AD-A280 180

JMENTATION PAGE

Form Approved
OMB No 0704-0188

2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
25 SEPTEMBER 1979	MILITARY STANDARD

4. TITLE AND SUBTITLE
Integrated System Safety Program For The MX Weapon System

5. FUNDING NUMBERS
SAMSO-STD-79-1

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
DET 10, SPACE AND MISSILE SYSTEMS CENTER/SDC
1111 EAST MILL STREET
SAN BERNARDINO, CA 92408-1621

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
BMO-TR-94-23

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The purpose of the MX Weapon System Safety Program is to identify significant accident risk and define methods to cope effectively with that accident risk within program cost, schedule, performance, and risk acceptability parameters. The program encompasses the design, development, fabrication, checkout, modification, test, servicing, maintenance, transportation, handling, training, deployment, and normal/contingency operations of all elements. Elements of the MX Weapon System include operational and test flight vehicles; the ground support equipment required to handle, transport, service, maintain, checkout and test all elements of the MX Weapon System; the ground and flight software required to checkout and control all elements of the MX Weapon System; and the operational and test facilities.

This standard, in conjunction with MIL-STD-1574A, defines the MX integrated system safety program and includes both the management and technical functions to be performed by all contractors providing MX equipment or services to the ICBM Program Office.

SAMSO-STD-79-1 is a tailored application of MIL-STD-1574A and provides for a standardized implementation of the system safety program requirements for the MX Weapon System.

14. SUBJECT TERMS	15. NUMBER OF PAGES
accident risk, risk acceptability parameters, system safety	16. PRICE CODE

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

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

DOD	See DoDD 5230.24, "Distribution Statements on Technical Documents."
DOE	See authorities.
NASA	See Handbook NHB 2200.2.
NTIS	Leave blank.

Block 12b. Distribution Code.

DOD	Leave blank.
DOE	Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
NASA	Leave blank.
NTIS	Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., "UNCLASSIFIED"). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assigned to be unlimited.

*U.S. GPO: 1990-0-273-271

SAMSO STD 79-1
79 September 25

SAMSO STANDARD
INTEGRATED SYSTEM SAFETY PROGRAM

FOR THE

MX WEAPON SYSTEM

SPACE AND MISSILE SYSTEM ORGANIZATION
El Segundo, California

Integrated System Safety Program for the MX Weapon System

SAMSO STD 79-1

1. This SAMSO Standard is approved for use by the Space and Missile System Organization (AFSC), Department of the Air Force.

2 Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: SAMSO/MNBS, Norton Air Force Base, CA 92409, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document, or by letter.

FOREWORD

1. The purpose of the MX Weapon System Safety Program is to identify significant accident risk and define methods to cope effectively with that accident risk within program cost, schedule, performance, and risk acceptability parameters. The program encompasses the design, development, fabrication, checkout, modification, test, servicing, maintenance, transportation, handling, training, deployment, and normal/contingency operations of all elements. Elements of the MX Weapon System include operational and test flight vehicles; the ground support equipment required to handle, transport, service, maintain, checkout and test all elements of the MX Weapon System; the ground and flight software required to checkout and control all elements of the MX Weapon System; and the operational and test facilities.

2. This standard, in conjunction with MIL-STD-1574A, defines the MX integrated system safety program and includes both the management and technical functions to be performed by all contractors providing MX equipment or services to the ICBM Program Office.

3. SAMSO-STD-79-1 is a tailored application of MIL-STD-1574A and provides for a standardized implementation of the system safety program requirements for the MX Weapon System.

CONTENTS

FIGURES

TABLES

APPENDICES

APPENDIX A

MX HAZARD CONTROL ANALYSIS

FIGURES

TABLES

APPENDIX B

MX INTEGRATED SYSTEM FAULT TREE ANALYSIS

APPENDIX C

MX CABLE FAILURE MATRIX ANALYSIS

FIGURES

APPENDIX D

MX SOFTWARE HAZARDOUS EFFECTS ANALYSIS

FIGURES

APPENDIX E

MX HAZARD CONTROL ASSESSMENT REPORT

FIGURES

1. SCOPE

1.1 Purpose. This is a tailored application of MIL-STD-1574A that specifies the system safety program for the Missile X (MX) Weapon System program.

1.2 Application. This standard is applicable to the Space and Missile Systems Organization (SAMSO), MX Associate Contractors, and all other organizations and agencies participating in the MX Weapon System development, test, production, and deployment functions.

2. REFERENCED DOCUMENTS

2.1 Issues of documents. The following documents, of the issue in effect on date of invitation for bids or request for proposal, form a part of this standard to the extent specified herein.

STANDARDS

Military

MIL-STD-1512	Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods
MIL-STD-1574A	System Safety Program for Space and Missile Systems

SAMSO

SAMSO-STD 77-1	Human Factors Engineering for Intercontinental Ballistic Missile Systems
SAMSO-STD 77-6	System Requirements Analysis Program for the MX Weapon System

PUBLICATIONS

AFR 122-10	Nuclear Weapon Systems Safety Design and Evaluation Criteria
AFR 127-12	Air Force Occupational Safety and Health Program
AFR 127-100	Explosives Safety Standards
AFR 127-101	Ground Accident Prevention Handbook
AFR 800-16	USAF System Safety Programs
FED-STD-313A	Material Safety Data Sheets Preparation and Submission of

ICBM PO ED 77-3	Integrated Test Plan for MX Weapon System
ICBM 78-3	Missile X System Safety Program Plan
ICBM 78-4	Missile X System Safety Group Charter
SAMTECM 127-1	Range Safety Manual

3. DEFINITIONS

The following definitions, in addition to all the definitions contained in paragraph 3. of MIL-STD-1574A, apply to this document:

3.1 Accepted risk. A residual hazard which after thorough review and evaluation has been accepted by program management.

3.2 Hazard level categories. MX Weapon System hazard categories are defined by the following examples of worst potential consequences resulting from human error, environmental conditions, deficiency/inadequacy of designs or procedures, or subsystem/component failure or malfunction:

a. Category I – May result in:

1) Loss of life or multiple major personnel injuries/illness/medical effects.

2) Based on a single event, the loss of major MX Weapon System assemblies such as a missile prior to launch, a launch facility, weapon system support facility, or a transporter erector launcher (TEL).

3) Nuclear safety undesired events (as defined in 3.4).

4) Test missile impact outside of hazard corridor.

b. Category II – May result in:

1) Single major or multiple minor personnel injuries/illness/medical effects.

2) Loss of a single element of the MX Weapon System such as a stage, G&C drawer, or important support equipment.

3) Damage to fabrication or weapon system support facilities that would require more than 60 days to repair.

4) Conditions that result in the MX Weapon System being one event (failure or human error) away from a Category I hazard.

c. Category III – Conditions where the worst case potential effect is less than above.

3.3 MX element. A separately contracted entity of the MX Weapon System, e.g. a missile stage, flight computer, transportation and handling (T&H) equipment.

3.4 Nuclear safety undesired events.

a. Accidental motor ignition (AMI) – Accidental initiation of propulsive burning of any missile stage motor, including the post boost vehicle, from causes other than the inadvertent initiation and propagation of a launch sequence. The possibility of human error is not considered when calculating the probability of this event.

b. Faulty launch (FL) – An authorized launch which results in an armed nuclear warhead impacting outside of specified boundaries. The possibility of human error is not considered when calculating the probability of this event.

c. Inadvertent nuclear detonation (IND) – Attainment of nuclear yield from a warhead (more than 4 lbs. TNT equivalent) at any point in the stockpile to target sequence and from any cause other than normal functioning of the warhead upon issuance of an authorized launch command. The possibility of human error or the deliberate unauthorized issuance of secure launch commands are not considered when calculating the probability of this event.

d. Inadvertent programmed launch (IPL) – The inadvertent entrance into terminal countdown or launch countdown and the resultant launch of a missile to a predetermined target. The possibilities of either human error or the deliberate issuance of secure launch messages are not considered when calculating the probability of this event.

e. Inadvertent transmission of intent command – The unintended transmission of the intent command signal, resulting in prearming the weapon. The possibility of human error is not considered when calculating the probability of this event.

f. Inadvertent weapon enabling – A condition which results in the unintentional enabled condition of the weapon, that is, weapon will accept and act on a prearming or arming command. The possibility of human error is not considered when calculating the probability of this event.

3.5 Residual hazard. Any condition that retains the potential of causing injury to personnel or damage to equipment after intended design or other control actions have been taken to reduce the probability and consequences.

3.6 Unique acronyms.

AFOSH	Air Force occupational safety and health
AISP	Analysis Integration and Support Plan
AMI	accidental motor ignition

CSAR	computerized sort and retrieve system
CFMA	cable failure matrix analysis
FL	faulty launch
FMA	failure mode analysis
FTA	fault tree analysis
HCA	hazard control analysis
HCAR	hazard control assessment report
HCR	hazard control report
HCRL	hazard control requirements list
HCRS	hazard control requirements summary
IND	inadvertent nuclear detonation
IPL	inadvertent programmed launch
ISFTA	integrated system fault tree analysis
ISHCAR	integrated system hazard control assessment report
ISSPS	integrated system safety program schedule
NSAR	Nuclear Safety Analysis Report
NWSSG	Nuclear Weapon System Safety Group
PHM	potential hazard matrix
RSP	render safe procedures
SAIC	Safety Analysis Integration Contractor
SHEA	software hazardous effects analysis
SSG	System Safety Group
SSM	System Safety Manager
SSWG	System Safety Working Group
SSPP	System Safety Program Plan
TSA	test safety analysis

4. GENERAL REQUIREMENTS

4.1 System safety program requirements.

4.1.1 Applicable requirements. All requirements contained in MIL-STD-1574A, except as specified in 4.1.2 below or modified by the implementing directions and interpretations contained herein, shall apply to the MX system safety program.

4.1.2 Excepted requirements. The following requirements of MIL-STD-1574A are not applicable to the MX Weapon System contractor system safety programs:

a. Paragraph 4.5.2 – Safety Review Team support

b. Paragraph 4.12.2 – Special nuclear safety analyses:

1) Item b. – Unauthorized launch analysis.

2) Item c. – Nuclear safety crosscheck analysis.

3) Item d. – Safety engineering analysis.

4.2 System safety management.

4.2.1 Management organization.

4.2.1.1 ICBM program office. The responsibility to design, develop, test, and acquire the Missile X Weapon System rests with the ICBM Program Office of the Space and Missile Systems Organization (SAMSO), Air Force Systems Command. The responsibility for establishment of policy and overall management of the MX system safety program has been delegated to the ICBM Program Office System Safety Division (MNBS). Technical and management assistance is provided to MNBS by the Systems Engineering and Technical Assistance (SE/TA) contractor, TRW. A Safety Analysis Integration Contractor (SAIC) assists in performing the coordination and technical integration functions required to implement MNBS safety policies. The relationships and the respective responsibilities of MX Associate Contractors shall be as defined in ICBM-78-3 and this standard. A preliminary definition of organizational relationships during Production and Deployment phases is also contained in ICBM-78-3. System safety programs implemented by agencies/contractors supporting the MX Weapon System development shall recognize and be compatible with this management concept.

4.2.1.2 Supporting contractors. The design, development, test and production of MX Weapon System hardware and software is accomplished by the team of MX Associate Contractors. Each MX Associate Contractor is responsible for establishing and maintaining a system safety program in accordance with the requirements of their respective contracts. Contractual agreements or changes thereto between MX Associate Contractors and the ICBM Program Office shall be made only through the Procuring Contracting Officer (PCO).

4.2.2 General responsibilities.

4.2.2.1 Safety Analysis Integration Contractor (SAIC). The SAIC shall provide system safety integration and support services to MNBS as defined by ICBM-78-3 and in accordance with paragraph 4.3.1 of MIL-STD-1574A and this standard. General tasks shall include performing safety analyses of the overall system, integrating MX Associate Contractor safety analyses, providing assistance in implementing the MX integrated system safety program, and coordinating the activities of the MX Associate Contractor SSMs. MNBS concurrence shall be obtained before the SAIC requests an action from an MX Associate Contractor to assure that the requested action is within the terms and conditions of the respective contracts. When required, the SAIC shall notify MNBS that contractual action is necessary to assure that MX Associate Contractors are responsive to the

integrated systems safety program requirements. The internal organization and functions of the SAIC shall be defined in an Analysis Integration and Support Plan (AISP).

4.2.2.2 MX associate contractors. Contractors providing hardware, software or services to the MX program under direct contract to the ICBM Program Office are designated as MX Associate Contractors. Each MX Associate Contractor Systems Safety Manager (SSM) shall provide support to and be responsive to MNBS and the SAIC as defined by ICBM-78-3 and in accordance with paragraph 4.3.2 of MIL-STD-1574A. Each MX Associate Contractor shall prepare and implement a System Safety Program Plan (SSPP) that defines the scope of the contracted effort and the associated system safety effort.

4.2.2.3 Subcontractors. Each MX Associate Contractor is responsible for the system safety program/activities of his own subcontractors, suppliers or vendors. The method used to establish subcontractor system safety program requirements shall comply with paragraph 4.4 of MIL-STD-1574A, be consistent with the respective MX Associate Contractor requirements, and be approved by MNBS. The hardware or software delivered by an MX Associate Contractor shall be subject to the same assessment and verification, whether produced by the MX Associate Contractor or a first or subsequent tier subcontractor.

4.2.3 Functional responsibilities. Each MX Associate Contractor's System Safety Manager (SSM) shall be responsible to provide an adequate level of effort to comply with all management requirements defined in paragraph 4.1.3 of MIL-STD-1574A. Each MX Associate Contractor shall stress coordination with internal program management, technical elements/disciplines, personnel/industrial safety, and other MX system safety organizations.

4.2.4 Armed services procurement regulations (ASPR). ASPR clauses applicable to each contract are defined in the General Provisions of each contract. This section provides supplemental implementation direction for those ASPR clauses so specified.

4.2.4.1 Accident reporting and investigation (ASPR 7-104.81). Electrically transmitted notifications shall be provided to MNBS, or an agency designated by MNBS within 24 hours of occurrence of any accident involving fatalities, multiple disabling injuries, estimated damages in excess of $10,000, or estimated delays of 20 days for product delivery or 10 days for test site/operational base activities. An internal investigation shall be conducted and a report of all pertinent facts will be prepared and submitted to the Administrative Contracting Officer and MNBS, or an agency designated by MNBS, within 30 calendar days. MNBS/TRW may participate in such investigations at their discretion. If MNBS elects to participate in the investigation, the SSM shall provide all necessary support and assistance.

4.2.4.2 Hazardous material safety data (ASPR 7-104.98). When used in relation to ASPR 7-104.98, the term Hazardous Material shall be as defined in paragraph S20.3.1 of FED-STD 313A. On the MX Weapon System program, Hazardous Material Data Sheets shall be submitted only on material(s) that is delivered to

the government in a form or state that meets the definition of a hazardous material. Transportation data shall be limited to "Proper Shipping Name" and "DOT Classification" as defined in FED-STD 313A. As used on the MX Weapon System Program, the term "disposal" applies to the disposal of hazardous raw material as a normal function. Copies of completed Material Safety Data Sheets shall also be submitted to MNBS.

4.3 System safety engineering.

4.3.1 Primary technical responsibilities. To implement the technical tasks of MIL-STD-1574A, each MX Associate Contractor's system safety engineering function shall be responsible for providing system safety requirements (functional/performance/design constraints) to all program activities, participating in functional analyses and trade studies, performing hazard control analyses and assessments, and supporting system test and operations activities. The tasks required by these responsibilities are presented in calendar format in Figure 1 to show the relationship between tasks and major program milestones. The functional relationship of the major system safety engineering activities are indicated in Figure 2.

4.3.1.1 Design/planning development. The system safety engineering activities shall be continuous iterative processes during the design development and test operations planning of each MX Element. Each analysis, study, or assessment shall be prepared and updated concurrent with design and test or operational planning development in accordance with paragraphs 5.1.3 and 5.2 of MIL-STD-1574A.

