kf8dec;
60     PART OF:                    reference-monitor-decision;
61     CONSISTS OF:
62                                 decision-type;
63     DERIVED BY:                 create-object;
64
65 OUTPUT                          create-subject-response;
66     SYNONYMS ARE:               cresubres;
67     PART OF:                    administrative-security-resp;
68     CONSISTS OF:
69                                 validation-code;
70     DERIVED BY:                 create-subject;
71
72 OUTPUT                          delete-object-decision;
73     SYNONYMS ARE:               kf9dec;
74     PART OF:                    reference-monitor-decision;
75     CONSISTS OF:
76                                 decision-type;
77     DERIVED BY:                 delete-object;
```

AD-A065 948 MICHIGAN UNIV ANN ARBOR DEPT OF INDUSTRIAL AND OPERA--ETC F/G 5/9
URL/URA TRAINING EXAMPLE.(U)
DEC 78

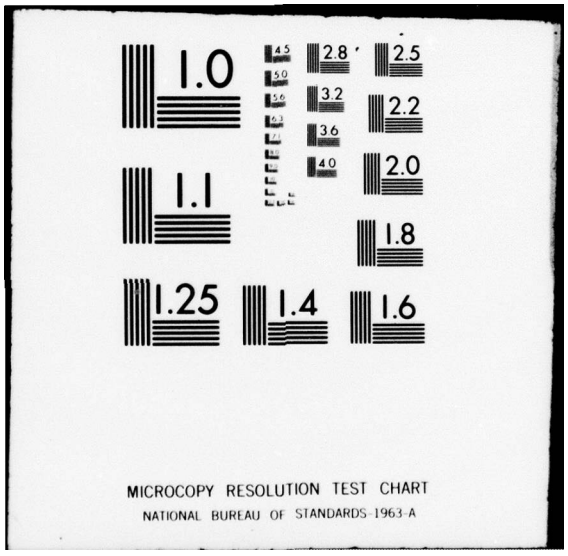
F19628-76-C-0197

UNCLASSIFIED ESD-TR-78-126 NL

3 OF 3
AD
A065948



END
DATE
FILMED
5-79
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Security-control-example

FORMATTED PROBLEM STATEMENT

```
78
79 OUTPUT                                  delete-subject-response;
80     SYNONYMS ARE:                       delsubres;
81     PART OF:                            administrative-security-resp;
82     CONSISTS OF:
83                                         validation-code;
84     DERIVED BY:                         delete-subject;
85
86 OUTPUT                                  dump-audit-trail;
87     SYNONYMS ARE:                       dumauditra;
88     PART OF:                            audit-trail;
89     CONSISTS OF:
90       number-of-incidents               sub-obj-inc-audit-information;
91     DERIVED BY:                         dump-audit;
92     HAPPENS:
93       number-of-dump-audit TIMES-PER    month;
94
95 OUTPUT                                  get-execute-decision;
96     SYNONYMS ARE:                       kf3dec;
97     PART OF:                            reference-monitor-decision;
98     CONSISTS OF:
99                                         decision-type;
100    DERIVED BY:                         get-execute;
101
102 OUTPUT                                 get-read-decision;
103    SYNONYMS ARE:                       kf1dec;
104    PART OF:                            reference-monitor-decision;
105    CONSISTS OF:
106                                        decision-type;
107    DERIVED BY:                         get-read;
108
109 OUTPUT                                 get-read-write-decision;
110    SYNONYMS ARE:                       kf4dec;
111    PART OF:                            reference-monitor-decision;
112    CONSISTS OF:
113                                        decision-type;
114    DERIVED BY:                         get-read-write;
115
116 OUTPUT                                 get-write-decision;
117    SYNONYMS ARE:                       kf2dec;
118    PART OF:                            reference-monitor-decision;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
119     CONSISTS OF:
120                                     decision-type;
121     DERIVED BY:                     get-write;
122
123 OUTPUT                               give-usage-attr-decision;
124     SYNONYMS ARE:                   kf6dec;
125     PART OF:                        reference-monitor-decision;
126     CONSISTS OF:
127                                     decision-type;
128     DERIVED BY:                     give-usage-attr;
129
130 OUTPUT                               inc-audit-trail;
131     SYNONYMS ARE:                   incaudtra;
132     PART OF:                        audit-trail;
133     CONSISTS OF:
134                                     sub-obj-audit-information;
135     DERIVED BY:                     inc-audit;
136
137 OUTPUT                               link-reference-monitor-resp;
138     SYNONYMS ARE:                   linrmonres;
139     PART OF:                        administrative-security-resp;
140     CONSISTS OF:
141                                     validation-code;
142     DERIVED BY:                     link-reference-monitor;
143
144 OUTPUT                               obj-audit-trail;
145     SYNONYMS ARE:                   objaudtra;
146     PART OF:                        audit-trail;
147     CONSISTS OF:
148                                     sub-inc-audit-information;
149     DERIVED BY:                     obj-audit;
150     HAPPENS:
151       number-of-obj-audit TIMES-PER month;
152
153 OUTPUT                               obj-inc-audit-trail;
154     SYNONYMS ARE:                   objincaudtra;
155     PART OF:                        audit-trail;
156     CONSISTS OF:
157                                     sub-audit-information;
158     DERIVED BY:                     obj-inc-audit;
159
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
160 OUTPUT                                  reference-monitor-decision;
161     SYNONYMS ARE:                       rmondec;
162     DESCRIPTION;
163                     These are decisions in answer  to the reference
164               monitor subject's request and allow for read, write, or
165               execute access to system information.;
166     KEYWORDS:                           level-2;
167     PART OF:                            security-control-output;
168     SUBPARTS ARE:                       get-read-decision,
169                                         get-write-decision,
170                                         get-execute-decision,
171                                         get-read-write-decision,
172                                         release-usage-attr-decision,
173                                         give-usage-attr-decision,
174                                         rescind-usage-attr-decision,
175                                         create-object-decision,
176                                         delete-object-decision,
177                                         change-sub-curr-sec-level-dec,
178                                         change-obj-sec-level-decision;
179     DERIVED BY:                         reference-monitor;
180     GENERATED BY:                       reference-monitor;
181     RECEIVED BY:                        reference-monitor-subject;
182
183 OUTPUT                                  release-usage-attr-decision;
184     SYNONYMS ARE:                       kf5dec;
185     PART OF:                            reference-monitor-decision;
186     CONSISTS OF:
187                                         decision-type;
188     DERIVED BY:                         release-usage-attr;
189
190 OUTPUT                                  rescind-usage-attr-decision;
191     SYNONYMS ARE:                       kf7dec;
192     PART OF:                            reference-monitor-decision;
193     CONSISTS OF:
194                                         decision-type;
195     DERIVED BY:                         rescind-usage-attr;
196
197 OUTPUT                                  security-control-output;
198     SYNONYMS ARE:                       scout;
199     DESCRIPTION;
200                     The system will produce outputs of several
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
201              different types: approvals to data access or modification
202              requests, audit trails on security features, a
203              record of outputs produced, etc.;
204      SEE-MEMO:                              system-philosophy-memo;
205      KEYWORDS:                              level-1;
206      ATTRIBUTES ARE:
207        specification-derivation             implicit;
208      SUBPARTS ARE:                          reference-monitor-decision,
209                                             administrative-security-resp,
210                                             audit-trail;
211      GENERATED BY:                          security-control-system;
212      RECEIVED BY:                           security-control-interface;
213      SECURITY IS:                           unclassified;
214
215  OUTPUT                                      sub-audit-trail;
216      SYNONYMS ARE:                          subaudtra;
217      PART OF:                               audit-trail;
218      CONSISTS OF:
219                                             obj-inc-audit-information;
220      DERIVED BY:                            sub-audit;
221      HAPPENS:
222        number-of-sub-audit TIMES-PER        month;
223
224  OUTPUT                                      sub-inc-audit-trail;
225      SYNONYMS ARE:                          subincaudtra;
226      PART OF:                               audit-trail;
227      CONSISTS OF:
228                                             obj-audit-information;
229      DERIVED BY:                            sub-inc-audit;
230
231  OUTPUT                                      sub-obj-audit-trail;
232      SYNONYMS ARE:                          subobjaudtra;
233      PART OF:                               audit-trail;
234      CONSISTS OF:
235                                             inc-audit-information;
236      DERIVED BY:                            sub-obj-audit;
237
238  OUTPUT                                      sub-obj-inc-audit-trail;
239      SYNONYMS ARE:                          subobjincaudtra;
240      PART OF:                               audit-trail;
241      CONSISTS OF:
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
242                                    audit-information;
243      DERIVED BY:                   sub-obj-inc-audit;
244
245 EOF EOF EOF EOF EOF
```

Security-control-example

INPUT STRUCTURE

PARAMETERS FOR: STR

INPUT INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 security-control-input
    2      2   reference-monitor-request
    3       3     get-read-request
    4       3     get-write-request
    5       3     get-execute-request
    6       3     get-read-write-request
    7       3     release-usage-attr-request
    8       3     give-usage-attr-request
    9       3     rescind-usage-attr-request
   10       3     create-object-request
   11       3     delete-object-request
   12       3     change-sub-curr-sec-level-req
   13       3     change-obj-sec-level-request
   14      2   administrative-security-comd
   15       3     create-subject-command
   16       3     delete-subject-command
   17       3     change-sub-max-sec-level-comd
   18       3     link-reference-monitor-comd
   19      2   auditing-request
   20       3     sub-obj-audit-request
   21       3     sub-inc-audit-request
   22       3     sub-obj-inc-audit-request
   23       3     sub-audit-request
   24       3     obj-inc-audit-request
   25       3     obj-audit-request
   26       3     inc-audit-request
   27       3     dump-audit-request
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	3	3	23				

Security-control-example

Name Generation

'ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='INP' ORDER=BYTYPE

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	change-obj-sec-level-request	INPUT
4	change-sub-curr-sec-level-req	INPUT
5	change-sub-max-sec-level-comd	INPUT
6	create-object-request	INPUT
7	create-subject-command	INPUT
8	delete-object-request	INPUT
9	delete-subject-command	INPUT
10	dump-audit-request	INPUT
11	get-execute-request	INPUT
12	get-read-request	INPUT
13	get-read-write-request	INPUT
14	get-write-request	INPUT
15	give-usage-attr-request	INPUT
16	inc-audit-request	INPUT
17	link-reference-monitor-comd	INPUT
18	obj-audit-request	INPUT
19	obj-inc-audit-request	INPUT
20	reference-monitor-request	INPUT
21	release-usage-attr-request	INPUT
22	rescind-usage-attr-request	INPUT
23	security-control-input	INPUT
24	sub-audit-request	INPUT
25	sub-inc-audit-request	INPUT
26	sub-obj-audit-request	INPUT
27	sub-obj-inc-audit-request	INPUT

Security-control-example

FORMATTED PROBLEM STATEMENT