4.3.1.2 Change analysis. In support of the implementation of paragraph 4.1.3.m of MIL-STD-1574A, each proposed change to an approved design, as defined in MX Associate Contractor Configuration Management Plans, shall be reviewed by the MX Associate Contractor system safety to determine if a potential safety impact would exist, including interface considerations. The results of this review shall be submitted as part of the Engineering Change Proposal (ECP) package.

4.3.2 System safety technical support. In addition to the criteria, analysis, and trade study activities discussed herein, each MX Associate Contractor's system safety engineering function shall provide informal technical support to program engineering activities in accordance with paragraph 4.1.3.l of MIL-STD-1574A.

5. DETAILED REQUIREMENTS

5.1 System safety program management functions.

5.1.1 System safety program milestones and schedules. System safety milestones shall be defined in relation to major MX Weapon System program milestones. The program milestones shall also provide the basis for all system safety program schedules developed in accordance with paragraph 4.2 of MIL-STD-1574A. The initial definition of major program milestones for the FSED phase is provided in 6.1.

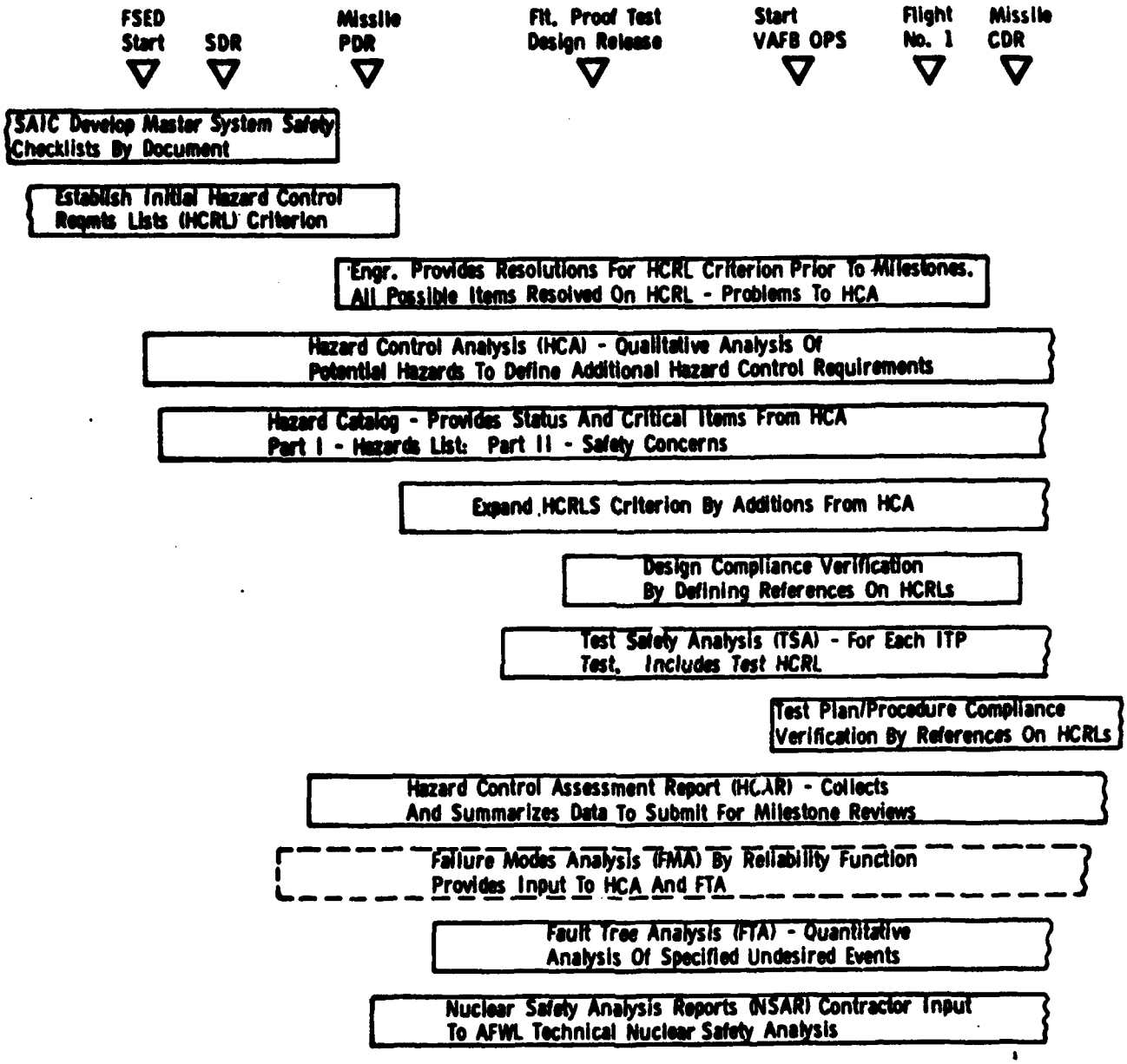


FIGURE 1. System Safety Engineering Activities

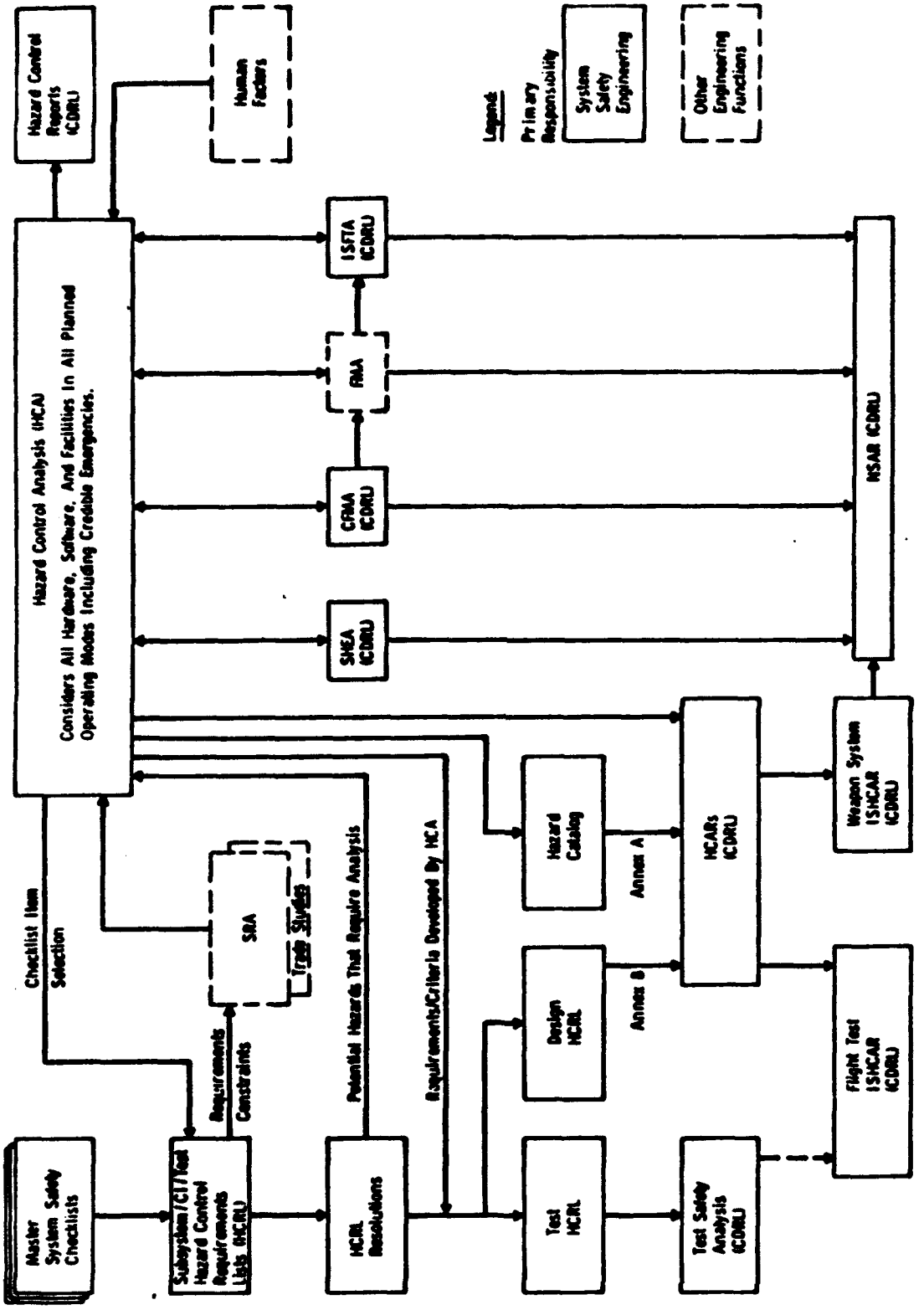


FIGURE 2. Functional Relationship of Tasks

5.1.1.1 Integrated system safety program schedule (ISSPS). The SAIC shall develop and maintain an Integrated System Safety Program Schedule to support the MNBS program management activity. The integrated schedule shall be oriented to major MX Program milestones and shall be based on MX Associate Contractor inputs submitted to the SAIC. The ISSPS shall display items that can be related to either program milestones or calendar dates such as, but not limited to, the following:

a. Contract data requirements.

b. Meetings of the MX system safety group and subgroups.

c. Master System Safety checklists.

d. Audit program activities.

Each MX Associate Contractor shall provide inputs to the ISSPS in a schedule format approved by the SAIC. Associate Contractors may use their existing scheduling techniques and schedules if sufficient detail is provided to meet the SAIC requirements. As a minimum, schedule formats must meet the following requirements:

a. Schedules are time line oriented.

b. Starts and completions are identifiable.

c. Discrete events/milestones are calendar dated.

d. Schedule reflects status, missed events, schedule slippages, etc.

e. Identifies input requirements which constrain an event and the input source.

f. Identifies interfaces between events which are dependent upon each other.

g. Significant safety items identified by the SAIC.

Detail schedules shall be updated each month by the Associate Contractors as part of their monthly status report (see 5.1.1.3). The SAIC shall integrate all schedules and coordinate changes required to achieve compatibility and MNBS approval. The SAIC shall then publish and distribute the Integrated System Safety Program Schedule to all MX Associate Contractors. After the initial issue, the ISSPS will be updated and published by the SAIC as part of the Integrated Monthly Status Report (see 5.1.1.3).

5.1.1.2 Activity schedules and status. In addition to the formal ISSPS, the SAIC shall establish and maintain schedules and status reports of other MX system safety program activities. These activities include items that have short or flexible schedule spans but need to be tracked and recorded. These items shall include, but are not limited to, the following:

a. MX system safety group action items.

b. Potential problem areas list.

c. Informal Data Exchange Schedule and Report.

d. Safety significant trade study support.

e. MX Associate Contractor internal safety audits.

Each MX Associate Contractor shall provide schedule and status reports to these items as required by the System Safety Group, coordination with the SAIC, or as a minimum part of the Monthly Report input (see 5.1.1.3). The SAIC shall integrate all Activity Schedules and Status and publish reports as part of the Integrated Monthly Status Report.

5.1.1.3 Monthly status reports. Each MX Associate Contractor shall provide a monthly letter report to the SAIC concerning the system safety program status. These reports shall be submitted in accordance with the CDRL and shall include the following:

a. Status of applicable ISSPS items, including preparation starts, submittals, and approvals.

b. Safety significant trade studies started or completed during the month including a very brief statement of potential impact of completed items.

c. Dates of internal safety audits.

d. Program reviews or technical interchange meetings supported.

e. Updated Associate Contractor schedules.

f. Activities summary.

g. Information of general interest.

The SAIC shall incorporate the MX Associate Contractor data and provide an Integrated Monthly Status Report that includes the ISSPS, Action Item and data exchange status, and general information. This letter report shall be provided to SAMSO/TRW and all MX Associate Contractors.

5.1.2 Safety data. The following paragraphs identify the safety related data activities for the MX Weapon System Program and provide for the implementation of paragraph 5.4 of MIL-STD-1574A.

5.1.2.1 System safety data requirements. The system safety deliverable data required by MIL-STD-1574A, as tailored by this standard, shall be provided by existing Data Item Descriptions (DIDs) modified as necessary for the MX Weapon System Program. Deliverable safety data, as cited in the CDRLs, shall be presented in the specified format. If no format is specified by either the CDRL or the SAIC, each MX Associate Contractor shall use any format that adequately presents the information. A list of MX program data that may be generated during the program by MX Associate Contractor system safety functions is provided in paragraph 6.1. In accordance with paragraph 5.4.1 of MIL-STD-1574A, management approval and submittal of all safety data listed in 6.2 6.1 shall constitute certification that accuracy, completeness and validity has been attested to by a qualified system safety engineer and that the system can be operated safely. Such certification is required before product acceptance.

5.1.2.2 Safety critical program documentation. Each MX Associate Contractor SSM shall maintain internal project approval authority over safety critical program documentation in accordance with paragraph 4.1.3.d of MIL-STD-1574A. Approval shall be granted only when the document contains all appropriate system safety requirements and constraints. Each SSM shall maintain a log of documentation reviewed in accordance with paragraphs 4.1.3.c and 5.4.4 of MIL-STD-1574A. This log shall be available for review by SAMSO/TRW/SAIC. Table I provides a list of data that is considered safety critical for the MX Weapon System Program.

5.1.2.3 Data acquisition and dissemination. The SAIC shall implement and maintain a data acquisition and dissemination system that assures all applicable system safety data is identified and all program data required by any MX Associate Contractor/agency is provided in a timely manner. To accomplish this, the SAIC shall perform the following specific tasks:

a. Evaluate all contractor CDRLs to determine if safety data distribution is proper and compatible with the Integrated System Safety Program Schedule (see 5.1.1.1).

b. Request SAMSO/MNBS to initiate contract changes to CDRLs as required.

c. Maintain a composite data file as described in 5.1.2.4.

d. Provide for and maintain a system of informal data exchange as described in 5.1.2.5.

TABLE I. Safety critical program data.

Item	Document Title, Subtitle
1	Prime Item Development Specifications
2	Critical Item Development Specifications
3	Facility Development Specifications
4	Computer Program Development Specifications
5	Interface Control Drawings
6	Engineering Change Proposals
7	Equipment Test Plans and Procedures
8	System/Design Trade Study Reports
9	Failure Mode Analysis
10	Medical Incident Notification
11	Hazardous Material Data Sheets
12	Flight Plan Approval Package
13	Hazard Analysis Study Report, Range Safety
14	Missile Flight Safety Data, Range Safety
15	Flight Termination System Report, Missile
16	Radiological Safety Analysis Summary and Radiation Protection Plan
17	Procurement Drawings/Specifications
18	System Test Procedures

5.1.2.4 Data files. The SAIC shall maintain MX Weapon System safety related data/documentation in an MX System Safety Library. This library shall include MX Associate Contractor data, integration management data, deliverable data/documentation, data obtained from program reviews and system safety group meetings, and reference material. Full identification of all items in the library, with current revision status, will be maintained by a Computerized Catalog Index. The index shall be provided to SAMSO/TRW and MX Associate Contractors with quarterly updates. This library shall be available to SAMSO/TRW and MX Associate Contractors at the SAIC facility. Individual documents will be made available for loan as determined by the SAIC. Each MX Associate Contractor system safety organization shall maintain current safety data listed in the MX System Safety Library index that is pertinent to that contract. The MX Associate Contractor SSM shall also be responsible for dissemination of system safety information to their other organizational elements, including subordinate contractors/suppliers.

5.1.2.5 Informal data interchanges. Technical data shall be interchanged between contractors on an informal basis in accordance with paragraph 4.3.1.h of MIL-STD-1574A. Technical data, as used in this paragraph, shall include draft or preliminary copies of data to be delivered formally under the contract at a later date, data developed in response to an MX Action Item, or published information. In the event proprietary data is involved, it shall be controlled in accordance with the applicable contracts. Data requests and status reports of all data interchanges shall be provided to the SAIC for incorporation into an Informal Data Exchange Schedule and Report. This monthly report shall be computerized and maintained similar to an action item list.