```
PARAMETERS FOR: PPS

   FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 BNMARG=71 CMARG=1 HMARG=40 DESG
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 INPUT                                  administrative-security-comd;
    2     SYNONYMS ARE:                     admscom;
    3     DESCRIPTION;
    4                  These are commands necessary to the performance
    5             of administrative security functions and will allow for
    6             the maintenance of the reference monitor data base.;
    7     KEYWORDS:                         level-2;
    8     ATTRIBUTES ARE:
    9       occurrences                     unscheduled;
   10     PART OF:                          security-control-input;
   11     SUBPARTS ARE:                     create-subject-comand,
   12                                       delete-subject-command,
   13                                       change-sub-max-sec-level-comd,
   14                                       link-reference-monitor-comd;
   15     GENERATED BY:                     system-security-administrator;
   16     RECEIVED BY:                      administrative-security-system;
   17     USED BY:                          administrative-security-system;
   18
   19 INPUT                                  auditing-request;
   20     SYNONYMS ARE:                     audreq;
   21     DESCRIPTION;
   22                  These are requests to view audit data stored in
   23             the auditing system data base by the reference
   24             monitor.;
   25     KEYWORDS:                         level-2;
   26     ATTRIBUTES ARE:
   27       occurrences                     scheduled;
   28     PART OF:                          security-control-input;
   29     SUBPARTS ARE:                     sub-obj-audit-request,
   30                                       sub-inc-audit-request,
   31                                       sub-obj-inc-audit-request,
   32                                       sub-audit-request,
   33                                       obj-inc-audit-request,
   34                                       obj-audit-request,
   35                                       inc-audit-request,
   36                                       dump-audit-request;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37      GENERATED BY:                   system-security-administrator;
38      RECEIVED BY:                    auditing-system;
39      USED BY:                        auditing-system;
40
41  INPUT                                change-obj-sec-level-request;
42      SYNONYMS ARE:                   kf11req;
43      PART OF:                        reference-monitor-request;
44      CONSISTS OF:
45                                      subject-id,
46                                      object-id,
47                                      obj-sec-level;
48      USED BY:                        change-obj-sec-level;
49
50  INPUT                                change-sub-curr-sec-level-req;
51      SYNONYMS ARE:                   kf10req;
52      PART OF:                        reference-monitor-request;
53      CONSISTS OF:
54                                      subject-id,
55                                      sub-curr-sec-level;
56      USED BY:                        change-sub-curr-sec-level;
57
58  INPUT                                change-sub-max-sec-level-comd;
59      SYNONYMS ARE:                   chasubmaxseclevcom;
60      PART OF:                        administrative-security-comd;
61      CONSISTS OF:
62                                      security-id,
63                                      subject-id,
64                                      sub-max-sec-level;
65      USED BY:                        change-sub-max-sec-level;
66
67  INPUT                                create-object-request;
68      SYNONYMS ARE:                   kf8req;
69      PART OF:                        reference-monitor-request;
70      CONSISTS OF:
71                                      subject-id,
72                                      object-id,
73                                      obj-sec-level;
74      USED BY:                        create-object;
75
76  INPUT                                create-subject-command;
77      SYNONYMS ARE:                   cresubcom;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
 78     PART OF:                          administrative-security-comd;
 79     CONSISTS OF:
 80                                       security-id,
 81                                       subject-id,
 82                                       sub-max-sec-level,
 83                                       sub-curr-sec-level;
 84     USED BY:                          create-subject;
 85
 86 INPUT                                  delete-object-request;
 87     SYNONYMS ARE:                     kf9req;
 88     PART OF:                          reference-monitor-request;
 89     CONSISTS OF:
 90                                       subject-id,
 91                                       object-id;
 92     USED BY:                          delete-object;
 93
 94 INPUT                                  delete-subject-command;
 95     SYNONYMS ARE:                     delsubcom;
 96     PART OF:                          administrative-security-comd;
 97     CONSISTS OF:
 98                                       security-id,
 99                                       subject-id;
100     USED BY:                          delete-subject;
101
102 INPUT                                  dump-audit-request;
103     SYNONYMS ARE:                     dumaudreq;
104     PART OF:                          auditing-request;
105     USED BY:                          dump-audit;
106     HAPPENS:
107       number-of-dump-audit TIMES-PER  month;
108
109 INPUT                                  get-execute-request;
110     SYNONYMS ARE:                     kf3req;
111     PART OF:                          reference-monitor-request;
112     CONSISTS OF:
113                                       subject-id,
114                                       object-id,
115                                       usage-attribute;
116     USED BY:                          get-execute;
117
118 INPUT                                  get-read-request;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
119      SYNONYMS ARE:                    kf1req;
120      PART OF:                         reference-monitor-request;
121      CONSISTS OF:
122                                       subject-id,
123                                       object-id,
124                                       usage-attribute;
125      USED BY:                         get-read;
126
127  INPUT                                 get-read-write-request;
128      SYNONYMS ARE:                    kf4req;
129      PART OF:                         reference-monitor-request;
130      CONSISTS OF:
131                                       subject-id,
132                                       object-id,
133                                       usage-attribute;
134      USED BY:                         get-read-write;
135
136  INPUT                                 get-write-request;
137      SYNONYMS ARE:                    kf2req;
138      PART OF:                         reference-monitor-request;
139      CONSISTS OF:
140                                       subject-id,
141                                       object-id,
142                                       usage-attribute;
143      USED BY:                         get-write;
144
145  INPUT                                 give-usage-attr-request;
146      SYNONYMS ARE:                    kf6req;
147      PART OF:                         reference-monitor-request;
148      CONSISTS OF:
149                                       requesting-subject-id,
150                                       receiving-subject-id,
151                                       object-id,
152                                       usage-attribute;
153      USED BY:                         give-usage-attr;
154
155  INPUT                                 inc-audit-request;
156      SYNONYMS ARE:                    incaudreq;
157      PART OF:                         auditing-request;
158      CONSISTS OF:
159                                       incident-type;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
160     USED BY:                              inc-audit;
161
162 INPUT                                      link-reference-monitor-comd;
163     SYNONYMS ARE:                         linrmoncom;
164     PART OF:                              administrative-security-comd;
165     CONSISTS OF:
166                                           security-id;
167     USED BY:                              link-reference-monitor;
168
169 INPUT                                      obj-audit-request;
170     SYNONYMS ARE:                         objaudreq;
171     PART OF:                              auditing-request;
172     CONSISTS OF:
173                                           object-id;
174     USED BY:                              obj-audit;
175     HAPPENS:
176       number-of-obj-audit TIMES-PER       month;
177
178 INPUT                                      obj-inc-audit-request;
179     SYNONYMS ARE:                         objincaudreq;
180     PART OF:                              auditing-request;
181     CONSISTS OF:
182                                           object-id,
183                                           incident-type;
184     USED BY:                              obj-inc-audit;
185
186 INPUT                                      reference-monitor-request;
187     SYNONYMS ARE:                         rmonreq;
188     DESCRIPTION;
189                    These are requests to access or modify information
190               in the system and may include output options.;
191     KEYWORDS:                             level-2;
192     ATTRIBUTES ARE:
193       occurrences                         unscheduled;
194     PART OF:                              security-control-input;
195     SUBPARTS ARE:                         get-read-request,
196                                           get-write-request,
197                                           get-execute-request,
198                                           get-read-write-request,
199                                           release-usage-attr-request,
200                                           give-usage-attr-request,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
                                        rescind-usage-attr-request,
                                        create-object-request,
                                        delete-object-request,
                                        change-sub-curr-sec-level-req,
                                        change-obj-sec-level-request;
    GENERATED BY:                       reference-monitor-subject;
    RECEIVED BY:                        reference-monitor;
    USED BY:                            reference-monitor;

INPUT                                    release-usage-attr-request;
    SYNONYMS ARE:                       kf5req;
    PART OF:                            reference-monitor-request;
    CONSISTS OF:
                                        subject-id,
                                        object-id,
                                        usage-attribute;
    USED BY:                            release-usage-attr;

INPUT                                    rescind-usage-attr-request;
    SYNONYMS ARE:                       kf7req;
    PART OF:                            reference-monitor-request;
    CONSISTS OF:
                                        requesting-subject-id,
                                        receiving-subject-id,
                                        object-id,
                                        usage-attribute;
    USED BY:                            rescind-usage-attr;

INPUT                                    security-control-input;
    SYNONYMS ARE:                       scinp;
    DESCRIPTION;
                The input to the security control system
            consists of requests by users to access and
            modify information in the system and of commands
            by security personnel to monitor the system.;
    SEE-MEMO:                           system-philosophy-memo;
    KEYWORDS:                           level-1;
    ATTRIBUTES ARE:
      specification-derivation          implicit;
    SUBPARTS ARE:                       reference-monitor-request,
                                        administrative-security-comd,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
242                                        auditing-request;
243     GENERATED BY:                      security-control-interface;
244     RECEIVED BY:                       security-control-system;
245     SECURITY IS:                       unclassified;
246
247 INPUT                                   sub-audit-request;
248     SYNONYMS ARE:                      subaudreq;
249     PART OF:                           auditing-request;
250     CONSISTS OF:
251                                        subject-id;
252     USED BY:                           sub-audit;
253     HAPPENS:
254       number-of-sub-audit TIMES-PER    month;
255
256 INPUT                                   sub-inc-audit-request;
257     SYNONYMS ARE:                      subincaudreq;
258     PART OF:                           auditing-request;
259     CONSISTS OF:
260                                        subject-id,
261                                        incident-type;
262     USED BY:                           sub-inc-audit;
263
264 INPUT                                   sub-obj-audit-request;
265     SYNONYMS ARE:                      subobjaudreq;
266     PART OF:                           auditing-request;
267     CONSISTS OF:
268                                        subject-id,
269                                        object-id;
270     USED BY:                           sub-obj-audit;
271
272 INPUT                                   sub-obj-inc-audit-request;
273     SYNONYMS ARE:                      subobjincaudreq;
274     PART OF:                           auditing-request;
275     CONSISTS OF:
276                                        subject-id,
277                                        object-id,
278                                        incident-type;
279     USED BY:                           sub-obj-inc-audit;
280
281 EOF EOF EOF EOF EOF
```

Security-control-example

INTERFACE STRUCTURE

PARAMETERS FOR: STR

INTERFACE INDENT=3 NOINDEX

```
COUNT LEVEL NAME

    1     1 security-control-interface
    2      2   reference-monitor-subject
    3      2   system-security-administrator
```

LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT	LEVEL	COUNT
1	1	2	2						

Security-control-example

Name Generation

PARAMETERS FOR: NG

```
   PRINT PUNCH EMPTY SELECTION='INTF' ORDER=BYTYPE

   1    reference-monitor-subject          INTERFACE
   2    security-control-interface         INTERFACE
   3    system-security-administrator      INTERFACE
```

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=30 AMARG=7 BMARG=39 BNMARG=70 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 INTERFACE                                reference-monitor-subject;
 2     SYNONYMS ARE:                        rmonsub;
 3     DESCRIPTION;
 4                 A reference monitor subject may be a user, a
 5             process, or a job which generates requests on the
 6             reference monitor.;
 7     KEYWORDS:                            level-2;
 8     PART OF:                             security-control-interface;
 9     GENERATES:                           reference-monitor-request;
10     RECEIVES:                            reference-monitor-decision;
11     RESPONSIBLE-PROBLEM-DEFINER IS:      james-m-amster;
12
13 INTERFACE                                security-control-interface;
14     SYNONYMS ARE:                        scint;
15     DESCRIPTION;
16                 There will be several different types of users
17             generating requests on the system and retrieving
18             data from it.  The security controls of the system
19             must be capable of allowing users of different
20             authorizations to process concurrently while preventing
21             the release of information to unauthorized users.;
22     SEE-MEMO:                            system-philosophy-memo;
23     KEYWORDS:                            level-1;
24     ATTRIBUTES ARE:
25       specification-derivation           explicit;
26     SUBPARTS ARE:                        reference-monitor-subject,
27                                          system-security-administrator;
28     GENERATES:                           security-control-input;
29     RECEIVES:                            security-control-output;
30     RESPONSIBLE FOR:                     security-control-data-base;
31     SECURITY IS:                         unclassified;
32
33 INTERFACE                                system-security-administrator;
34     SYNONYMS ARE:                        ssa,
35                                          ssadm;
36     DESCRIPTION;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37                  The system security administrator will have the
38              responsibility of receiving and reviewing audit data
39              contained in the auditing system data base and
40              performing administrative functions dealing with the
41              initiation and maintenance of system subject and object
42              information contained in the reference monitor data
43              base.;
44      KEYWORDS:                          level-2;
45      PART OF:                           security-control-interface;
46      GENERATES:                         administrative-security-comd,
47                                         auditing-request;
48      RECEIVES:                          administrative-security-resp,
49                                         audit-trail;
50      RESPONSIBLE FOR:                   reference-monitor-data-base,
51                                         auditing-system-data-base;
52      RESPONSIBLE-PROBLEM-DEFINER IS:    michel-j-bastarache;
53
54 EOF EOF EOF EOF EOF
```

Security-control-example

Name Generation

'ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='ENTITY' ORDER=BYTYPE

1	incident-information	ENTITY
2	object-information	ENTITY
3	subject-information	ENTITY

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=79 CMARG=1 HMARG=40 DESG
ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

```
 1 ENTITY                                  incident-information;
 2     SYNONYMS ARE:                      incinfo;
 3     DESCRIPTION;
 4                   This information holds data about where and
 5             when an incident has occurred.;
 6     CONTAINED IN:                      auditing-system-data-base;
 7     CONSISTS OF:
 8                                        date-time,
 9                                        consol-nr,
10                                        incident-type;
11     /* RIGHT */ RELATED TO:
12       subject-information VIA          sub-inc-audit-relation;
13     /* RIGHT */ RELATED TO:
14       object-information VIA           obj-inc-audit-relation;
15     DERIVED BY:                        produce-audit-incident
16       USING:                           error-code;
17     OCCURRENCES:                       number-of-incidents;
18     VOLATILITY;
19                   The contents of this type of entity are never
20             changed after creation.;
21     RESPONSIBLE-PROBLEM-DEFINER IS:    james-m-amster;
22
23 ENTITY                                  object-information;
24     SYNONYMS ARE:                      objinfo;
25     DESCRIPTION;
26                   This information holds identification, security,
27             and location information for a particular object.;
28     CONTAINED IN:                      top-secret-file,
29                                        secret-file,
30                                        confidential-file,
31                                        unclassified-file;
32     CONSISTS OF:
33                                        object-id,
34                                        obj-sec-level,
35                                        object-location;
36     /* LEFT */ RELATED TO:
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37        incident-information VIA          obj-inc-audit-relation;
38      /* RIGHT */ RELATED TO:
39        subject-information VIA           subject-access-to-object;
40      /* RIGHT */ RELATED TO:
41        subject-information VIA           subject-need-to-know-object;
42      /* RIGHT */ RELATED TO:
43        subject-information VIA           sub-obj-audit-relation;
44      IDENTIFIED BY:                      object-id;
45      DERIVED BY:                         create-object-information
46        USING:                            object-id,
47                                          obj-sec-level;
48      OCCURRENCES:                        number-of-objects;
49      VOLATILITY;
50                    The obj-sec-level may be changed by either the
51              owner of the object or the system security administrator.
52              Changing the object-location is done based on need by
53              the operating system.;
54      RESPONSIBLE-PROBLEM-DEFINER IS:     james-m-amster;
55
56  ENTITY                                   subject-information;
57      SYNONYMS ARE:                       subinfo;
58      DESCRIPTION;
59                    This information holds identification and
60              security data about a reference monitor subject.;
61      CONTAINED IN:                       top-secret-file,
62                                          secret-file,
63                                          confidential-file,
64                                          unclassified-file;
65      CONSISTS OF:
66                                          subject-id,
67                                          sub-max-sec-level,
68                                          sub-curr-sec-level;
69      /* LEFT */ RELATED TO:
70        object-information VIA            subject-access-to-object;
71      /* LEFT */ RELATED TO:
72        object-information VIA            subject-need-to-know-object;
73      /* LEFT */ RELATED TO:
74        incident-information VIA          sub-inc-audit-relation;
75      /* LEFT */ RELATED TO:
76        object-information VIA            sub-obj-audit-relation;
77      IDENTIFIED BY:                      subject-id;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
78      OCCURRENCES:                        number-of-subjects;
79      VOLATILITY;
80                      The sub-max-sec-level can only be changei by a
81                  systen security administrator ani only on decision
82                  of the administrator.  The sub-curr-sec-level may
83                  change several times within the course of one session
84                  on the system.;
85      RESPONSIBLE-PROBLEM-DEFINER IS:    james-m-amster;
86
87 EOF EOF EOF EOF EOF
```