5.1.3 System safety group support. An MX System Safety Group (SSG), established under the provisions of AFR 800-16 assists the SAMSO Program Manager in implementing the MX safety program. Membership includes respresentatives of major Air Force commands, supporting agencies and MX Associate Contractors as specified in ICBM-78-4. This group reviews safety policies and procedures for the MX system, assists in resolving safety problems, and initiates required corrective action. The MX SSG is chaired by the SAMSO Assistant Deputy for Missile X, with the SAIC acting as recorder.

5.1.3.1 Contractor support requirements. In accordance with paragraph 4.5.1 of MIL-STD-1574A, each MX Associate Contractor shall be members of the MX SSG and provide support as required by ICBM-78-4. Each MX Associate Contractor shall respond to Action Items and provide requested presentations at MX SSG meetings. The SAIC shall also provide the normal clerical and administrative services required for the SSG operation, including preparation of the agenda and minutes. Action Items assigned by the SSG chairman shall be recorded and tracked by the SAIC. The status of Action Items shall be reported at each SSG meeting, in SSG meeting minutes, in monthly letter reports, and upon MNBS request. The SAIC shall coordinate activities and interchanges between the SSG and its subgroups.

5.1.3.2 MX System Safety Working Groups (SSWG). MX SSWGs will be formed as subgroups to work specific problems or provide specialized support to the MX SSG. Each MX Associate Contractor shall provide support to any SSWG established in accordance with its charter or implementing SSG directive. The SAIC, with MNBS concurrence, shall schedule meetings as required to integrate the safety effort, coordinate data exchange schedules, and resolve safety problems. The SAIC shall provide complete secretarial services, including preparation of minutes and maintenance of Action Item lists.

5.1.3.3 Nuclear Weapon System Safety Group (NWSSG). The NWSSG reviews all nuclear safety aspects of the design and operational procedures of the MX Weapon System to ensure compliance with DOD nuclear safety standards and operational requirements. The SAIC and each MX Associate Contractor shall support NWSSG studies, including briefings to the NWSSG on the complete weapon system and its nuclear safety aspects, to assure that nuclear safety standards have been met. The NWSSG support shall be provided as requested as part of the direct support to the nuclear weapon system program objectives defined in paragraph 4.12 of MIL-STD-1574A.

5.1.4 System safety audit program. The MX system safety audit program is a management process which assures that the objectives and requirements of the MX Weapon System accident risk management program are accomplished in conjunction with the overall MX program milestones. Implementation of paragraph 5.6 of MIL-STD-1574A shall be in accordance with the following.

5.1.4.1 ICBM program office audits. SAMSO/MNBS will conduct, with SAIC assistance, audits of the MX Associate Contractors system safety program. The audits performed of the MX Associate Contractors will measure the current program status of each safety task, assess compliance with their contract, determine the interrelationship between safety and other program disciplines, and provide documented evidence of safety criteria implementation. MX Associate Contractors shall correct identified deficiencies and MNBS will initiate corrective actions to resolve any safety program contract incompatibilities. The audit schedule established shall be shown on the Integrated System Safety Program Schedule (see 5.1.1.1). An audit data file shall be maintained by the SAIC for MNBS. Each MX Associate Contractor SSM shall provide support to MNBS for government directed audits.

5.1.4.2 MX associate contractor audits. An internal system safety audit program, independent from the MX System Safety Organization, shall be conducted by each MX Associate Contractor in compliance with paragraph 5.6 of MIL-STD-1574A. Each MX Associate Contractor shall conduct audits, including audits of subcontractors, at least annually. MX Associate Contractor audit reports, including subcontractor audits, shall be maintained on file for review by MNBS and the SAIC. Reports shall include discrepant items, the corrective action and schedule required, and followup reports to closeout items.

5.1.5 Program/design reviews. Each MX Associate Contractor System Safety Manager shall provide safety participation in all design reviews of their equipment in compliance with paragraph 5.6.2 of MIL-STD-1574A. Presentation of system safety program status and problems that impact MX program goals shall be included in each program review. Presentation of MX Associate Contractor system safety analysis status, identification of unacceptable accident risk factors, and hazard reduction status shall be included in each design review.

5.2 System safety criteria.

5.2.1 Hazard classification. Identified hazards shall be classified in accordance with 3.2 based on conditions arising from human error, environmental conditions, deficiency/inadequacy of design or procedures, or subsystem/component failure or malfunction. The qualitative categories of 3.2 are defined by examples to provide guidance in classification. The assignment of categories is subjective and should be considered primarily to establish priorities for defining/accomplishing corrective actions.

The list of examples of unacceptable and acceptable conditions contained in paragraphs 5.1.1.1 and 5.1.1.2 of MIL-STD-1574A shall also be used as a separate guide to classify hazards, except that 5.1.1.1.b and 5.1.1.2.b do not apply to the MX Weapon System. Each MX Associate Contractor shall develop and refine lists of unacceptable and acceptable conditions for the specific equipment being provided. The lists shall contain only conditions that are applicable to the operational weapon system. The lists shall be included in the applicable Hazard Control Assessment Report (see 5.8) and the SAIC shall integrate the lists in the Integrated System Hazard Control Assessment Reports.

5.2.2 Safety concerns. The designation of any accident risk factor/hazard as a "Safety Concern" will be given by MNBS. Each MX Associate Contractor shall maintain a working file of those accident risk factors which they consider significant enough to be designated as "Safety Concerns". The working file shall be reviewed by MNBS and the SAIC at SSG/TIM or analysis/data coordination meetings. The agreed upon "Safety Concerns" shall be reported as Part II of the Hazard Catalog in accordance with 5.4 and Appendix A.

5.2.3 Hazard closure. The following criteria shall apply to the closure of all identified potential accident risk factors/hazards.

5.2.3.1 Closure requirements. An identified potential accident risk factor/hazard shall be considered closed when one of the following conditions exist.

a. Analysis has determined that the potential hazard is not a credible condition.

b. The hazard is eliminated by design and design accomplishment has been confirmed.

c. The hazard has been controlled by appropriate design, safety devices, alarm/caution and warning devices, or special automatic/manual procedures and the control has been verified by test and/or analysis. The order of precedence defined in 5.2.4 applies to all hazard control actions.

5.2.3.2 Approval requirements. The following level of authority is required to approve the closure of accident risk factor/hazards.

a. A system safety engineer may, subject to SSM review, close analysis items that result in hazard level Category III or are not credible.

b. Closure of Category I and II items not designated as "Safety Concerns" shall require approval of the MX Associate Contractor System Safety Manager.

c. Closure of all "Safety Concerns" shall be approved by the applicable MX Associate Contractor Program Manager and the SAMSO Program Office.

5.2.4 System safety precedence. The order of precedence for actions to eliminate or control accident risks is to design for minimum hazard, use appropriate safety devices, use protective systems, use warning devices, or develop special procedures (see 5.1.2 of MIL-STD-1574A). Acceptable justification for descending the order of precedence shall be provided in Hazard Analysis Reports and Hazard Control Assessment Reports.

5.2.5 Design/operations requirements. The minimum system safety requirements, criteria, and constraints for the MX Weapon System are contained in existing established specifications, standards, regulations and manuals. The MX System Safety Program shall use computerized data management methods to develop, disseminate, and control standardized design and operations requirements to implement paragraph 5.1.3 of MIL-STD-1574A. The MX System Safety computer files are an element of the Computerized Sort and Retrieval (CSAR) system used by all MX Associate Contractors in the System Requirements Analysis (SRA) process. The following data files are used for requirements processing.

5.2.5.1 System safety checklists. The SAIC shall prepare standardized System Safety Checklists for use by MX Associate Contractors in a format compatible with the Hazard Control Requirements List format of Figure 3. A master System Safety Checklist shall be developed for each applicable established document to include all requirements defined in that document. These master checklists shall be maintained by the SAIC and made available to MX Associate Contractors in the form of a computer data set and one printed copy.

5.2.5.2 Hazard control requirements lists (HCRL). To implement paragraph 5.2.2 of MIL-STD-1574A, each MX Associate Contractor shall develop HCRLs, in the format of Figure 3, that are tailored and applicable to specific subsystems, configuration items (CI), test operations, or engineering disciplines. The initial HCRLs shall be developed by combining criterion items from applicable master System Safety Checklists. Each SSM shall assure that the HCRLs include all and

Hazard Control Requirements List

Doc. & Rev. / Item No.	Prog Element: / Source: / Type:		COMPLIANCE	NON COMPL	NOT APPL	Sect. Or System / Criterion Date: / Resolution Date:	Sect. No: / Page	
ddd.rr-nnnnn	Criterion	System				Resolution		Reference

FIGURE 3. Hazard Control Requirement List

only applicable requirements. The HCRLs shall be maintained and updated throughout the MX program life cycle. The following instructions apply to the maintenance and use of HCRLs.

a. The requirements listed in the HCRL Criterion section shall be adjusted by adding or deleting items during coordination with responsible engineering functions. Any required change in wording shall be coordinated with the SAIC.

b. The HCRL Criterion sections may be used to provide system safety requirements to project functions.

c. The responsible engineering functions shall provide data for an explanation, in the Resolution section, of the provisions for compliance or the rationale for noncompliance with each criterion. Initial response shall be provided to support PDRs with progressively greater detail at successive design reviews.

d. All Resolution section entries shall be reviewed/approved by system safety engineering. Items of noncompliance considered to be an accident risk factor shall be subjected to the Hazard Control Analysis discussed in 5.4. Insofar as possible, however, Criterion items shall be resolved on the HCRL in lieu of initiating a Hazard Analysis report for that item.

e. Additional criterion developed by the Hazard Control Analysis described in 5.4 shall be incorporated after being computerized in accordance with 5.2.5.3.

f. Compliance with all system safety requirements shall be verified by providing appropriate reference(s) to specification, drawing, procedure or similar controlling documentation in the Reference column. References shall be provided when documents are under configuration control to implement paragraph 5.2.12 of MIL-STD-1574A.

g. The HCRLs shall be included as part of the Hazard Control Assessment Report as discussed in 5.8.

5.2.5.3 Hazard control requirements summary. To assist in the incorporation of criterion developed by the Hazard Control Analysis into the HCRLs, a computer data file, identified as a Hazard Control Requirements Summary (HCRS), shall be established for each section of the Hazard Control Analysis. As the individual Hazard Analysis Reports (see Appendix A) are completed, the hazard control requirements shall be entered into the HCRS for that analysis section. The HCRS is in effect a master system safety checklist of the analysis results and simply provides for computer storage and data management of hazard control requirements developed by the Hazard Control Analysis. The computer sort capability is then used to separate and merge these items with the appropriate design or test HCRL.

5.2.6 Deviations. Compliance with all contractually imposed technical and policy safety requirements/criteria is mandatory unless exceptions are approved by SAMSO. Noncompliance with safety requirements for management policies or

functions, equipment design, documentation, software, or procedures shall require formal approval. For the MX program, paragraph 5.1.4 of MIL-STD-1574A shall be implemented as follows:

a. Requests for deviations to system safety requirements or criteria shall be prepared by the responsible MX Associate Contractor SSM and submitted to MNBS with one copy to the SAIC.

b. Each request shall include the data required by paragraph 5.1.4 of MIL-STD-1574A.

c. The SAIC shall evaluate the request to determine program or system impact and submit a recommendation to MNBS. The SAIC shall establish and maintain the master record of all requests submitted including subject, date submitted, and disposition.

d. Each request will be processed by SAMSO in accordance with provisions of the individual contracts. Deviations approved by SAMSO will be incorporated in an Appendix to the applicable SSPP or Hazard Control Assessment Report (see 5.8).

5.3 System requirements analysis (SRA). A primary objective of the MX Integrated system safety program of each MX Associate Contractor is to support the SRA process defined in SAMSO STD 77-6 including the Operational Requirements Analysis (ORA), the Test Planning Analysis (TPA), the Logistics Support Analysis (LSA), and the Assembly and Checkout Technical Analysis (A&CO).

5.3.1 System safety requirements. Each MX Associate Contractor shall review and evaluate the functional flow diagrams, associated Forms B, and the Configuration Item Constraint Identification matrices relating to equipment for which they are responsible. System safety functional/constraint requirements/inputs shall be provided to the SRA functional element. This evaluation and input shall initially be based on the System Safety Checklists/HCRLs discussed in 5.2.5, then on the Hazard Control Analysis discussed in 5.4 and the Test Safety Analysis of 5.6. The functional flows and Forms B also provide input to these analyses to aid in the identification of potential hazards. Traceability between the SRA process and system safety engineering documentation shall be provided and maintained.

5.3.2 Emergency analysis. The ORA includes investigation of possible emergencies in conjunction with the critical fault assessment. The Hazard Control Analysis provides the method of predicting potential emergencies to be examined by the SRA Emergency Analysis. Each MX Associate Contractor system safety function shall participate in the conduct of the SRA Emergency Analysis in accordance with paragraph 5.1.5 of SAMSO STD 77-6.

5.3.3 SRA system safety integration. The SAIC shall review all functional flows and verify that all functions are assigned to the appropriate MX Associate

Contractor system safety organization for review and input. The SAIC shall periodically review MX Associate Contractor SRA activities and provide guidance and assistance as required to assure uniform safety inputs.

5.3.4 Trade study support. To implement paragraphs 4.1.3.n and 4.14 of MIL-STD-1574A, each MX Associate Contractor shall establish a method that ensures system safety organization participation in all studies of safety concern performed by that contractor. In addition, each MX Associate Contractor shall assure that safety impact items and hazard control assessments are significantly highlighted and given appropriate weight as decision drivers. Trade Study Reports shall show that the selected alternative has the least accident risk or provide sufficient justification for recommending another alternative. System safety studies and analyses shall be performed as required to assess the relative accident risk for each proposed alternate solution.

When directed by MNBS, the SAIC shall review results of MX trade studies which involve two or more MX Associate Contractors to assure that management level decisions include the optimum safety provisions consistent with other program considerations. The SAIC shall identify differences between MX Associate Contractors in technical areas related to safety, and shall make recommendations on trade study results to MNBS.

5.4 Hazard control analysis. The analyses of paragraphs 5.2, 5.2.1, 5.2.3, 5.2.4, 5.2.5, 5.2.8, and 5.2.9 of MIL-STD-1574A for the MX Weapon System shall be conducted as a continuous iterative Hazard Control Analysis (HCA) in accordance with this Section and Appendix A.

5.4.1 Purpose. The purpose of the HCA is to identify potential accident risk, establish design criteria and operational constraints to eliminate or control that accident risk, and provide the basis for hazard control assessments. The analysis shall consider all hardware and software elements in all planned normal operations and credible abnormal/emergency conditions. The software elements shall be considered as an entity with the associated hardware element. The method described in Appendix A provides the means to systematically examine each hardware system/subsystem in each of its activity phases or operating modes and combines the features of design and operational hazard analyses. The procedure used for this comprehensive analysis method implements the intent of paragraph 5.2.13 of MIL-STD-1574A. The results shall include definition of test procedure cautions/warnings and personnel protective equipment requirements. Operational considerations include those accident risks that could result in damage to the equipment/system or interfacing equipment that would preclude a successful operation. Those conditions which are confined to the equipment/system and only result in performance degradation shall be considered to fall within the jurisdiction of the engineering and reliability functions.

5.4.2 Schedule. The HCA shall be initiated by each MX Associate Contractor at the start of the development effort. All potential hazards and supporting data included in Preliminary Hazards Lists during the System Definition Phase shall be included in the HCA and maintained current by the documentation of 5.4.3. The HCA activity shall be continuous until final CDR, then updated as required for engineering changes.

5.4.3 Documentation. The initiation and results of the analysis of identified potential hazards shall be documented and submitted periodically as Hazard Control Reports (HCR) in accordance with the CDRL. HCRs shall consist of legible working papers of Potential Hazard Matrices and Hazard Analysis Reports (see Appendix A) with supporting data that includes all items initiated or revised during the period.

Hazard Catalogs (see Appendix A) shall be submitted as Annex A to the Hazard Control Assessment Reports described in 5.8 and Appendix E.

5.5 Specialized safety analyses.

5.5.1 Integrated system fault tree analysis (ISFTA). The SAIC shall conduct an MX ISFTA in accordance with Appendix B to implement paragraph 4.12.2.a of MIL-STD-1574A.

5.5.1.1 Purpose. The primary purpose of the ISFTA is to verify compliance with defined quantitative safety requirements.

5.5.1.2 Schedule. The ISFTA of the nuclear weapon system undesired events shall be initiated by the SAIC immediately after the last missile element PDR and continue until program completion. Each MX Associate Contractor shall support the SAIC by assuring that the FMA provides adequate and timely numerical data and by development of subsystem FTAs as directed by the procuring contracting officer.

5.5.1.3 Documentation. Formal submittal of the FTAs shall be in accordance with the CDRLs.

5.5.2 Cable failure matrix analysis (CFMA). Each MX Associate Contractor responsible for development of cable assemblies shall develop CFMAs in accordance with Appendix C to support implementation of paragraph 5.2 of MIL-STD-1574A.

5.5.2.1 Purpose. In addition to and in support of the FMA required by Appendix A, paragraph 50.6 of SAMSO STD 77-6, a CFMA shall be developed for the interconnecting cables and connectors for each cable assembly within a CI. The predominant failure events identified from the cable failure matrix, affecting the desired output of a cable, will be included in the FMA for the associated CI.

5.5.2.2 Documentation. Formal submittal of the CFMA shall be in accordance with the CDRL. The matrices may also be included in the FMA report.

5.5.3 Software hazardous effects analysis (SHEA). Each MX Associate Contractor responsible for the development of software shall conduct a SHEA in accordance with Appendix D to implement paragraphs 5.2.6 and 5.2.7 of MIL-STD-1574A. For the purposes of this section, the term software system shall include the system specification, computer program, the computer itself, and all the peripheral equipments which enable the system to operate.

5.5.3.1 Purpose. The SHEA shall be performed on all software having direct interface with the operational nuclear weapon system and shall be performed by

the software development contractor during software design and development. The objective of the SHEA is to identify potential hazardous effects to the weapon system, both external to the software system (such as erroneous or improperly timed commands) and internally controlled actions; such as computer commands causing illegal entry into critical routines. All routines and functions of the software system are to be examined. The results of the SHEA shall be used to:

a. Affect the design of the software system wherever practical to assure control of possible system hazards.

b. Identify to the SAIC, for inclusion in the integrated weapon system fault tree analysis, those potential hazards introduced or impacted by the software system.

5.5.3.2 Documentation. Formal submittal of the SHEA shall be in accordance with the CDRL.

5.6 Test safety analysis (TSA). Paragraph 5.2.10 of MIL-STD-1574A and Analysis Table 20-A52, Operating and Testing Hazard Analysis, of ED 77-3 shall be implemented by the performance of Test Safety Analyses.

5.6.1 Purpose. The Hazard Control Analysis (HCA) of 5.4 identifies operational constraints and cautions/warnings to eliminate or control specific accident risk factors in each MX element. A TSA shall be performed for each MX Weapon System test identified in ED 77-3 to assure a systematic and complete evaluation of all the functional aspects and test interfaces. The TSA shall be based on applicable HCA and the SRA Test Planning Analysis (TPA) and shall provide inputs to detail test/operations plans, procedures, and technical publications.

5.6.2 Content. Each test shall be evaluated to identify hazardous materials or operations. TSA reports for hazardous tests shall include the following:

a. A narrative introduction to define the purpose, scope and summary of the analysis.

b. A definition of the test operation including a brief narrative, with reference to detail data, single line diagram(s), and a test sequence flow or timelines.

c. An assessment of the test in both narrative form and a list of potential hazards with control requirements.

d. The Hazard Control Requirements List (see 5.2.5.2) for the test and the test items.

Data developed by the TPA process shall be used to the maximum extent. The SSM, however, shall be responsible for the accuracy of all data contained in the TSA report.

TSA reports for non-hazardous tests shall be brief statements to verify that the test was evaluated and no hazards were identified.

5.6.3 Schedule. TSAs shall be conducted concurrently with the TPA activity and drafts shall be completed to provide support to test procedure development. The final TSA shall include verification that procedures comply with safety requirements and shall be available for pretest reviews.

5.6.4 Documentation. MX Associate Contractors shall be responsible for the TSA, with support from others as required, when designated as the test conductor in ED 77-3. SAMSO shall be responsible for the TSA when a governmental agency is designated as test conductor in ED 77-3. The TSA Reports shall be submitted in accordance with the CDRL.

5.7 Nuclear safety analysis.

5.7.1 Nuclear safety analysis report (NSAR) The SAIC shall be responsible for the preparation of an integrated Nuclear Safety Analysis Report in support of paragraph 4.12 of MIL-STD-1574A. Each MX Associate Contractor shall provide necessary support and data to the SAIC.

5.7.1.1 Purpose. The NSAR will provide contractor input to the Technical Nuclear Safety Analysis (TNSA) performed by the Air Force Weapons Laboratory. The TNSA supports the nuclear safety evaluation conducted by the Nuclear Weapon System Safety Group.

5.7.1.2 Content. The NSAR shall be based on MX Associate Contractor System Safety Analyses, Hazard Control Assessment Reports, other contracted data, and the Integrated System Fault Tree Analysis. The NSAR shall include complete description of the MX Weapon System and capabilities, evaluation of malfunction modes and effects, nuclear safety features and deficiencies, and an overall assessment of the nuclear safety of the weapon system.

5.7.1.3 Schedule. The NSAR shall be prepared to support the Initial NWSSG Study and the Preoperational NWSSG Study during the Full Scale Engineering Development Phase.

5.7.1.4 Documentation. Formal submittals of the NSAR shall be in accordance with the CDRLs .

5.7.2 Unauthorized launch analysis. An Unauthorized Launch Analysis will be conducted by TRW in support of paragraph 4.12 of MIL-STD-1574A. Selected MX Associate Contractors will evaluate portions of their equipment to determine susceptibility to actions leading to unauthorized launch.

5.7.2.1 Purpose. The Unauthorized Launch Analysis defines the time, tools, and equipment required to accomplish the actions leading to unauthorized launch. This information will be utilized by the nuclear safety evaluation agency in determining whether or not design changes or additional procedural constraints are required to provide adequate protection against these unauthorized activities.

5.7.2.2 Content. Launch scenarios will be drawn up by TRW with assistance from the selected MX Associate Contractors. These scenarios will be further divided into specific actions against individual items of equipment. The MX Associate Contractor whose equipment is involved will be tasked to identify the vulnerability of his equipment to the specific actions. Individual contractor inputs will become an appendix to the Unauthorized Launch Study report. TRW will assemble the final report using the inputs from individual associates, supplemented by TRW analyses to cover the interfaces.

5.7.2.3 Schedule. The analysis will start about midway between PDR and CDR such that sufficient evaluation will have been done by CDR to uncover all major system vulnerabilities. The report will be finalized subsequent to the CDR and will reflect an evaluation of the CDR design.

5.7.2.4 Documentation. Formal data submittals shall be in accordance with the CDRLs.

5.8 Hazard control assessment report (HCAR). Paragraph 5.2.14.2 of MIL-STD-1574A shall be implemented by the preparation of HCARs in accordance with this section and Appendix E. The certifications of paragraph 5.3 of MIL-STD-1574A shall be accomplished by the submittal of HCARs showing approval as defined in Appendix E.

5.8.1 Purpose. The HCARs shall provide a comprehensive evaluation of the safety critical accident risk factors/hazards involved when the MX Weapon System is subjected to checkout, test, and operation at a test facility or operating site. The HCARs shall be the product of the system safety engineering tasks and shall verify that system designs and operational planning meet the safety requirements of the test site and the MX system can be safely operated and maintained.

5.8.2 Content. Each MX Associate Contractor shall prepare an HCAR for each MX Element, system, Configuration Item(s), and/or facility within their responsibility in accordance with Appendix E. A single HCAR may be prepared for like items of noncomplex CIs or several CIs that form an operating entity. Collecting of CIs into a single HCAR shall be subject to approval by MNBS. The reports shall contain narrative introductions, assessment summaries, element hardware and functional descriptions and detailed assessments. Each complete HCAR shall also include the following annexes:

a. Hazard Control Analysis Hazard Catalog

b. Hazard Control Requirements Lists

c. Deviations (when required)

d. Classified Data (as a separate document when required).

The SAIC shall develop two basic Integrated System Hazard Control Assessment Reports (ISHCARs) as follows:

a. A Flight Test ISHCAR which shall include all the elements (hardware, software, and facilities) required to conduct the MX flight test program.

b. A Nuclear Weapon System ISHCAR which shall include all the elements (hardware, software, and facilities) required to deploy, operate, and maintain the MX Weapon System.

The ISHCARs shall incorporate the appropriate HCARs, assess all interface problems, and summarize MX Weapon System Safety concerns. The ISHCAR shall retain each element HCAR as an appendix. Classified data annexes shall be bound separately.

5.8.3 Schedule. The HCARs shall be prepared incrementally in conjunction with other system safety engineering tasks.

5.8.4 Documentation. Formal submittals of the HCAR shall be by individual sections and annexes in accordance with the CDRL. The first complete report shall be available to support Flight Proof Test Design Release. MX Associate Contractors shall provide working paper data when requested by MNBS for incremental review at SSG or Technical Interchange Meetings.

5.9 Operating safety considerations. The system safety program related to operating safety considerations (system tests/flight tests/operational base activities) shall provide for assuring safe facilities and support equipment, compliance with range/explosives/nuclear safety requirements, and the controls/surveillance to assure safe tests and operations. These factors shall also be included in all analysis and planning activities to prepare for production, deployment, and operational program phases. Since test activities will be well underway prior to start of operational base activities, the test safety analyses and hazard control analyses already accomplished on transportation and handling equipment, test (maintenance) equipment and launcher equipment will be revisited to assure consideration of currently defined activities at an operational base. Many of the procedures used during test, along with their caution and warning notes, will be refined and after validation and verification will become part of the Technical Orders by which the weapon system will be operated and maintained. Any operating base peculiar operations shall be subjected to a Test Safety Analysis to determine the precautionary measures required in procedures. Each MX Associate Contractor is responsible for the operating safety considerations of the subsystem/elements developed on his respective contract. MX Associate Contractors will validate these procedures and participate in the verification of these procedures by the Using Command.

5.9.1 Facilities and support equipment. Safety requirements and design criteria for facilities and support equipment/materials shall be provided by the MX Associate Contractors and the SAIC in compliance with paragraphs 4.8 and 4.11 of MIL-STD-1574A. A Hazard Control Analysis (see 5.4) shall include each new MX test and operational facility and all items of support equipment (test and operational) to assure identification and control of hazards. The siting and design

of facilities shall comply with the explosives safety criteria of AFR 127-100. Designs of facilities and support equipment shall comply with AFR 127-101, applicable AFOSH Standards developed in accordance with AFR 127-12, construction and health/environmental requirements and nuclear safety criteria. In verifying the adequacy of safety provisions, consideration shall be given to both the test program and the deployment/operational phases. Evaluation criteria shall include the applicable Air Force, State or Federal OSHA regulations. Identified requirements and criteria shall be upgraded and refined to incorporate additional safety requirements as inputs from the MX Associate Contractors' Hazard Control Analyses are received. Identified safety problems concerning Government furnished facilities and support equipment shall be reported to MNBS and the SAIC.

5.9.2 Range safety. Although the MX Weapon System must satisfy the applicable safety criteria of SAMTECM 127-1 during test and operations at VAFB, compliance shall be accomplished in a manner that does not degrade or compromise the operational effectiveness of the Weapon System. Each MX Associate Contractor shall implement paragraph 4.9 of MIL-STD-1574A by assuring that applicable Range Safety criteria/requirements are considered in Hazard Control Analyses and Test Safety Analyses. Verification that system design and operational planning comply with range or test site safety requirements (except for flight analysis, flight termination and trajectory requirements) shall be documented in the Hazard Control Assessment Report (See 5.8).

5.9.3 Explosives and ordnance safety. The design, test, and operation of ordnance initiation systems and devices, and solid rocket motors shall comply with the criteria specified in AFR 127-100, AFR 122-10, and MIL-STD-1512. Required waivers or deviations, including Explosives Quantity-Distances, shall be processed in accordance with 5.2.6. Explosive systems, subsystems, and components shall be subjected to the analyses described in 5.4, 5.5, and 5.6 for early identification and elimination or reduction of unacceptable accident risks. MX Associate Contractors shall assure that each explosive and ordnance item is properly identified by its military explosive hazard classification, storage compatibility group, fire symbol, and DOT shipping classification. Control of explosive items shall be provided by Data Cards for Explosive Assemblies, Subassemblies, and Parts prepared in accordance with the CDRL. Explosives Hazard Classification Data on any new or modified explosive items or components that have not previously received a USAF approved hazard classification shall be submitted by the applicable MX Associate Contractor in accordance with their CDRL. Explosive Ordnance Disposal (EOD) Procedures including Explosives Render Safe Procedures (RSP) shall be developed early enough in the program to assure that a disaster response capability is available in the event of an accident or potential hazard. These procedures shall be submitted in accordance with the applicable CDRL.

5.9.4 Nuclear weapon system safety. The prime purpose of the MX system safety program is to field a nuclear weapon system which is safe to assemble, transport, operate, and maintain. All elements of safety are involved in accomplishing this overall objective. There are, however, specific nuclear safety design criteria and

requirements contained in AFR 122-10 which must be applied to the missile with reentry vehicle, the facilities and support equipment which interface with the missile, as well as the means for controlling the missile. Specific analyses must be accomplished to demonstrate that the qualitative and quantitative requirements of AFR 122-10 have been met. These are explained in more detail in paragraph 4.12 of MIL-STD-1574A, and nuclear safety evaluation criteria are contained in Chapter 9 of AFR 122-10. These and the results of the various safety tests and analysis will be used by the NWSSG in determining whether or not the system meets the four DOD nuclear safety standards and can be certified for operational use.

5.9.5 Test operations safety. In accordance with paragraph 4.10 of MIL-STD-1574A, test planning documents and procedures shall incorporate the safety requirements and criteria identified by the MX Associate Contractor and SAIC system safety analyses. Requirements for both safety testing and safe test performance shall be identified. Where possible, safety testing shall be integrated with other test operations to achieve a cost-effective program.

5.9.5.1 Test/operating plans. Assurance of adequate safety consideration is provided by the respective System Safety Manager's approval authority over test plans. The Test Conductor, as designated by ED 77-3, is responsible for integrated system test activities, including performance or coordination of system safety functions. The SAIC shall prepare for MNBS an Operations Safety Plan for each government controlled test site. These plans shall be prepared and submitted in accordance with the CDRL to detail responsibilities and authorities of all participants in all aspects of safety at the test beds.

5.9.5.2 Test/operating procedure reviews. The safe performance of tests shall be assured by system safety review/approval of each test procedure, safety surveillance of each hazardous test operation, and individual/crew training and certifications. Each MX Associate Contractor's system safety organization shall review each test/operating procedure, for which they have responsible involvement, against the Hazard Control Requirements List (see 5.2.5.2) prepared for that test. Safety signature approval of each procedure shall be provided only when the procedure complies with established safety requirements or constraints and contains appropriate caution and warning notations. Each SSM is responsible for review/approval of test procedures for tests of equipment produced under that Associate Contractor's MX contract. The Test Conductor, as designated by ED 77-3, shall review/approve all integrated system test procedures. Procedures for potentially hazardous tests/operations at VAFB will also require approval by SAMTEC. Test procedures for use at KAFB will require approval by the AFWL Technical Safety Committee. Procedures for use at operational bases will be validated by the MX Associate Contractors and verified by the Using Command as part of the normal technical order approval process.