Security-control-example

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='GROUP OR ELE' ORDER=BYTYPE

1	category-set	ELEMENT
2	classification-level	ELEMENT
3	consol-nr	ELEMENT
4	date-time	ELEMENT
5	decision-type	ELEMENT
6	error-code	ELEMENT
7	incident-type	ELEMENT
8	object-id	ELEMENT
9	object-location	ELEMENT
10	receiving-subject-id	ELEMENT
11	requesting-subject-id	ELEMENT
12	security-id	ELEMENT
13	subject-id	ELEMENT
14	usage-attribute	ELEMENT
15	validation-code	ELEMENT
16	audit-information	GROUP
17	inc-audit-information	GROUP
18	obj-audit-information	GROUP
19	obj-inc-audit-information	GROUP
20	obj-sec-level	GROUP
21	sub-audit-information	GROUP
22	sub-curr-sec-level	GROUP
23	sub-inc-audit-information	GROUP
24	sub-max-sec-level	GROUP
25	sub-obj-audit-information	GROUP
26	sub-obj-inc-audit-information	GROUP

Security-control-example

FORMATTED PROBLEM STATEMENT

PARAMETERS FOR: FPS

```
   FILE NOINDEX PRINT NOPUNCH SMARG=5 NMARG=39 AMARG=7 BMARG=39 RNMARG=70 CMARG=1 HMARG=40 DESG
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 ELEMENT                                  category-set;
    2     DESCRIPTION;
    3                     This is a set of categories of information which
    4              may be owned by a subject  or an object.;
    5     SEE-MEMO:                           category-set-memo;
    6     CONTAINED IN:                       sub-max-sec-level,
    7                                         sub-curr-sec-level,
    8                                         obj-sec-level;
    9
   10 ELEMENT                                  classification-level;
   11     DESCRIPTION;
   12                     This is a level of classification which may
   13               range up from unclassified to top secret and may be
   14               owned by a subject or an object.;
   15     SEE-MEMO:                           clearance-memo;
   16     CONTAINED IN:                       sub-max-sec-level,
   17                                         sub-curr-sec-level,
   18                                         obj-sec-level;
   19
   20 ELEMENT                                  consol-nr;
   21     DESCRIPTION;
   22                     This is the number of the console at which the audit
   23                  incident occurred.;
   24     CONTAINED IN:                       incident-information,
   25                                         inc-audit-information,
   26                                         obj-audit-information,
   27                                         audit-information,
   28                                         obj-inc-audit-information,
   29                                         sub-audit-information,
   30                                         sub-inc-audit-information,
   31                                         sub-obj-audit-information,
   32                                         sub-obj-inc-audit-information;
   33     VALUES ARE:
   34       0 THRU                           25;
   35
   36 ELEMENT                                  date-time;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37      DESCRIPTION;
38                      This is the date and time an audit incident
39                  occurred.;
40      CONTAINED IN:                       incident-information,
41                                          inc-audit-information,
42                                          obj-audit-information,
43                                          audit-information,
44                                          obj-inc-audit-information,
45                                          sub-audit-information,
46                                          sub-inc-audit-information,
47                                          sub-obj-audit-information,
48                                          sub-obj-inc-audit-information;
49
50  ELEMENT                                  decision-type;
51      DESCRIPTION;
52                      This is the affirmative or negative decision to
53                  a subject's request.;
54      CONTAINED IN:                       get-read-decision,
55                                          get-write-decision,
56                                          get-execute-decision,
57                                          get-read-write-decision,
58                                          release-usage-attr-decision,
59                                          give-usage-attr-decision,
60                                          rescind-usage-attr-decision,
61                                          create-object-decision,
62                                          delete-object-decision,
63                                          change-sub-curr-sec-level-dec,
64                                          change-obj-sec-level-decision;
65      DERIVED BY:                         generate-decision
66        USING:                            error-code;
67
68  ELEMENT                                  error-code;
69      DERIVED BY:                         check-need-to-know-usage
70        USING:                            subject-id,
71                                          object-id,
72                                          usage-attribute;
73      DERIVED BY:                         check-sub-obj-sec-levels
74        USING:                            sub-curr-sec-level,
75                                          obj-sec-level;
76      DERIVED BY:                         check-access-usage
77        USING:                            subject-id,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
                                        object-id,
                                        usage-attribute;
    DERIVED BY:                         delete-access-relation
      USING:                            subject-id,
                                        object-id;
    DERIVED BY:                         delete-object-information
      USING:                            object-id,
                                        obj-sec-level;
    USED BY:
      produce-audit-incident
       TO DERIVE                        incident-information;
    USED BY:
      generate-decision TO DERIVE       decision-type;

ELEMENT                                  incident-type;
    DESCRIPTION;
                  This specifies the type of audit incident which
            has occurred.;
    CONTAINED IN:                       incident-information,
                                        inc-audit-information,
                                        sub-inc-audit-request,
                                        sub-obj-inc-audit-request,
                                        obj-inc-audit-information,
                                        obj-inc-audit-request,
                                        sub-inc-audit-information,
                                        inc-audit-request,
                                        sub-obj-inc-audit-information;

ELEMENT                                  object-id;
    DESCRIPTION;
                  This is a unique identifier for an object.;
    CONTAINED IN:                       object-information,
                                        get-read-request,
                                        get-write-request,
                                        get-execute-request,
                                        get-read-write-request,
                                        release-usage-attr-request,
                                        give-usage-attr-request,
                                        rescind-usage-attr-request,
                                        create-object-request,
                                        delete-object-request,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
119                                    change-obj-sec-level-request,
120                                    sub-obj-audit-request,
121                                    obj-audit-information,
122                                    sub-obj-inc-audit-request,
123                                    obj-inc-audit-information,
124                                    obj-inc-audit-request,
125                                    obj-audit-request,
126                                    sub-obj-audit-information,
127                                    sub-obj-inc-audit-information;
128     IDENTIFIES:                    object-information;
129     USED BY:
130       check-need-to-know-usage
131        TO DERIVE                   error-code;
132     USED BY:
133       check-access-usage TO DERIVE error-code;
134     USED BY:
135       delete-access-relation
136        TO DERIVE                   error-code;
137     USED BY:
138       create-object-information
139        TO DERIVE                   object-information;
140     USED BY:
141       delete-object-information
142        TO DERIVE                   error-code;
143     USED BY:
144       create-access-relation
145        TO UPDATE                   usage-attribute;
146
147 ELEMENT                             object-location;
148     DESCRIPTION:
149                   "This is a pointer to the actual object which
150               contains the information of interest to a subject and
151               which exists outside the security control system.";
152     CONTAINED IN:                  object-information;
153
154 ELEMENT                             receiving-subject-id;
155     CONTAINED IN:                  give-usage-attr-request,
156                                    rescind-usage-attr-request;
157
158 ELEMENT                             requesting-subject-id;
159     CONTAINED IN:                  give-usage-attr-request,
```