5.9.6 Training. Each MX Associate Contractor shall implement paragraph 5.5 of MIL-STD-1574A by providing safety training requirements as part of the overall training program for the MX Weapon System.

5.9.6.1 Training requirements. These safety training programs shall include instruction on hazard types, recognition, causes/effects, preventive and control measures, procedures, checklists, safeguards, safety devices, and protective equipment. The contractors' training program shall also include Government/Military personnel who will be involved in their activities. The SAIC shall review and provide input to the MX Integrated Logistics Plan to assure that safety concerns are identified, training programs are tailored for specific types and levels of personnel, and that all personnel receive equivalent training for similar operations. The SAIC shall also review flight operations training to assure that the range safety requirements of SAMTECM 127-1 are met.

5.9.6.2 Certification. All test, operations, and field support personnel shall be certified as having completed a training course in safety principles and methods. Certification shall encompass personnel technical knowledge, formal training courses, on-the-job training, verification of skills, and demonstration of individual and crew capabilities. Medical examinations shall be required in accordance with skill certification requirements.

5.9.7 Industrial safety. Each MX Associate Contractor SSM shall be responsible to assure that the System Safety Program supplements existing industrial safety activities in accordance with paragraph 4.6 of MIL-STD-1574A. This objective is achieved through the conduct of the Hazard Control Analysis defined in paragraph 5.4.

6. NOTES

6.1 Program milestones. The major program milestones for the Full Scale Engineering Development phase are listed below. The related system safety activities and general data requirements for each milestone are as noted. Formal submittal of data shall be in accordance with the applicable contracts data list.

a. Contract award – Each contractor SSPP and the AISP update, 30 days following. Initial Hazard Control Assessment Report (consisting of Annex A and B only), 90 days after.

b. Subsystem PDR – Applicable draft of Sections I and III and update Annex A and B of Hazard Control Assessment Report (HCAR), 30 days before.

c. Final hardware PDR – SAIC Preliminary Integrated System HCAR, 60 days after. SAIC Initial Nuclear Safety Analysis Report (NSAR), 90 days after.

d. Interim design reviews (IDR) – Update/complete applicable HCAR 30 days before.

e. Nuclear Weapon System Safety Group (NWSSG) initial study – Contractor presentations as required approximately eight months after final hardware PDR.

f. Subsystem CDR – Update applicable associate HCAR 30 days before.

g. Flight proof test design release – Update/complete element HCARs 60 days before and update/complete Integrated System HCAR 30 days before.

h. Hazardous operation – Update applicable HCAR 60 days before first hazardous operation and each subsequent hazardous operation following incorporation of a change.

i. Missile launch – Update complete element HCARs 60 days before and Integrated System HCAR 30 days before first missile launch and each subsequent launch following incorporation of a change.

j. Final hardware CDR – Each associate final HCAR, 60 days after. SAIC preoperational NSAR, 90 days after. SAIC Integrated System HCAR and Integrated System Fault Tree Analysis (ISFTA), 120 days after.

k. NWSSG preoperational study – Contractor presentations as required approximately six months prior to Initial Operational Capability (IOC).

6.2 Data item description (DID) references. Data items associated with this standard are not deliverable unless specified by the contract data requirements list (CDRL). The data normally associated with this standard include the following:

DID	Title	Reference Paragraph	Source Document Reference
DI-H-7047	Analysis Integration and Support Plan	4.2.2.1	MIL-STD-882A
DI-H-7047	System Safety Program Plan	4.2.2.2	MIL-STD-882A
DI-H-7050	Monthly Status Report	5.1.1.3	MIL-STD-882A
DI-H-7048	System Safety Group Minutes	5.1.3.1	DI-A-2166
DI-H-7048	Hazard Control Report	5.4	MIL-STD-882A
DI-H-7048	Integrated System Fault Tree Analysis	5.5.1	MIL-STD-882A
DI-H-7048	Cable Failure Matrix Analysis	5.5.2	MIL-STD-882A
DI-H-7048	Software Hazardous Effects Analysis	5.5.3	MIL-STD-882A
DI-H-7048	Test Safety Analysis	5.6	MIL-STD-882A
DI-R-3532	Nuclear Safety Analysis Report	5.7	MIL-STD-882A
DI-S-30565A	Hazard Control Assessment Report	5.8	MIL-STD-1574A
DI-L-3317A	Data Cards for Explosive Assemblies, Subassemblies, and Parts	5.9.3	MIL-STD-1574A
DI-L-3311B	Explosive Hazard Classification Data	5.9.3	DOD 4145.26-M
DI-M-3403	Explosive Ordnance Disposal Procedure	5.9.3	MIL-STD-1574A
DI-S-30562	Operations Safety Plan	5.9.5.1	SAMSOR 127-7

APPENDIX A

MX HAZARD CONTROL ANALYSIS

10. SCOPE

10.1 Purpose. This appendix provides the detailed instructions for the conduct of the MX Hazard Control Analysis and preparation of required documentation.

10.2 Application. Compliance with this appendix by MX Associate Contractors is mandatory for performance of the MX Hazard Control Analysis required by paragraph 5.4.

20. REFERENCED DOCUMENTS

Not applicable

30. DEFINITIONS

Not applicable

40. GENERAL REQUIREMENTS

40.1 Qualitative analysis. The MX Weapon System shall be subjected to continuous iterative qualitative Hazard Control Analysis as defined in this appendix. Each MX Associate Contractor shall implement this process on all systems, subsystems, software, equipment, and facilities for which they are responsible.

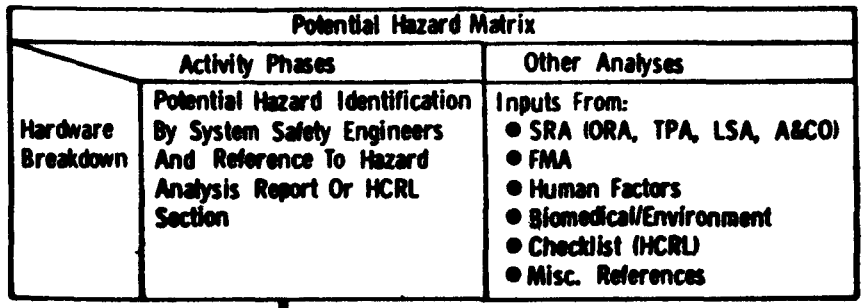
50. DETAILED REQUIREMENTS

50.1 Analysis method. A single qualitative analysis method shall be used for the MX HCA. An overview of the MX HCA method and the interrelationships of the elements of the analysis is provided in figure A-1. Each element is discussed separately in the following subparagraphs, but shall be combined into a single analysis process. Hazard Analysis Reports (see 50.1.2) shall be initiated for all system safety potential problems that require analysis or new hazard control requirements to resolve. Minor items that can be resolved by simple statements relative to existing hazard control requirements shall be documented on the HCRL (see 5.2.4.2) in lieu of initiating a Hazard Analysis Report.

50.1.1 Hazard identification. Potential hazard identification activities shall include the techniques of independent system safety engineering evaluation, other related analyses, and Hazard Control Requirements Lists (HCRL), as discussed below. Conditions identified by all techniques that are suspect of having accident risk are considered to be potential hazards and are documented on the Potential Hazard Matrix, illustrated in figure A-2, and analyzed on Hazard Analysis Report sheets as discussed in 50.1.2. The Potential Hazard Matrix (PHM) is a tool to

Aid To Systematic Analysis

- Guides Logical Assessment
- Used By Analysts And Reviewers
- Cross References Each Hazard To The Resolution
- Sectionalized By System Codes
- Legible Working Papers Deliverable With Hazard Analysis Reports

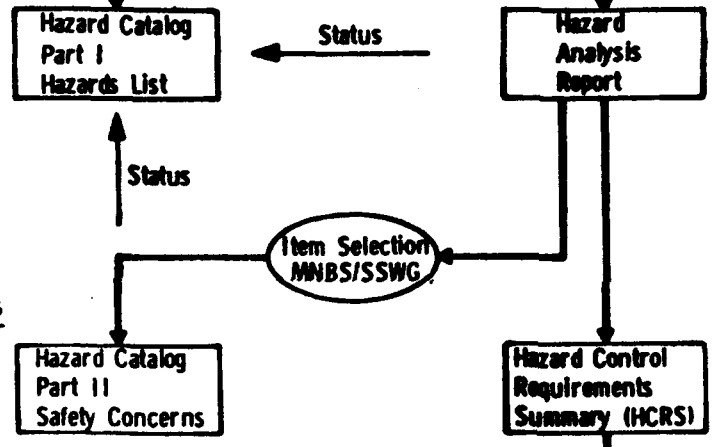


Computerized Status Reports

- Maintained On CSAR
- Sectionalized By System Codes
- Computer Sorts Such As:
  - Open/Closed
  - Classification
  - Eliminated/Accepted
  - Etc.
- Deliverable As Part Of Annex A Of Hazard Control Assessment Report

Primary Qualitative Analysis

- Use Only When Analysis Is Required For Resolution
- All Analysis Detail
  - Assumptions
  - Calculations
  - Rationale
- Defines Hazard Control Requirements
- Specific Reports For Informal Data Exchange
- Legible Working Papers Deliverable As Completed/Revised

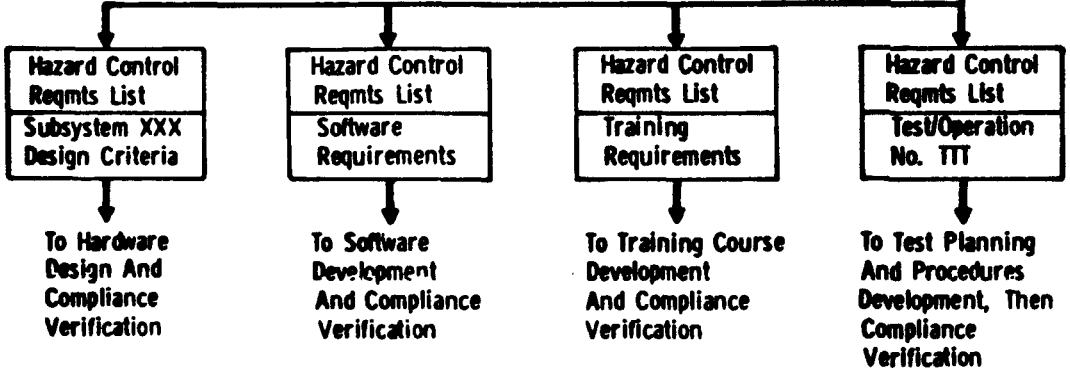


Significant Accident Risk Factor Reports

- One Page Summary Of H.A. Report
- Acceptance Signatures
- Deliverable In Annex A Of Hazard Control Assessment Report

Computerized Analysis Results

- Maintained On CSAR
- Sectionalized To Elements By Data Sets
- All Control Reqmts Referenced To Source
- Activity Phase/Test Reference



Hazard Control Requirements Lists

- Same Data As Summary
- Various Computer Sorts

Resolution & Verification

- Coordinated Resolutions
- Verification By Reference Column Entry

Figure A-1. Hazard control analysis elements.

MISSILE X WEAPON SYSTEM
POTENTIAL HAZARD MATRIX

Program Phase:
System:

Date:
Page:

Subsystem/Component \ Activity Phase	Fabrication	Handling And Transportation	Subsystem Tests	Weapon System Assembly	Integrated System Tests	Maintain Readiness	Missile Launch	Missile Flight	Maintenance	Emergency	Other Analyses: System Requirements Analysis	Other Analyses: Failure Mode Analysis	Other Analyses: Human Factors	Other Analyses: Biomedical Environment	Other Analyses: Hazard Cont. Requirements List (HCRL)	Other Analyses: Misc. References

Figure A-2. Potential hazard matrix.

record each identified potential hazard with references to both the source of identification and to the qualitative analysis item that addresses that potential hazard or the HCRL section that makes analysis unnecessary. The purpose of the PHM is to serve as a guide for a systematic and complete potential accident risk identification. The PHM is structured to provide a hardware/software breakdown applied against an activity phase breakdown and related analyses.

50.1.1.1 Hardware/software breakdown. To facilitate integration of the HCA the hardware/software breakdown shall generally follow the MX Standard Work Breakdown Structure (WBS) with software elements included as part of the associated hardware element. A two alphanumeric character coding system shall be used to identify the section and subsections of the PHM, Hazard Analysis Reports, HCRL, and Hazard Catalog sheets in a hardware system/subsystem order. The first character of the coding is used to indicate a major MX system element or Associate Contractor responsibility. The second character is used to identify subsystems, end items, or grouping of equipment for logical analysis and reporting. The first coding characters shall be controlled and assigned by the SAIC. The second coding character shall be assigned by the MX Associate Contractor responsible for the first character area except that the following standard characters shall be used by all contractors:

a. XA - Element complete as an assembly

b. XN - Operational Support Equipment (OSE) (WBS XX80)

c. XM - Maintenance Support Equipment (MSE) (WBS XX41A and XX44A)

d. XP - Depot Support Equipment (DSE) (WBS XX40)

e. XR - Training Equipment (WBS XX21)

f. XS - Special Test Equiment (STE)/Test Support Equipment (TSE) (WBS XX50 and XX80)

g. XT - Test Facilities (WBS XX57)

Lower indenture hardware breakdown, to component level when required, is accomplished on the system PHMs in a manner established by the respective SSM. To illustrate the identification of a potential hazard, XM.001 would indicate the first potential hazard identified associated with the MSE for a specific MX element.

50.1.1.2 Activity phase definitions. The activity phase structure shown in figure A-2, which is derived from the SRA Functional Flows, shall be used by all MX Associate Contractors. Each hardware/software element will be considered in each activity phase to identify inherent accident risks and/or undesired events associated with the specific hardware during one or more phases of activity. The activity phase definitions are as follows:

a. Fabrication	Includes all functions necessary to produce system components. Normally these operations are performed in a contractor facility.
b. Handling and Transportation	Includes any movement or rotation of system components or assemblies after completion of fabrication.
c. Subsystem Tests	All tests performed on AVE, SE, or RPIE components or assemblies up to and including Configuration Items. Acceptance tests and all subsequent tests, such as retest after repair, are included.
d. Weapon System Assembly	Includes all functions necessary for physical buildup or disassembly of an operational weapon or flight test assembly, such as mating/demating missile stages; missile canister, R/S, launcher assembly and disassembly; establishing OGE, SE, RPIE and facility interfaces with AVE.
e. Integrated System Tests	All test or checkout activities that involve two or more CIs. Includes interface verification and functional tests.
f. Maintain Readiness	Includes all normal activities between completion of Integrated System Test and Missile Launch, such as monitor and display status, maintain habitable environment for launch crew, target the missile, and control system operation.
g. Missile Launch	Includes all functions from initiation of launch sequence to missile first motion, such as transfer from ground power to airborne power, move missile to launch position, verify launch readiness, and ignition of canister gas generator.
h. Missile Flight	Includes all functions from missile first motion to detonation of the weapon for operational flights or provision of data for test flights. Functions include missile ejection from canister; stage ignition, guidance, and separation sequence; deploy and detonate RVs, and transmit data to ground. Destruct of a malfunctioning test missile is excluded.
i. Maintenance	Includes all scheduled and unscheduled maintenance and repair activities, such as on-site maintenance, strategic missile support base and/or primary support facility maintenance, technical repair center activities, and test facility refurbishment.
j. Emergency	Includes all credible contingency or emergency conditions, such as Toxic gases/fluid release, inadvertently armed ordnance, electric power loss, and destruct of missile on test flight.