FORMATTED PROBLEM STATEMENT

```
                                        rescind-usage-attr-request;

ELEMENT                                  security-id;
    DESCRIPTION;
                    This uniquely identifies the system security
               administrator.;
    CONTAINED IN:                       create-subject-command,
                                        delete-subject-command,
                                        change-sub-max-sec-level-comd,
                                        link-reference-monitor-comd;

ELEMENT                                  subject-id;
    DESCRIPTION;
               This is a unique identifier for a subject.;
    CONTAINED IN:                       subject-information,
                                        get-read-request,
                                        get-write-request,
                                        get-execute-request,
                                        get-read-write-request,
                                        release-usage-attr-request,
                                        create-object-request,
                                        delete-object-request,
                                        change-sub-curr-sec-level-req,
                                        change-obj-sec-level-request,
                                        create-subject-command,
                                        delete-subject-command,
                                        change-sub-max-sec-level-comd,
                                        sub-obj-audit-request,
                                        sub-inc-audit-request,
                                        sub-obj-inc-audit-request,
                                        sub-audit-request,
                                        sub-audit-information,
                                        sub-inc-audit-information,
                                        sub-obj-audit-information,
                                        sub-obj-inc-audit-information;
    IDENTIFIES:                         subject-information;
    USED BY:
      check-need-to-know-usage
       TO DERIVE                        error-code;
    USED BY:
      check-access-usage TO DERIVE      error-code;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
201     USED BY:
202       delete-access-relation
203         TO DERIVE                          error-code;
204     USED BY:
205       create-access-relation
206         TO UPDATE                          usage-attribute;
207
208 ELEMENT                                     usage-attribute;
209     DESCRIPTION;
210                   This specifies the type of usage, that is
211               read, write, or execute, that a subject may have of an
212               object.;
213     CONTAINED IN:                          get-read-request,
214                                            get-write-request,
215                                            get-execute-request,
216                                            get-read-write-request,
217                                            release-usage-attr-request,
218                                            give-usage-attr-request,
219                                            rescind-usage-attr-request;
220     ASSOCIATED WITH:                       subject-access-to-object,
221                                            subject-need-to-know-object;
222     USED BY:
223       check-need-to-know-usage
224         TO DERIVE                          error-code;
225     USED BY:
226       check-access-usage TO DERIVE         error-code;
227     UPDATED BY:                            create-access-relation
228       USING:                               subject-id,
229                                            object-id;
230
231 ELEMENT                                     validation-code;
232     DESCRIPTION;
233                   This is a validation of a command issued by
234               the system security administrator.;
235     CONTAINED IN:                          create-subject-response,
236                                            delete-subject-response,
237                                            change-sub-max-sec-level-resp,
238                                            link-reference-monitor-resp;
239
240 GROUP                                       audit-information;
241     SYNONYMS ARE:                          audinfo;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
242     CONTAINED IN:                   sub-obj-inc-audit-trail;
243     CONSISTS OF:
244                                     date-time,
245                                     consol-nr;
246
247 GROUP                              inc-audit-information;
248     SYNONYMS ARE:                   incaudinfo;
249     CONTAINED IN:                   sub-obj-audit-trail;
250     CONSISTS OF:
251                                     incident-type,
252                                     date-time,
253                                     consol-nr;
254
255 GROUP                              obj-audit-information;
256     SYNONYMS ARE:                   objaudinfo;
257     CONTAINED IN:                   sub-inc-audit-trail;
258     CONSISTS OF:
259                                     object-id,
260                                     date-time,
261                                     consol-nr;
262
263 GROUP                              obj-inc-audit-information;
264     SYNONYMS ARE:                   objincaudinfo;
265     CONTAINED IN:                   sub-audit-trail;
266     CONSISTS OF:
267                                     object-id,
268                                     incident-type,
269                                     date-time,
270                                     consol-nr;
271
272 GROUP                              obj-sec-level;
273     DESCRIPTION;
274                 This is the security level for an object.;
275     CONTAINED IN:                   object-information,
276                                     create-object-request,
277                                     change-obj-sec-level-request;
278     CONSISTS OF:
279                                     classification-level,
280                                     category-set;
281     SUBSETTING-CRITERION FOR:       reference-monitor-data-base;
282     USED BY:
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
283       check-sub-obj-sec-levels
284         TO DERIVE                          error-code;
285       USED BY:
286         create-object-information
287         TO DERIVE                          object-information;
288       USED BY:
289         delete-object-information
290         TO DERIVE                          error-code;
291
292   GROUP                                     sub-audit-information;
293       SYNONYMS ARE:                       subaudinfo;
294       CONTAINED IN:                       obj-inc-audit-trail;
295       CONSISTS OF:
296                                           subject-id,
297                                           date-time,
298                                           consol-nr;
299
300   GROUP                                     sub-curr-sec-level;
301       DESCRIPTION;
302                    This is the current security level for a subject.;
303       CONTAINED IN:                       subject-information,
304                                           change-sub-curr-sec-level-req,
305                                           create-subject-command;
306       CONSISTS OF:
307                                           classification-level,
308                                           category-set;
309       SUBSETTING-CRITERION FOR:           reference-monitor-data-base;
310       USED BY:
311         check-sub-obj-sec-levels
312         TO DERIVE                         error-code;
313
314   GROUP                                     sub-inc-audit-information;
315       SYNONYMS ARE:                       subincaudinfo;
316       CONTAINED IN:                       obj-audit-trail;
317       CONSISTS OF:
318                                           subject-id,
319                                           incident-type,
320                                           date-time,
321                                           consol-nr;
322
323   GROUP                                     sub-max-sec-level;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
324     DESCRIPTION;
325                   This is the maximum security level for a subject.;
326     CONTAINED IN:                       subject-information,
327                                         create-subject-command,
328                                         change-sub-max-sec-level-cmd;
329     CONSISTS OF:
330                                         classification-level,
331                                         category-set;
332
333 GROUP                                    sub-obj-audit-information;
334     SYNONYMS ARE:                       subobjaudinfo;
335     CONTAINED IN:                       inc-audit-trail;
336     CONSISTS OF:
337                                         subject-id,
338                                         object-id,
339                                         date-time,
340                                         consol-nr;
341
342 GROUP                                    sub-obj-inc-audit-information;
343     SYNONYMS ARE:                       subobjincaudinfo;
344     CONTAINED IN:                       dump-audit-trail;
345     CONSISTS OF:
346                                         subject-id,
347                                         object-id,
348                                         incident-type,
349                                         date-time,
350                                         consol-nr;
351
352 EOF EOF EOF EOF EOF
```

Security-control-example

KWIC INDEX

PARAMETERS FOR: KWIC

DIR=20 FILE

SEQ	N A M E (PERMUTED)	
1	attribute	usage
2	audit-information	
3	audit-information	inc
4	audit-information	obj
5	audit-information	sub
6	audit-information	obj-inc
7	audit-information	sub-inc
8	audit-information	sub-obj
9	audit-information	sub-obj-inc
10	category-set	
11	classification-level	
12	code	error
13	code	validation
14	consol-nr	
15	curr-sec-level	sub
16	date-time	
17	decision-type	
18	error-code	
19	id	object
20	id	subject
21	id	security
22	id	receiving-subject
23	id	requesting-subject
24	inc-audit-information	
25	inc-audit-information	obj
26	inc-audit-information	sub
27	inc-audit-information	sub-obj
28	incident-type	
29	information	audit
30	information	inc-audit
31	information	obj-audit
32	information	sub-audit
33	information	obj-inc-audit
34	information	sub-inc-audit
35	information	sub-obj-audit

Security-control-example

KWIC INDEX

SEQ	N A M E (PERMUTED)	
36	information	sub-obj-inc-audit
37	level	obj-sec
38	level	sub-max-sec
39	level	sub-curr-sec
40	level	classification
41	location	object
42	max-sec-level	sub
43	nr	consol
44	obj-audit-information	
45	obj-audit-information	sub
46	obj-inc-audit-information	
47	obj-inc-audit-information	sub
48	obj-sec-level	
49	object-id	
50	object-location	
51	receiving-subject-id	
52	requesting-subject-id	
53	sec-level	obj
54	sec-level	sub-max
55	sec-level	sub-curr
56	security-id	
57	set	category
58	sub-audit-information	
59	sub-curr-sec-level	
60	sub-inc-audit-information	
61	sub-max-sec-level	
62	sub-obj-audit-information	
63	sub-obj-inc-audit-information	
64	subject-id	
65	subject-id	receiving
66	subject-id	requesting
67	time	date
68	type	decision
69	type	incident
70	usage-attribute	
71	validation-code	