50.1.1.3 System safety engineering evaluation. The independent system safety engineering evaluation consists of an examination of each MX system/subsystem in each activity phase. As a minimum, the Hazard Identification Checklist presented in Table A-I shall be used by MX Associate Contractors as a standardized guide for identification of potential hazards. The evaluation shall be an iterative process continuing through and includes contingency situations. Potential hazards identified by the system safety engineering evaluation shall be incorporated in the Potential Hazard Matrix.

50.1.1.4 Related Analyses. MX Associate Contractor potential hazard identification activities shall not duplicate other MX program analyses, but shall utilize and incorporate safety related data produced by them. The MX Associate Contractors' system safety organization shall review and evaluate these related analyses and incorporate identified potential hazards in the Potential Hazard Matrix by reference in the appropriate Other Analyses and Activity Phase columns.

The following MX program analyses shall be assessed for HCA input:

a. System requirements analysis (SRA) - Interrelationships with system safety are discussed in 5.3;

b. Failure mode analysis (FMA) - Identifies hardware failures and failure rates as inputs to the HCA and Fault Tree Analyses. The FMA requirements defined in SAMSO STD 77-6, Appendix A, Section 50.6 include "an analysis of each component part failure in all applicable modes including flight" and "current failure rates for each part failure." Parts are identified to the "bit and piece" level, including parts of printed circuit cards, electrical connectors, mechanical devices, etc. The MX Associate Contractor System Safety Manager has approval authority over the FMA, as shown in 5.1.2. That approval shall be contingent upon the FMA providing all the data required by SAMSO STD 77-6 and the numerical data to support the ISFTA of Appendix B of this standard;

c. Human factors – Provides identification of potential hazards by the critical task analyses and the identification of deficiencies with safety impact by the human factors test and evaluation performed in accordance with SAMSO-STD-77-1.

d. Biochemical/environment - Provides identification of potential hazards caused by dangerous substances and environmental conditions.

e. Hazard control requirements list - Incorporates potential accident risk factors identified through the HCRL activity discussed in paragraph 5.2.5.2.

f. Miscellaneous references – Provides for identification of potential hazards by other studies or analyses and incorporation of lessons learned from the findings of accident/incident investigations.

Table A-1. Hazard identification checklist.

Item	Hazard	Abbreviation	Definition	Potential Accident/Effect
1.	Acceleration/ Shock	Accel.	Change in velocity, impact energy of vehicles, components or fluids.	1. Structural deformation. 2. Breakage by impact. 3. Displacement of parts or piping. 4. Seating or unseating valves or electrical contacts. 5. Loss of fluid pressure head (cavitation). 6. Pressure surges in fluid systems. 7. Detonation of shock sensitive explosives. 8. Disruption of metering equipment.
2.	Chemical Energy	Chem.	Chemical disassociation or replacement of fuels, oxidizers, explosives, organic materials or compounds.	1. Fire. 2. Explosion. 3. Nonexplosive exothermic reaction. 4. Material degradation. 5. Toxic gas production. 6. Corrosion fraction production. 7. Swelling of organic materials.
3.	Contamination	Contam.	Producing or introducing contaminants to surfaces, orifices, filters, etc.	1. Clogging or blocking of components. 2. Friction between moving surfaces. 3. Deterioration of fluids. 4. Degradation of performance sensors or operating components. 5. Erosion of lines or components. 6. Fracture of lines or components by fast moving large particles. 7. Electrical insulation breakdown.

Table A-1. Hazard identification checklist. (Continued)

Item	Hazard	Abbreviation	Definition	Potential Accident/Effect
4.	Electrical Energy	Elec.	System or component potential energy release or failure. Includes shock, thermal, and static.	1. Electrocution. 2. Involuntary personnel reaction. 3. Personnel burns. 4. Ignition of combustibles. 5. Equipment burnout. 6. Inadvertent activation of equipment or ordnance devices. 7. Necessary equipment unavailable for functions or caution and warning. 8. Release of holding devices. 9. Interruption of communications.
5.	Human Capability	H. Cap.	Human factors including perception, dexterity, life support, and error probability.	1. Personnel injury due to: a. Restricted egress/evacuation routes. b. Hazardous location of equipment/controls. c. Inadequate visual/audible warnings. 2. Equipment damage by improper operation due to: a. Inaccessible control location. b. Inadequate control/display identification. c. Inadequate data for decision making.
6.	Human Hazards	H. Haz.	Conditions that could cause skin abrasions, cuts, bruises, falls, etc.	1. Personnel injury due to: a. Sharp edges/corners. b. Dangerous heights. c. Unguarded floor/wall openings. d. Limited work area.

Table A-1. Hazard identification checklist. (Continued)

Item	Hazard	Abbreviation	Definition	Potential Accident/Effect
7.	Interface/ Interaction	Inter.	Compatibility between systems/subsystems/GSE/ facilities/software.	1. Incompatible materials reaction. 2. Interfacing systems/component reactions. 3. Unintended operations caused/prevented by software.
8.	Kinetic Energy	Kinetic	System/component linear or rotary motion.	1. Linear impact. 2. Disintegration of rotating components.
9.	Material Deformation	Mat'l	Degradation of material by corrosion, aging, embrittlement, oxidation, etc.	1. Change in physical or chemical properties. 2. Structural failure. 3. Delamination of layered material. 4. Electrical short circuiting.
10.	Mechanical Energy	Mech.	System/component potential energy such as compressed springs.	1. Personnel injury or equipment from energy release.
11.	Natural Environment	Nat. Env.	Conditions including lightning, wind, projectiles, thermal, pressure, gravity, humidity, etc.	1. Structural damage from wind. 2. Electrical discharge. 3. Meteorite penetrations. 4. Structural damage from space vacuum. 5. Dimension changes from solar heating.
12.	Pressure	Press.	System/component potential energy including high, low or changing pressure.	1. Blast/fragmentation from container overpressure rupture. 2. Line/hose whipping. 3. Container implosion. 4. System leaks. 5. Heating/cooling by rapid changes. 6. Aeroembolism, bends, choking, or shock.

Table A-1. Hazard identification checklist. (Continued)

Item	Hazard	Abbreviation	Definition	Potential Accident/Effect
13.	Radiation	Rad.	Conditions including electromagnetic, ionizing, thermal or ultraviolet radiation.	1. Initiation of ordnance devices. 2. Electronic equipment interference. 3. Human tissue damage. 4. Charring of organic materials. 5. Decomposition of chlorinated hydrocarbons into toxic gases. 6. Ozone or nitrogen oxide generation.
14.	Thermal	Therm.	System/component potential energy, including high, low or changing temperature.	1. Ignition of combustibles. 2. Initiation of other reactions. 3. Distortion of parts. 4. Expansion/contraction of solids or fluids. 5. Liquid compound stratification. 6. Personnel injury.
15.	Toxicants	Toxic	Adverse human effects of inhalants or ingesta.	1. Respiratory system damage. 2. Blood system damage. 3. Body organ damage. 4. Skin irritation or damage. 5. Nervous system effects.
16.	Vibration/ Sound	Vibra.	System/component produced energy.	1. Material failure. 2. Personnel fatigue or injury. 3. Pressure/shock wave effects. 4. Loosening of parts. 5. Chattering of valves or contacts. 6. Communication interference. 7. Impairment or failure of displays.

50.1.2 Hazard analysis report. The MX Weapon System accident risk of each potential hazard identified on the Potential Hazard Matrix shall be evaluated using the Hazard Analysis Report format of figure A-3. MX Associate Contractors shall use this hazard analysis format to ensure compatibility and proper incorporation into the Integrated Hazard Control Analysis by the SAIC. The complete analysis shall include a description of how the hazard can propagate into an accident, the potential effects, and the assumptions and rationale used to develop hazard controls. All design and/or operational requirements necessary to eliminate or control the hazard shall be defined and referenced to the appropriate HCRL.

Individual Hazard Analysis Reports shall be initiated by the MX Associate Contractors' system safety organization by preliminary entries that are refined and completed as the analysis progresses. The Assumptions/Rationale space shall contain all pertinent facts or assumptions used as the basis of analysis, reference data, calculations, or other analyses. This space also provides the flexibility to incorporate or reference specialized analysis methods such as stress analysis, sneak circuit, or electrical loads analysis.

Following initiation by system safety, the responsible engineering activity shall review applicable analyses and provide additional technical input. The elimination/control of potential hazards shall be resolved jointly between the responsible engineering activity and system safety. Those safety requirements conflicting with other program considerations shall be resolved by conducting a trade study discussed in 5.3.4. The disposition and resulting hazard category shall then be included in the Hazard Analysis Report. Negotiated hazard control requirements, expressed in normal criteria/requirement terms, shall be listed in the following groups:

a. A. Hardware design

b. B. Software design

c. C. Training

d. D. Test operations procedures

e. E. Personnel protective equipment.

f. F. Maintenance procedures

g. G. Transportation

Only the applicable group(s) need to be listed on the report, but the identification including the letter prefix shall always be as shown above. If existing HCRL items provide the required hazard control, simply list the specific HCRL item numbers. Each requirement shall be referenced to and included in the appropriate HCRL section. The analysis report may then be closed in accordance with the requirements of 5.2.3.

MISSILE X WEAPON SYSTEM
HAZARD ANALYSIS REPORT

Hazard Level:	Status:	No.
Hazard Group:		Page: Of
Program Phase:		Date:

System: Subsystem:

Activity Phase:

___ 1. Fabrication	___ 5. Integrated System Tests	___ 8. Missile Flight
___ 2. Handling & Transportation	___ 6. Maintain Readiness	___ 9. Maintenance
___ 3. Subsystem Tests	___ 7. Missile Launch	___ 0. Emergency
___ 4. Weapon System Assy		

Hazard Description:

Potential Effects:

Assumptions/Rationale:

Hazard Control Requirements:	Reference

Disposition:

Originator/Location:

Figure A-3. Hazard analysis report format.

50.1.3 Hazard catalog. The hazard analysis reports shall be integrated by each MX Associate Contractor into a Hazard Catalog according to the formats in figures A-4 and A-5. Part I of the Hazard Catalog shall contain a list of all accident risks analyzed and the following status information:

a. Hazard classification in accordance with 5.2.1.

b. Identification of "Safety Concerns" by an entry of "SSM" for candidates and "MNBS" for approved designations.

c. Identification of interface concerns with other contractors as determined by the originating SSM.

d. Indication of elimination of hazard (by design) by an X in the "ELIM" column.

e. Status of acceptance in accordance with 5.2.3 by date entries.

f. Dates item was initiated, closed, and resolution needed.

Each MX Associate Contractor shall establish and maintain Part I of the Hazard Catalog on the remote CSAR terminals. The computerized data shall be updated 10 days prior to each System Safety Group or Technical Interchange meeting or Hazard Control Assessment Report submittal, as a minimum.

Part II of the Hazard Catalog shall consist of a one page summary of each hazard that has been designated as a "Safety Concern", as defined in 5.2.2. The summary shall include a description of the hazard and its potential effects, the recommended corrective action, the rationale for descending the order of precedence (see 5.2.4), and the disposition, including signatures of approval.

50.2 Analysis reporting. Formal submittal of the various HCA elements shall be in accordance with the CDRLs. The Hazard Control Analysis Reports shall be submitted as legible working papers periodically and shall include the following:

a. System description data consisting of the minimum text, figures and diagrams required to substantiate/explain item c. below.

b. Potential hazard matrixes initiated or revised during the period.

c. Hazard Analysis Reports initiated or revised during the period.

Selected Hazard Analysis Reports and supporting data shall be, upon request by MNBS, presented at meetings of the MX System Safety Group or any of its subgroups, or transmitted informally to SAMSO or other MX Associate Contractors.

The Hazard Catalog, Part I and Part II, shall be submitted as Annex A to the Hazard Control Assessment Report (see 5.8 and Appendix E).

MISSILE X WEAPON SYSTEM
HAZARD CATALOG
PART I - HAZARD LIST

ANALYSIS ITEM NUMBER	HAZARD DESCRIPTION	CLASSIFICATION		INTER-FACE CONCERN	ELIM	ACCEPTED			ACTION STATUS		
		HAZARD LEVEL	SAFETY CONCERN			CONTRACTOR SSM	MGR	SPO	OPENED	NCED	CLOSED

Figure A-4. Hazard catalog part I - Hazards list.

MISSILE X WEAPON SYSTEM HAZARD CATALOG
PART I - SAFETY CONCERNS

SYSTEM: _____ ITEM NO. _____

SUBSYSTEM: _____ HAZARD LEVEL _____

COMPONENT: _____ DATE _____

HAZARD DESCRIPTION:

RECOMMENDATION:

RATIONALE:

DISPOSITION:

ACCEPTED:

MX SYSTEM SAFETY MANAGER	CONTRACTOR	DATE
MX PROJECT DIRECTOR	CONTRACTOR	DATE
SYSTEM PROGRAM OFFICE	SAMSO/_____	DATE

Figure A-5. Hazard catalog part II - Safety concern.

APPENDIX B

MX INTEGRATED SYSTEM FAULT TREE ANALYSIS (ISFTA)

10. SCOPE

10.1 Purpose. This appendix defines the analysis technique that will be used by the SAIC, with support by the MX Associate Contractors to determine the probability of occurrence for, as a minimum, the following nuclear safety undesired events.

a. Inadvertent Nuclear Detonation

b. Inadvertent Weapon Enabling

c. Accidental Motor Ignition

d. Inadvertent Programmed Launch

e. Faulty Launch

f. Inadvertent Transmission of Intent Command

10.2 Application. The ISFTA methodology described by this appendix will be accomplished by the MX SAIC. However, the MX Associate Contractors will be required to provide design and operations data and selected Fault Trees as directed by SAMSO.

The MX ISFTA consists of two major parts; development of the Fault Trees, and calculation of the numerical probabilities. The Fault Trees will be developed by the SAIC with support of the MX Associate Contractors and reviewed with SAMSO. The probability of failure of systems, subsystems, and components will be acquired from the Integrated Failure Mode Analysis.

20. REFERENCE DOCUMENTS

Not Applicable.

30. DEFINITIONS

30.1 Component failure. The state of a component whereby it ceases to accomplish the function it was designed for either completely or intermittently.

30.2 Primary component failure. The failure of a component is called "primary" if it occurs while the component is functioning within the operating parameters for which it was designed.

30.3 Secondary component failure. A failure occurring when the component is subjected to abnormal environmental stresses, such as failures in related equipment.

30.4 Commanded failures. Undesired events resulting from proper component operation at the wrong time or place are called "commanded failures." These failures are the linking events between the various levels of the fault tree from primary failure events to the ultimate undesired event. It is primarily through these linking events that the fault tree analysis is elaborated.

40. GENERAL REQUIREMENTS

40.1 Fault tree development. The development of a particular fault tree is accomplished in an orderly manner and commences with definition and/or identification of an undesired event or potential accident. Once this has been accomplished, the system is analyzed and all logical combinations of functional failures which can cause the undesired event or potential accident are determined. Such analysis is entirely dependent upon a thorough knowledge of the system functions and equipment. Each of these contributing failures is further analyzed to determine the logical relationships of system failures which may cause them. In this manner, a diagram of logical relationships among failures is developed. The development is continued until all "input" failures on the fault tree are defined in terms of basic, identifiable failures which may be quantified for evaluation.

50. DETAILED REQUIREMENTS

50.1 Fault tree data requirements. Availability of proper and complete source materials is basic to the success of the entire hazard analysis. Detailed logic and schematic diagrams are required for preliminary analysis and failure analysis. Physical layout plans and operating and maintenance instructions are needed to estimate the length of time a single fault may remain in the equipment before it is discovered and corrected. In an operational system, it is also important for the safety analyst to obtain all engineering change proposals and trouble reports so that the study can be kept current and responsive to system needs.

The following specific data will be required by the SAIC in performance of the MX ISFTA:

a. End item specifications
b. System block diagrams
c. Design drawings
d. All engineering change proposals
e. Preliminary design review data
f. Critical design review data
g. Operating handbooks/procedures
h. Maintenance handbooks/procedures.

The data identified above will be provided as GFP to the SAIC to support the ISFTA.

50.2 Fault tree construction. The process by which a qualitative logic diagram is constructed for the system shall be as follows:

a. The system operating modes shall be divided into the Activity Phases identified for the Hazard Control Analysis. A phase is that increment of a system's life cycle which can be analyzed independently, yet recognizing that there can be commonality of analysis for any of the phases. A fault tree branch shall be constructed separately for each phase. The fault tree development process for each phase should be logical and systematic.

b. Assuming the basic functional relationships are defined and understood, the development of the fault tree can proceed from the defined top level event down through the various event levels to the component failures and combinations of failures that can cause the top level undesired event.

c. The questions of "primary failure", "secondary failure", and "command failure" are guidelines to be used for development of component failure modes. At the component level of the fault tree, the following steps should be followed:

(1) Describe the component event to be developed utilizing part and/or component numbers.

(2) List all primary faults.

(3) List all secondary faults for those equipments which are environment-sensitive, i.e., those conditions which can "cause" each primary fault mode.

(4) Define the input or command events which are a normal function at the wrong time or caused by a fault.

(5) Repeat steps (2) and (3) for the events described by (4).

(6) Continue this process to the level of detail required.

d. When the Fault Tree Logic diagram is completed, it shall be reviewed against the hardware design to assure the correct part or component number are entered on each event.

50.3 Graphic symbology. The following graphic symbology shall be used in preparing a fault tree.

Events. The various kinds of events used in fault trees are represented by the following symbols:

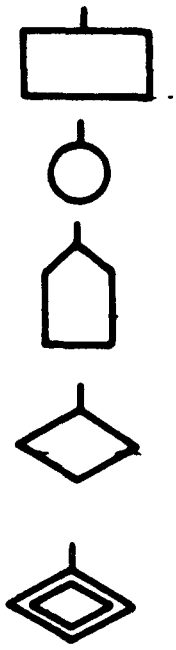
(1) The RECTANGLE identifies an event in a Fault Path that results from a combination of fault events.

(2) The CIRCLE identifies a primary failure of a device.

(3) The HOUSE indicates an event or state which is normal for the system.

(4) The DIAMOND identifies a secondary failure, or a set of failures which do not require further development. Failure Rate Data is known sufficiently at this level of the Fault Tree Branch.

(5) The DOUBLE DIAMOND terminates a branch which has not been fully developed due to lack of information.



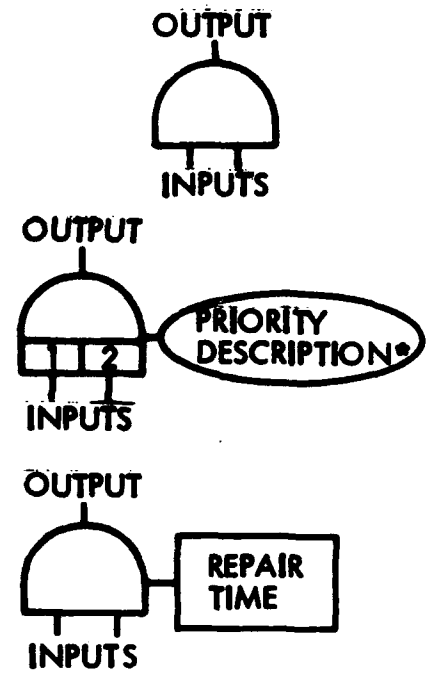
AND gates. The AND gate logic operators required to develop the fault trees are defined and symbolized as follows:

(1) The AND gate describes the logical operation which requires the coexistence of all inputs to cause the output.

(2) The PRIORITY AND gate performs the same function as the AND gate except that the inputs must occur in the sequence stipulated.

*Priority description is required only when necessary to clarify relationship between inputs.

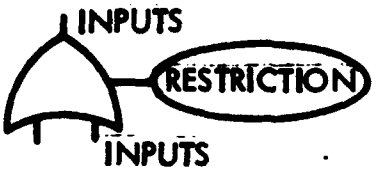
(3) The CONSTANT REPAIR AND gate performs the same function as the AND gate except that the repair time of the output event is not dependent on the repair times of the inputs, but is as stipulated.



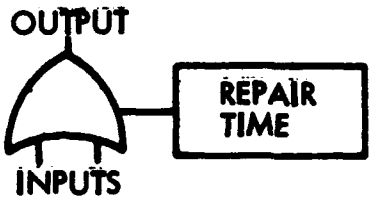
OR gates. The OR gate logic operators required develop the fault trees are defined and symbolized as follows.

(1) The OR gate describes the logical operation whereby the output is caused by the occurrence of any of the inputs.

(2) The EXCLUSIVE OR gate performs the same function as the OR gate except that specified inputs cannot coexist.

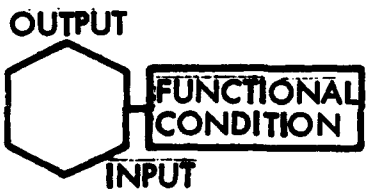


(3) The CONSTANT REPAIR OR gate performs the same function as the OR gate except that the repair time of the output event is not dependent on the repair times of the input, but is as stipulated.

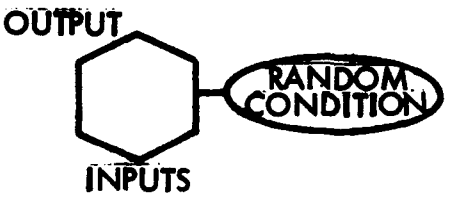


Special symbols. Special symbols are used in order to simplify the graphic representation of fault tree construction. These special symbols are shown below:

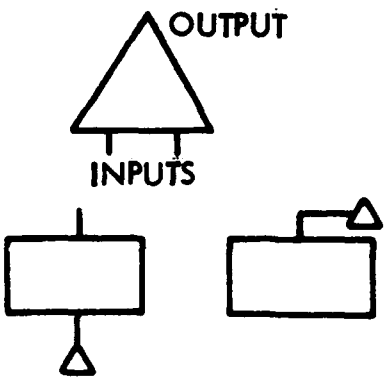
(1) The INHIBIT gate describes a situation in which a certain condition of the system must exist before one failure produces another. The inhibit condition may be either normal to the system or be the result of equipment failures.



(2) The MATRIX gate is used to describe a situation in which an output event is produced for certain combinations of events at the inputs. A matrix showing the event combinations that produce the output event will accompany each usage of this symbol.



(3) The TRANSFER symbol is used to show continuity between two parts of the tree. A line into the side of the triangle transfers every thing below to another area identified by the triangle with a line drawn from the apex.



50.4 Calculation of numerical probabilities. The failure rate data for the components identified in the fault tree comes from the MX Failure Mode Analysis Data. This data will be stored in the computer by component number and merged directly to the fault tree by the computer. Merging of the MX probability data onto the fault trees makes the fault tree classified data. The SAIC shall perform the calculations of the probabilities, make the final fault tree plots with failure rate data included, and deliver to SAMSO in accordance with the CDRL.

APPENDIX C

MX CABLE FAILURE MATRIX ANALYSIS

10. SCOPE

10.1 Purpose. This appendix provides instructions for the conduct of the MX Cable Failure Matrix Analysis (CFMA) that is a shorthand method used to concisely represent many of the possible combinations of failures which can occur within the cable assembly.

10.2 Application. Compliance with this appendix by MX Associate Contractors is mandatory for performance of the CFMA required by 5.5.2.

20. REFERENCED DOCUMENTS

Not Applicable.

30. DEFINITIONS

Not Applicable.

40. GENERAL REQUIREMENTS

40.1 Analysis requirements. The MX CFMA shall be conducted by each MX Associate Contractor that produces cable assemblies. The MX CFMA shall provide data in a timely manner to support the MX Failure Mode Analysis (FMA) and the Nuclear Safety Analysis Report (NSAR). The MX FMA function shall be responsible for all failure rate data associated with failures identified by CMFA.

40.2 Analysis elements. The CFMA prepared by each MX Associate Contractor shall consist of the following:

a. An index to provide a cross reference of cable numbers and connectors.

b. Cable diagrams to represent the physical configuration of each cable assembly.

c. Connector matrix and pin location drawing for each different connector.

d. Cable wire table for each cable.

50. DETAILED REQUIREMENTS

50.1 Index development. A CFMA Index shall be developed by each MX Associate Contractor required to perform a CFMA. The index shall identify each cable assembly produced by the MX Associate Contractor and include the following data:

a. Common use identification number

b. Nomenclature

c. Part number

d. Each connector including cable assembly number, manufacturer's part number, and connector matrix number in the CFMA report.

The index shall provide necessary cross references to permit use of only one connector matrix for each different manufacturer's part number connector. The index shall be in the format shown in the example of figure C-1.

Cable No.	Nomenclature	Assembly Number	Connector Number	Connector P/N	Connector Matrix No.
W103	xxxxxxxxxxxx	xxxx	1	xxx	xx
			2	xxxx	xx
			3	xxxx	xx
			4	xxxx	xx
			5	xxxx	xx
W107	xxxxxxxxxxxx	xxxx	1	xxx	xx
			2	xxx	xx

FIGURE C-1. CFMA index format.

50.2 Cable diagrams. A diagram of each cable assembly shall be provided in a format similar to that shown in figure C-2. The diagram shall identify the cable sections, connectors, equipment/cable connector interfaces, and the physical location (missile compartment, facility room, etc.) of installed connectors.

50.3 Connector matrices. A connector matrix shall be developed for each different connector provided by the MX Associate Contractor. The following ground rules shall be used in the development of a connector matrix:

a. Each connector matrix shall include a drawing to identify pin locations in the connector, a table showing the gauge of each pin, and a matrix diagram to identify all credible failure modes of connector pins.

b. Nonconductive connector cases shall be noted on the matrix sheet.

c. Failure mode identification shall consist of only credible (geometrically possible) faults that can occur from bent pins.

d. The CFMA Index (see 50.1) shall be used to preclude constructing connector matrices more than once for a particular connector.

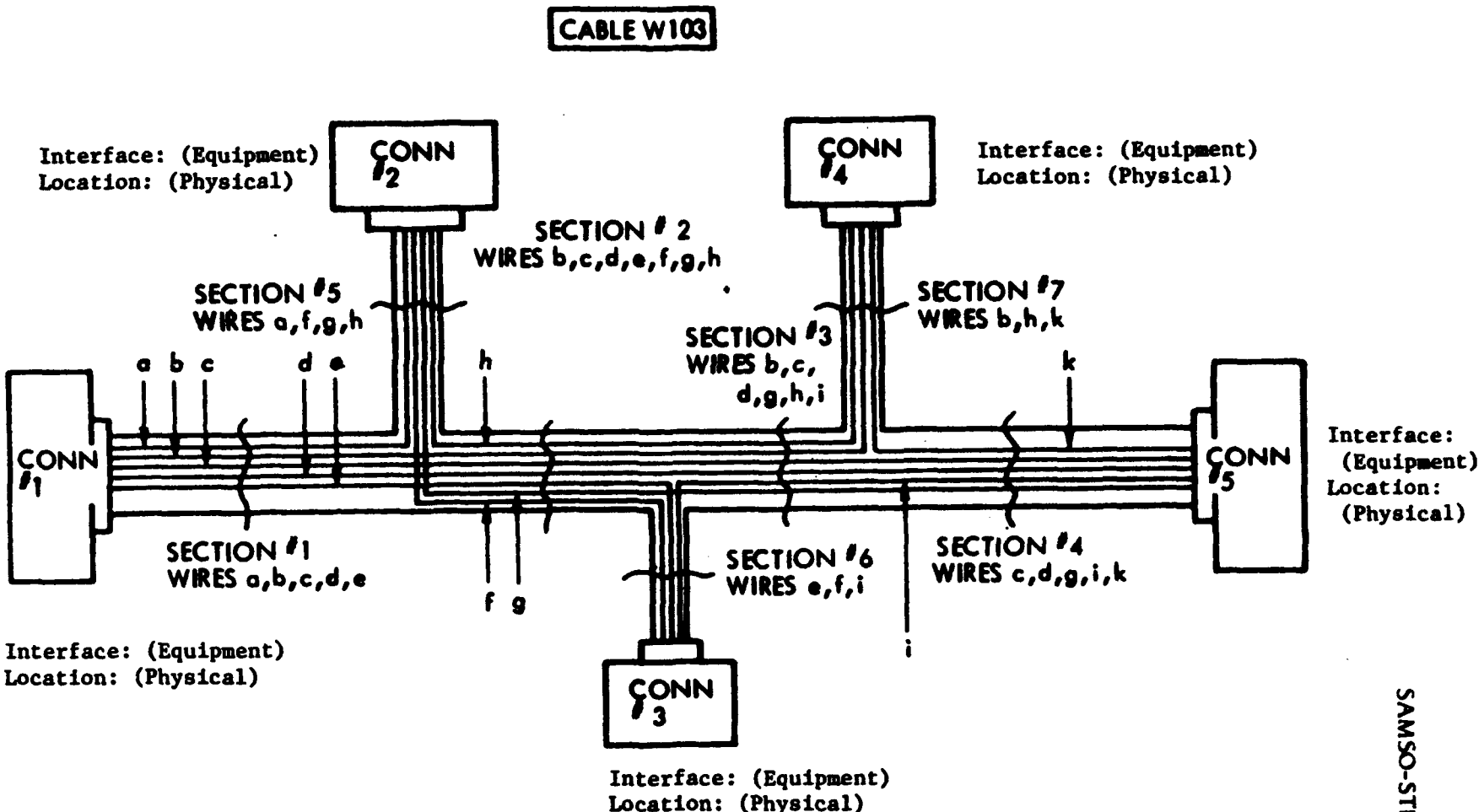
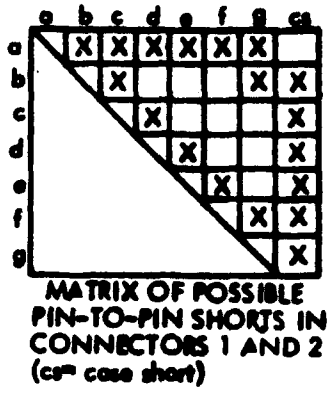


Figure C-2. Multiconnector cable diagram.

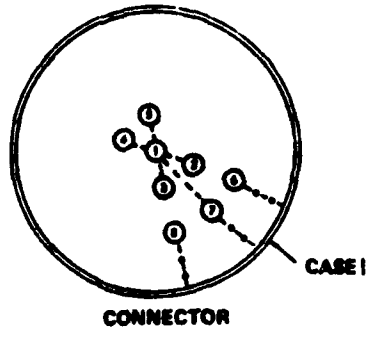
CABLE W107



PINS vs GAUGE

# PINS	AWG#
a	22
b	22
c	22
d	22
e	22
f	22
g	22

FIGURE C-3. Cable failure matrix.



— — — 1. PIN 1 HAS IMMEDIATELY ADJACENT INNER PINS 2,3,4,5 AND ADJACENT OUTER PIN 7.

– o— o — 2. PINS 6,7 AND 8 CAN SHORT TO THE CASE

FIGURE C-4. Connector pin short potentials.

Each connector matrix shall be prepared in a format similar to the example shown in figure C-3.

50.3.1 Connector failure modes. There are two major failure modes which can occur within a connector:

a. Pin-to-pin shorts between two pins, caused by the bending of pins. The pin length, size and pin spacing must be considered in the determination of credible pin-to-pin shorts caused by bent pins. Pin-to-pin shorts from bent pins are considered only if a pin can directly bend to immediately adjacent pins or between adjacent pins to outer pins (see figure C-4).

b. Pin-to-case shorts, which can be caused by a bent pin. The same considerations discussed in a. apply for credible conditions of pin-to-case shorts. This failure mode shall be designated "CS" on the matrix diagram.