Security-control-example

CONSISTS MATRIX REPORT

PARAMETERS FOR: CM

FILE CONTAINED

URA311:CONROW : THE FOLLOWING ARE NOT CONTAINED IN ANYTHING:
error-code

	ROW NAMES		COLUMN NAMES	
1	category-set	ELEMENT	1 sub-max-sec-level	GROUP
2	classification-level	ELEMENT	2 sub-curr-sec-level	GROUP
3	consol-nr	ELEMENT	3 obj-sec-level	GROUP
4	date-time	ELEMENT	4 incident-information	ENTITY
5	decision-type	ELEMENT	5 inc-audit-information	GROUP
6	error-code	ELEMENT	6 obj-audit-information	GROUP
7	incident-type	ELEMENT	7 audit-information	GROUP
8	object-id	ELEMENT	8 obj-inc-audit-information	GROUP
9	object-location	ELEMENT	9 sub-audit-information	GROUP
10	receiving-subject-id	ELEMENT	10 sub-inc-audit-information	GROUP
11	requesting-subject-id	ELEMENT	11 sub-obj-audit-information	GROUP
12	security-id	ELEMENT	12 sub-obj-inc-audit-information	GROUP
13	subject-id	ELEMENT	13 get-read-decision	OUTPUT
14	usage-attribute	ELEMENT	14 get-write-decision	OUTPUT
15	validation-code	ELEMENT	15 get-execute-decision	OUTPUT
16	audit-information	GROUP	16 get-read-write-decision	OUTPUT
17	inc-audit-information	GROUP	17 release-usage-attr-decision	OUTPUT
18	obj-audit-information	GROUP	18 give-usage-attr-decision	OUTPUT
19	obj-inc-audit-information	GROUP	19 rescind-usage-attr-decision	OUTPUT
20	obj-sec-level	GROUP	20 create-object-decision	OUTPUT
21	sub-audit-information	GROUP	21 delete-object-decision	OUTPUT
22	sub-curr-sec-level	GROUP	22 change-sub-curr-sec-level-dec	OUTPUT
23	sub-inc-audit-information	GROUP	23 change-obj-sec-level-decision	OUTPUT
24	sub-max-sec-level	GROUP	24 sub-inc-audit-request	INPUT
25	sub-obj-audit-information	GROUP	25 sub-obj-inc-audit-request	INPUT
26	sub-obj-inc-audit-information	GROUP	26 obj-inc-audit-request	INPUT
			27 inc-audit-request	INPUT
			28 object-information	ENTITY
			29 get-read-request	INPUT
			30 get-write-request	INPUT

Security-control-example

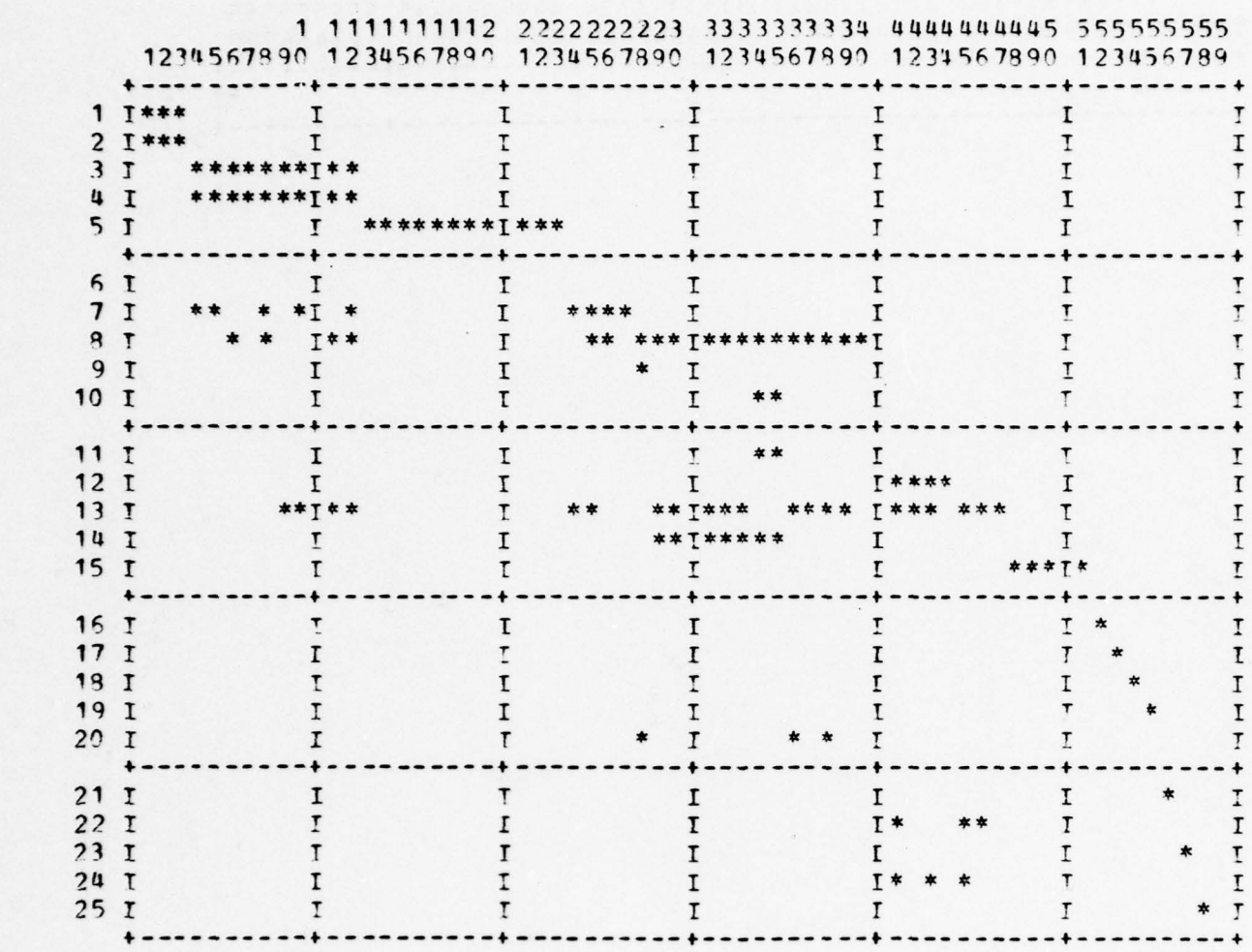
CONSISTS MATRIX REPORT

ROW NAMES	COLUMN NAMES	
31	get-execute-request	INPUT
32	get-read-write-request	INPUT
33	release-usage-attr-request	INPUT
34	give-usage-attr-request	INPUT
35	rescind-usage-attr-request	INPUT
36	create-object-request	INPUT
37	delete-object-request	INPUT
38	change-obj-sec-level-request	INPUT
39	sub-obj-audit-request	INPUT
40	obj-audit-request	INPUT
41	create-subject-command	INPUT
42	delete-subject-command	INPUT
43	change-sub-max-sec-level-comd	INPUT
44	link-reference-monitor-comd	INPUT
45	subject-information	ENTITY
46	change-sub-curr-sec-level-req	INPUT
47	sub-audit-request	INPUT
48	create-subject-response	OUTPUT
49	delete-subject-response	OUTPUT
50	change-sub-max-sec-level-resp	OUTPUT
51	link-reference-monitor-resp	OUTPUT
52	sub-obj-inc-audit-trail	OUTPUT
53	sub-obj-audit-trail	OUTPUT
54	sub-inc-audit-trail	OUTPUT
55	sub-audit-trail	OUTPUT
56	obj-inc-audit-trail	OUTPUT
57	obj-audit-trail	OUTPUT
58	inc-audit-trail	OUTPUT
59	dump-audit-trail	OUTPUT

THE ROWS ARE CONTAINED IN THE COLUMNS WITH *S

Security-control-example

CONSISTS MATRIX REPORT



Security-control-example

CONSISTS MATRIX REPORT

	1 1234567890	1111111112 1234567890	2222222223 1234567890	3333333334 1234567890	4444444445 1234567890	5555555555 1234567890
26	I	I	I	I	I	*I

Security-control-example

CONSISTS MATRIX REPORT

THE NUMBER OF COLUMNS THAT CONTAIN THE ROWS

	ROW	TYPE	COUNT
13	subject-id	ELEMENT	21
8	object-id	ELEMENT	19
5	decision-type	ELEMENT	11
3	consol-nr	ELEMENT	9
4	date-time	ELEMENT	9
7	incident-type	ELEMENT	9
14	usage-attribute	ELEMENT	7
12	security-id	ELEMENT	4
15	validation-code	ELEMENT	4
1	category-set	ELEMENT	3
2	classification-level	ELEMENT	3
20	obj-sec-level	GROUP	3
22	sub-curr-sec-level	GROUP	3
24	sub-max-sec-level	GROUP	3
10	receiving-subject-id	ELEMENT	2
11	requesting-subject-id	ELEMENT	2
9	object-location	ELEMENT	1
16	audit-information	GROUP	1
17	inc-audit-information	GROUP	1
18	obj-audit-information	GROUP	1
19	obj-inc-audit-information	GROUP	1
21	sub-audit-information	GROUP	1
23	sub-inc-audit-information	GROUP	1
25	sub-obj-audit-information	GROUP	1
26	sub-obj-inc-audit-information	GROUP	1
6	error-code	ELEMENT	0

THE NUMBER OF ROWS CONTAINED IN THE COLUMNS

	COLUMN	TYPE	COUNT
12	sub-obj-inc-audit-information	GROUP	5
8	obj-inc-audit-information	GROUP	4
10	sub-inc-audit-information	GROUP	4
11	sub-obj-audit-information	GROUP	4
34	give-usage-attr-request	INPUT	4

Security-control-example

CONSISTS MATRIX REPORT

35	rescind-usage-attr-request	INPUT	4
41	create-subject-command	INPUT	4
4	incident-information	ENTITY	3
5	inc-audit-information	GROUP	3
6	obj-audit-information	GROUP	3
9	sub-audit-information	GROUP	3
25	sub-obj-inc-audit-request	INPUT	3
28	object-information	ENTITY	3
29	get-read-request	INPUT	3
30	get-write-request	INPUT	3
31	get-execute-request	INPUT	3
32	get-read-write-request	INPUT	3
33	release-usage-attr-request	INPUT	3
36	create-object-request	INPUT	3
38	change-obj-sec-level-request	INPUT	3
43	change-sub-max-sec-level-comd	INPUT	3
45	subject-information	ENTITY	3
1	sub-max-sec-level	GROUP	2
2	sub-curr-sec-level	GROUP	2
3	obj-sec-level	GROUP	2
7	audit-information	GROUP	2
24	sub-inc-audit-request	INPUT	2
26	obj-inc-audit-request	INPUT	2
37	delete-object-request	INPUT	2
39	sub-obj-audit-request	INPUT	2
42	delete-subject-command	INPUT	2
46	change-sub-curr-sec-level-req	INPUT	2
13	get-read-decision	OUTPUT	1
14	get-write-decision	OUTPUT	1
15	get-execute-decision	OUTPUT	1
16	get-read-write-decision	OUTPUT	1
17	release-usage-attr-decision	OUTPUT	1
18	give-usage-attr-decision	OUTPUT	1
19	rescind-usage-attr-decision	OUTPUT	1
20	create-object-decision	OUTPUT	1
21	delete-object-decision	OUTPUT	1
22	change-sub-curr-sec-level-dec	OUTPUT	1
23	change-obj-sec-level-decision	OUTPUT	1
27	inc-audit-request	INPUT	1
40	obj-audit-request	INPUT	1
44	link-reference-monitor-comd	INPUT	1

Security-control-example

CONSISTS MATRIX REPORT

47	sub-audit-request	INPUT	1
48	create-subject-response	OUTPUT	1
49	delete-subject-response	OUTPUT	1
50	change-sub-max-sec-level-resp	OUTPUT	1
51	link-reference-monitor-resp	OUTPUT	1
52	sub-obj-inc-audit-trail	OUTPUT	1
53	sub-obj-audit-trail	OUTPUT	1
54	sub-inc-audit-trail	OUTPUT	1
55	sub-audit-trail	OUTPUT	1
56	obj-inc-audit-trail	OUTPUT	1
57	obj-audit-trail	OUTPUT	1
58	inc-audit-trail	OUTPUT	1
59	dump-audit-trail	OUTPUT	1

Security-control-example

PROCESS INPUT/OUTPUT

PARAMETERS FOR: PRID

NAME=delete-object INPUT OUTPUT DESCRIPTION PROCEDURE NONEW-PAGE NOINDEX PRINT NOPUNCH

1* delete-object

This process decides whether or not subject with subject-id may delete an object with object-id from the appropriate set in the reference monitor data base.

*** INPUTS ***

1 delete-object-request USED

*** OUTPUTS ***

1 delete-object-decision DERIVED

Security-control-example

CHANGE-TYPE REPORT

PARAMETERS FOR: CHANGE-TYPE

FILE TYPE=GROUP

1* classification-level
OLD TYPE - ELEMENT
NEW TYPE - GROUP

2* category-set
OLD TYPE - ELEMENT
NEW TYPE - GROUP

3* subject-id
OLD TYPE - ELEMENT
NEW TYPE - GROUP

4* object-id
OLD TYPE - ELEMENT
NEW TYPE - GROUP

5* date-time
OLD TYPE - ELEMENT
NEW TYPE - GROUP

Security-control-example

RENAME REPORT

PARAMETERS FOR: RPN

INPUT

SEQ	OLD NAME	NEW NAME
1	security-control-input	security-control-inputs
2	security-control-data-base	security-control-data-bases

Security-control-example

D E L E T E D C O M M E N T E N T R I E S

PARAMETERS FOR: DCOM

DESCRIPTION NOPROCEDURE NOVOLATILITY NOVOLATILITY-MEMBER NOVOLATILITY-SET NODERIVATION
NOTRUE-WHILE NOFALSE-WHILE PRINT FILE

```
1*   security-control-data-bases
          DESCRIPTION;
     1                    The information in this set consists of all
     2               data stored and maintained by the security control
     3               system. ;

2*   security-control-interface
          DESCRIPTION;
     1                    There will be several different types of users
     2               generating requests on the system and retrieving
     3               data from it.  The security controls of the system
     4               must be capable of allowing users of different
     5               authorizations to process concurrently while preventing
     6               the release of information to unauthorized users. ;

3*   security-control-output
          DESCRIPTION;
     1                    The system will produce outputs of several
     2               different types: approvals to data access or modification
     3               requests, audit trails on security features, a
     4               record of outputs produced, etc. ;
```

Security-control-example

D E L E T I O N

PARAMETERS FOR: DEL

FILE

DELETED - security-control-interface
DELETED - security-control-system
DELETED - security-control-inputs
DELETED - security-control-output

R E P L A C E D C O M M E N T E N T R I E S

'ARAMETERS FOR: PCOM

PRINT

' DELETED COMMENT ENTRY **
1* sub-max-sec-level
DESCRIPTION ;
1 This is the maximum security level for a subject.;

' INSERTED COMMENT ENTRY **
1* sub-max-sec-level
DESCRIPTION ;
1 This is the maximum security level for a subject.
2 This subject must never be allowed to access an object
3 which exceeds this security level.;