Connector pins size 8 gauge or larger shall not be considered capable of bending over to contact another pin; but the other pins, if less than size 8 gauge, shall be considered to be capable of bending over to the larger gauge pin. Connector matrices need not be developed for pin-to-pin shorts caused by foreign material.

50.4 Cable wire tables. A cable wire table shall be developed for each cable assembly in the format used in the example of figure C-5. Each wire in the cable assembly shall be identified and recorded with the following information. A brief description of the function of the wire, e.g., issue ordnance ignition disc te, shall be entered in the function column. The identification, if any, of the function shall be entered in the Signal Identification column, and the worst case voltage/current levels of the wire shall be recorded in the voltage/current column. The latest interface control drawings shall be used to identify the voltages/currents on the cable wire table. The pin and connector assignments of both ends of the wire shall be placed in the From and To columns and the routing in a cable will be shown for branched cables. The wire type, size and shielding shall be noted in the last column.

50.4.1 Cable failure modes. There are three major modes in which a failure can occur within a wire bundle. These failure modes are:

a. Wire-to-wire shorts

b. Wire-to-shield shorts

c. Open wire faults.

The cable failure modes, effects, and failure rates shall be determined by the MX FMA function from CFMA and reliability data.

50.5 Analysis reporting. Formal submittal of the CFMA shall be in accordance with the CDRLs. The MX CFMA Report shall include the following:

WIRE TABLE CABLE W 103								
WIRE	FUNCTION	SIGNAL IDENT	VOLT./ CURRENT *	FROM	TO	ROUTING SECTION	TYPE & SIZE	SHIELD CONFIG
a	ISSUE ORDNANCE IGNITION DISCRETE	PO2		CONN 1 PIN c	CONN 2 PIN h	1,5	▷ 22 GA	SSC
b	MONITOR CONFIDENCE LOOP			CONN 1 PIN d	CONN 4 PIN h	1,2,3,7	▷ 22 GA	SC
c	ARM A&D DEVICE DISCRETE	PO1		CONN 1 PIN e	CONN 5 PIN c	1,2,3,4	▷ 22 GA	SC
d	A&D DEVICE ARMED MONITOR			CONN 1 PIN b	CONN 5 PIN g	1,2,3,4	▷ 20 GA	SSC
e	MONITOR-SAFETY LOOP			CONN 1 PIN a	CONN 3 PIN f	1,2,6	▷ 16 GA	TS2
f	MONITOR-CONFIDENCE LOOP			CONN 2 PIN f	CONN 3 PIN i	5,2,6	▷ 22 GA	SC
g	ORDNANCE IGNITION POWER APPLIED	ZO1	± 28vdc / 10ma	CONN 2 PIN a	CONN 5 PIN i	5,2,3,4	▷ 16 GA	SS
h	MONITOR-CONFIDENCE LOOP			CONN 2 PIN g	CONN 4 PIN k	5,2,3,7	▷ 22 GA	SSC
i	MONITOR-SAFETY LOOP			CONN 3 PIN e	CONN 5 PIN d	6,3,4	▷ 22 GA	TS2
k	SPARE			CONN 4 PIN b	CONN 5 PIN k	7,4	▷ 22 GA	SC

* WORST CASE

▷ MIL-W-XXXX WIRE

FIGURE C-5. Cable wire table.

a. An introduction, consisting of a narrative description of the purpose and scope of the analysis and report.

b. The CFMA index.

c. Cable diagrams.

d. Connector matrices.

e. Cable wire tables.

APPENDIX D

MX SOFTWARE HAZARDOUT EFFECTS ANALYSIS

10. SCOPE

10.1 Purpose. The Software Hazardous Effects Analysis (SHEA) is performed to ensure that system interlocks and functional controls are incorporated into software design to prevent weapon system hazards from being initiated by the software system.

10.2 Application. The SHEA defined in this appendix is applicable to the software which is used to prearm, arm, enable, unlock, target, launch or release the MX Weapon System. The SHEA shall be performed by the various MX Associate Contractors designing software defined above. The SHEA shall be provided to the SAIC for incorporation into the Integrated System Fault Tree Analysis.

20. REFERENCED DOCUMENTS

Not applicable.

30. DEFINITIONS

30.1 Software System. The software system consists of the system specification computer program, the computer itself, and all the peripheral equipments which enable the system to operate.

40. GENERAL REQUIREMENTS

40.1 Analysis requirements. The MX Associate Contractors shall perform the SHEA to provide a comprehensive evaluation of the risk being assumed when the assembled MX Nuclear Weapon System is subjected to deployment, operation, or maintenance. The analysis shall concentrate on potential errors in the software system, requirements, design, logic, coding, input/output devices, and maintenance. It shall also consider overlapping conditions to assure that non-planned events do not occur at the interfaces of system elements due to two routines changing a set state.

40.2 Analysis approach. The analysis shall include a review of the computer program development specification, flows, forms B, and the safety critical functions for the system elements. The analysis shall cover the human interfaces, the hardware/software interfaces across all system elements and evaluate the effect of the software on all system elements and the effect of the system elements on the software.

50. DETAILED REQUIREMENTS

50.1 Format. The format shown in figure D-1 shall be used in performing the SHEA. The following paragraphs provide instructions in the use of this format by reference to column heading.

Software function (change)	Function description Summary	System Hazard	Hazard Category	Safety Impact Discussion/ Conclusion	Recommended Requirements to Control Hazard	Remarks

FIGURE D-1. Software hazardous effects analysis format.

a. Software function (change). The particular software routine (or change if the original program is undergoing modification) is identified.

b. Function description summary. A brief summary of the purpose of the function, including identification of any critical command/monitor which impacts safety.

c. System hazard. Brief identification of a system hazard that could occur from improper operation/failure to operate of this function.

d. Hazard category. If the overall hazard category can be identified, include here. If the effect of the hazard is across a system interface and therefore unidentifiable, a marginal flag (P) should be entered. The SAIC will then be alerted to examine the interface area.

e. Safety impact (discussion/conclusion). (1) Discussion of the potential hazard or non-normal interface configuration caused by the improper operation, (2) any conclusions and supporting rationale for specific safety requirements.

f. Recommended requirements. Recommended safety requirements to eliminate or control the hazard within the software system. If the control cannot be effected within the software, suggested external controls or requirement shall be listed.

g. Remarks. Additional explanatory comments as required.

APPENDIX E

MX HAZARD CONTROL ASSESSMENT REPORT

10. SCOPE

10.1 Purpose. This appendix provides instructions for the preparation of MX Hazard Control Assessment Reports (HCAR) (see 5.8) and Integrated System Hazard Control Assessment Reports (ISHCARs).

10.2 Application. Compliance with this appendix by MX Associate Contractors is mandatory for the preparation of MX HCARs and ISHCARs.

20. REFERENCED DOCUMENTS

Not Applicable.

30. DEFINITIONS

Not Applicable.

40. GENERAL REQUIREMENTS

40.1 Assessment and verification. HCARs/ISHCARs shall provide comprehensive evaluations of compliance with MX safety requirements and assessments of the adequacy of MX hazard controls. They shall be used to certify hazard control provisions to the user organizations, such as contractor to SAMSO and SAMSO, as the "range user", to SAMTEC. The HCARs/ISHCARs shall be used for the life of the MX Weapon System as a baseline for decisions involving change to the system, facilities, or operational concepts.

40.2 Organization of HCARs. The several MX HCARs shall be organized in a manner similar to the structure shown in figure E-1.

40.3 General instructions. The HCARs/ISHCARs shall be developed and maintained in accordance with the following general instructions and groundrules:

a. Although each individual HCAR shall be an appendix to the appropriate ISHCAR(s), each HCAR shall be developed and maintained as a separate document.

b. Each HCAR submittal shall include sufficient level of detail to support the milestone events for the equipment included.

c. Each ISHCAR submittal shall include sufficient level of detail to support the appropriate program milestone event.

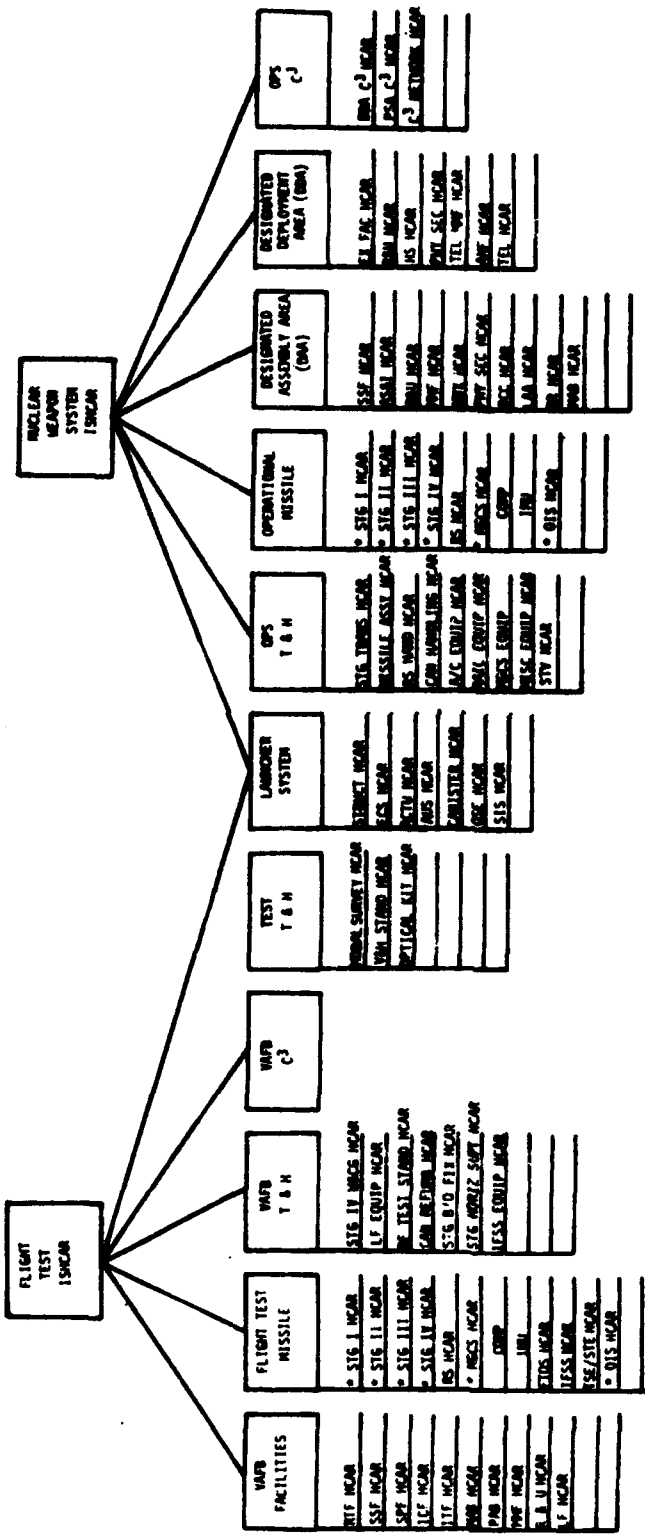


FIGURE E-1. Hazard control assessment report structure example.

d. Each basic HCAR and ISHCAR document shall contain only Unclassified data. A Classified Annex shall be provided if required.

e. Each incremental HCAR/ISHCAR submittal shall reflect progressively more detail from initial outline/partial data to the final with complete detail and assessment.

f. Revision by change pages will be used when practical.

g. HCAR/ISHCAR submittals shall be in accordance with the CDRLs.

50. DETAILED REQUIREMENTS

50.1 HCAR format. Each HCAR/ISHCAR shall contain the following sections:

a. Title page
b. Foreword
c. Table of Contents
d. Glossary of Terms
e. Section I – Introduction
f. Section II – Assessment Summary
g. Section III – Descriptions
h. Section IV – Assessment
i. Annex A – Hazard Catalog
j. Annex B – Hazard Control Requirements Lists
k. Annex C – Deviations (when required)
l. Annex D – Classified Data (as a separate document when required)

50.2 Individual HCAR content. Each individual HCAR shall provide data in accordance with the following detailed outline and general descriptions:

a. Title page shall include signatures of the MX Associate Contractor System Safety Manager and the Project Director.

b. Section I – Introduction

Note: This section should be limited to one page.

(1) Purpose and Scope

Provide a brief definition of the purpose of the document, the scope of the MX Weapon System equipment included and an overview of the relationship to other equipment/elements.

(2) Abstract

Provide an "Executive Summary" assessment of the accident risks.

c. Section II – Assessment Summary

Identify and summarize the significant problems and "Safety Concerns" that require management attention. Provide lists of "acceptable conditions" and "unacceptable conditions" defined for the MX equipment involved that would apply to the operational weapon system. Provide reference to more detailed analysis and assessments as appropriate, but do not duplicate data.

d. Section III – Description

(1) General Description

Provide a description of the total MX equipment involved, including items such as physical dimensions, nomenclature, etc. Provide definition of all subsystems or CIs in the HCAR. This subdivision should be compatible with the planned design reviews (PDRs and CDRs) to facilitate providing documentation to support those reviews.

(2) Subsystem (or CI) A

Provide detail information on the specific subsystem (or CI), including data such as schematics, materials, size/volume, pressures, temperatures, safety devices, certifications of proof tests, etc. Data included should be in sufficient detail to support the assessment. References to more detailed information may be used as appropriate.

(3) Subsystem (or CI) B

Same as above and repeat for all subsystems (or CIs).

e. Section IV – Assessment

(1) Design Features

Identify and discuss safety critical aspects of the MX equipment designs and actions taken to limit accident risks. Identify any incorporated safety devices, protective systems, and/or warning devices and provide the rationale for use.

(2) Interface Considerations

Identify potential problems with interfacing elements that require resolution in the ISHCAR.

(3) Test/Operation Plans

Discuss the planned activity at VAFB or operational site. Discuss any required planning for emergencies, including procedure and equipment requirements. Data should be in sufficient detail to convey a general understanding of the planned activity. References to more detailed information may be used as appropriate.

(4) Deviations

Provide a list of all approved deviations to contractual safety requirements including identification of the approval authority, date of approval, and reference to location of incorporation. System safety program management deviations are incorporated in the SSPP and copies of all approved deviations to technical requirements are included in Annex D of the HCAR.

f. Annex A – Missile X Weapon System Hazard Catalog

The Hazard Catalog is the two part catalog described in 50.1.3 of Appendix A.

Part I consists of a computerized list of all hazards analyzed and their status/disposition. The list and status shall be updated to the publication date of each submittal.

Part II consists of a one page summary of each "Safety Concern," including the rationale for descending the system safety order of precedence and for acceptance of residual hazards.

g. Annex B – Hazard Control Requirements Lists (HCRL)

The HCRLs are developed in accordance with 5.2.5.2 to include all and only requirements applicable to the MX equipment addressed in the HCAR. The HCRLs shall be structured to be compatible with the subsystem (or CI) identification in Section II of the HCAR.

h. Annex C – Deviations

This annex will be used as required to submit copies of all approved deviations to technical system safety requirements for the MX Weapon System equipment included in the HCAR.

i. Annex D – Classified Data

This annex will be used as required to submit all classified information required to complete and substantiate the HCAR.

50.3 ISHCAR content. Each ISHCAR shall be developed in the same format and outline as the HCARs but shall emphasize system level and interface considerations. The general descriptions of content presented in 50.2 shall apply except as follows:

a. Section III – Descriptions

This section shall identify each of the HCARs included and describe the physical and functional interfaces between them. Subsections shall be arranged to provide the most logical description of the equipment/interfaces.

b. Section IV – Assessment

(1) Design Features

Identify and discuss any system level or interface system safety aspects not covered in the supporting individual HCARs.

(2) Interface Considerations

Provide an assessment of all potential interface safety problems. As a minimum, resolution shall be provided for all potential interface problems identified in the supporting HCARs.