Security-control-example

DELETED URL

PARAMETERS FOR: DPSL

SOURCE NOXREF

```
LINE  S T M T                                                    ID FIELD

   1 >ENTITY:        objinfo;
   2 >          CONSISTS:    object-location;
   3 >OUTPUT:        dump-audit-trail;
   4 >          HAPPENS:     number-of-dump-audit    TIMES-PER  month;
   5 >PD:            michel-j-bastarache;
   6 >          MAILBOX:     isdos-project-ann-arbor;
   7 >EOF
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
PARAMETERS FOR: FPS

   FILE NOINDEX PRINT NOPUNCH SMARG=5 VMARG=20 AMARG=10 BMARG=25 RNMARG=70 CMARG=1 HMARG=40 DESG
   ONE-PER-LINE DEFINE COMMENT NONEW-PAGE NONEW-LINE

    1 GROUP                                   classification-level;
    2     DESCRIPTION;
    3                   This is a level of classification which may
    4              range up from unclassified to top secret and may be
    5              owned by a subject or an object.;
    6     SEE-MEMO:       clearance-memo;
    7     CONTAINED IN:   sub-max-sec-level,
    8                     sub-curr-sec-level,
    9                     obj-sec-level;
   10
   11 GROUP                                   category-set;
   12     DESCRIPTION;
   13                     This is a set of categories of information which
   14              may be owned by a subject  or an object.;
   15     SEE-MEMO:       category-set-memo;
   16     CONTAINED IN:   sub-max-sec-level,
   17                     sub-curr-sec-level,
   18                     obj-sec-level;
   19
   20 GROUP                                   subject-id;
   21     DESCRIPTION;
   22              This is a unique identifier for a subject.;
   23     CONTAINED IN:   subject-information,
   24                     get-read-request,
   25                     get-write-request,
   26                     get-execute-request,
   27                     get-read-write-request,
   28                     release-usage-attr-request,
   29                     create-object-request,
   30                     delete-object-request,
   31                     change-sub-curr-sec-level-req,
   32                     change-obj-sec-level-request,
   33                     create-subject-command,
   34                     delete-subject-command,
   35                     change-sub-max-sec-level-comd,
   36                     sub-obj-audit-request,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
37                  sub-inc-audit-request,
38                  sub-obj-inc-audit-request,
39                  sub-audit-request,
40                  sub-audit-information,
41                  sub-inc-audit-information,
42                  sub-obj-audit-information,
43                  sub-obj-inc-audit-information;
44      IDENTIFIES:     subject-information;
45      USED BY:
46           check-need-to-know-usage
47            TO DERIVE      error-code;
48      USED BY:
49           check-access-usage
50            TO DERIVE      error-code;
51      USED BY:
52           delete-access-relation
53            TO DERIVE      error-code;
54      USED BY:
55           create-access-relation
56            TO UPDATE      usage-attribute;
57
58  GROUP                                   object-id;
59      DESCRIPTION;
60                  This is a unique identifier for an object.;
61      CONTAINED IN:   object-information,
62                      get-read-request,
63                      get-write-request,
64                      get-execute-request,
65                      get-read-write-request,
66                      release-usage-attr-request,
67                      give-usage-attr-request,
68                      rescind-usage-attr-request,
69                      create-object-request,
70                      delete-object-request,
71                      change-obj-sec-level-request,
72                      sub-obj-audit-request,
73                      obj-audit-information,
74                      sub-obj-inc-audit-request,
75                      obj-inc-audit-information,
76                      obj-inc-audit-request,
77                      obj-audit-request,
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
78                  sub-obj-audit-information,
79                  sub-obj-inc-audit-information;
80      IDENTIFIES:     object-information;
81      USED BY:
82           check-need-to-know-usage
83            TO DERIVE     error-code;
84      USED BY:
85           check-access-usage
86            TO DERIVE     error-code;
87      USED BY:
88           delete-access-relation
89            TO DERIVE     error-code;
90      USED BY:
91           create-object-information
92            TO DERIVE     object-information;
93      USED BY:
94           delete-object-information
95            TO DERIVE     error-code;
96      USED BY:
97           create-access-relation
98            TO UPDATE     usage-attribute;
99
100 GROUP                                   date-time;
101     DESCRIPTION;
102                 This is the date and time an audit incident
103               occurred.;
104     CONTAINED IN:  incident-information,
105                    inc-audit-information,
106                    obj-audit-information,
107                    audit-information,
108                    obj-inc-audit-information,
109                    sub-audit-information,
110                    sub-inc-audit-information,
111                    sub-obj-audit-information,
112                    sub-obj-inc-audit-information;
113
114 SET                                     security-control-data-bases;
115     SYNONYMS ARE:  scdb;
116     SEE-MEMO:      system-philosophy-memo;
117     KEYWORDS:      level-1;
118     ATTRIBUTES ARE:
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
119          specification-derivation
120                         implicit;
121      SUBSETS ARE:    reference-monitor-data-base,
122                      auditing-system-data-base;
123      SECURITY IS:    unclassified;
124
125   /* NAME NOT FOUND IN DB-                 security-control-inputs
126    */
127
128   /* NAME NOT FOUND IN DB-                 scs
129    */
130
131  GROUP                                     sub-max-sec-level;
132      DESCRIPTION;
133                      This is the maximum security level for a subject.
134                 This subject must never be allowed to access an object
135                 which exceeds this security level.;
136      CONTAINED IN:   subject-information,
137                      create-subject-command,
138                      change-sub-max-sec-level-coml;
139      CONSISTS OF:
140                           classification-level,
141                           category-set;
142
143  DESIGNATE                                 objinfo
144       AS A SYNONYM FOR object-information;
145
146  OUTPUT                                    dump-audit-trail;
147      SYNONYMS ARE:   dumaudtra;
148      PART OF:        audit-trail;
149      CONSISTS OF:
150           number-of-incidents
151                           sub-obj-inc-audit-information;
152      DERIVED BY:     dump-audit;
153
154  PROBLEM-DEFINER                           michel-i-bastarache;
155      RESPONSIBLE FOR:
156                      auditing-system,
157                      administrative-security-system,
158                      reference-monitor,
159                      system-security-administrator;
```

Security-control-example

FORMATTED PROBLEM STATEMENT

```
160
161 EOF EOF EOF EOF EOF
```

University of Michigan - MTS

Name Generation

PARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='KEY=level-2 AND PROCESS' ORDER=BY TYPE

1	administrative-security-system	PROCESS
2	auditing-system	PROCESS
3	reference-monitor	PROCESS

University of Michigan - MTS

Name Generation

PARAMETERS FOR: NG

```
PRINT PUNCH EMPTY SELECTION='( NOT PROCESS ) * KEY=level-2' ORDER=BYTYPE
```

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	reference-monitor-request	INPUT
4	reference-monitor-subject	INTERFACE
5	system-security-administrator	INTERFACE
6	administrative-security-resp	OUTPUT
7	audit-trail	OUTPUT
8	reference-monitor-decision	OUTPUT
9	auditing-system-data-base	SET
10	reference-monitor-data-base	SET

University of Michigan - MTS

Name Generation

PARAMETERS FOR: NG

```
PRINT PUNCH EMPTY SELECTION='ATTR=occurrences,unscheduled AND SO=security-control-input'
ORDER=BYTYPE
```

1	administrative-security-comd	INPUT
2	reference-monitor-request	INPUT

Name Generation

ARAMETERS FOR: NG

PRINT PUNCH EMPTY SELECTION='(INPUT OR OUTPUT) * ATTR=specder,implicit' ORDER=BYTYPE

1	security-control-input	INPUT
2	security-control-output	OUTPUT

University of Michigan - MTS

Name Generation

PARAMETERS FOR: NG

```
   PRINT PUNCH EMPTY SELECTION='SO=security-control-input OR SO=security-control-output'
.  ORDER=BYTYPE
```

1	administrative-security-comd	INPUT
2	auditing-request	INPUT
3	change-obj-sec-level-request	INPUT
4	change-sub-curr-sec-level-req	INPUT
5	change-sub-max-sec-level-comd	INPUT
6	create-object-request	INPUT
7	create-subject-command	INPUT
8	delete-object-request	INPUT
9	delete-subject-command	INPUT
10	dump-audit-request	INPUT
11	get-execute-request	INPUT
12	get-read-request	INPUT
13	get-read-write-request	INPUT
14	get-write-request	INPUT
15	give-usage-attr-request	INPUT
16	inc-audit-request	INPUT
17	link-reference-monitor-comd	INPUT
18	obj-audit-request	INPUT
19	obj-inc-audit-request	INPUT
20	reference-monitor-request	INPUT
21	release-usage-attr-request	INPUT
22	rescind-usage-attr-request	INPUT
23	sub-audit-request	INPUT
24	sub-inc-audit-request	INPUT
25	sub-obj-audit-request	INPUT
26	sub-obj-inc-audit-request	INPUT
27	administrative-security-resp	OUTPUT
28	audit-trail	OUTPUT
29	change-obj-sec-level-decision	OUTPUT
30	change-sub-curr-sec-level-dec	OUTPUT
31	change-sub-max-sec-level-resp	OUTPUT
32	create-object-decision	OUTPUT
33	create-subject-response	OUTPUT
34	delete-object-decision	OUTPUT
35	delete-subject-response	OUTPUT
36	dump-audit-trail	OUTPUT

Name Generation

37	get-execute-decision	OUTPUT
38	get-read-decision	OUTPUT
39	get-read-write-decision	OUTPUT
40	get-write-decision	OUTPUT
41	give-usage-attr-decision	OUTPUT
42	inc-audit-trail	OUTPUT
43	link-reference-monitor-resp	OUTPUT
44	obj-audit-trail	OUTPUT
45	obj-inc-audit-trail	OUTPUT
46	reference-monitor-decision	OUTPUT
47	release-usage-attr-decision	OUTPUT
48	rescind-usage-attr-decision	OUTPUT
49	sub-audit-trail	OUTPUT
50	sub-inc-audit-trail	OUTPUT
51	sub-obj-audit-trail	OUTPUT
52	sub-obj-inc-audit-trail	OUTPUT

INDEX

URA Report	Page(s) found in Output
AS-IS SOURCE LISTING	1,3,6,14,23,41,75,96,109, 123
ATTRIBUTE REPORT	143
CHANGE TYPE	207
CONSISTS COMPARISON MATRIX	63
CONSISTS MATRIX	199
CONTENTS REPORT	57
CROSS REFERENCE	7
DATA BASE SUMMARY	27,55,87,100,113,126
DATA PROCESS REPORT	89
DELETED COMMENT ENTRIES	209
DELETED URL	212
DELETION	210
DICTIONARY	131
EXTENDED PICTURE	94
FORMATTED PROBLEM STATEMENT	9,18,33,73,102,105,118, 122,128,147,163,172,181, 184,188,213
FREQUENCY REPORT	108
IDENTIFIER INFORMATION REPORT	70
INDEX	60
KWIC INDEX	197
NAME GENERATION	8,17,32,35,56,62,69,72,88, 101,105,117,121,127,130, 133,142,146,162,171,180, 183,187,218,219,220,221, 222
NAME LIST	22,136
PICTURE	10,12,36
PROCESS CHAIN	114
PROCESS INPUT/OUTPUT	206
PUNCHED COMMENT ENTRIES	134
RENAME	208
REPLACED COMMENT ENTRIES	211
STRUCTURE	28,29,30,31,144,161,170, 179