

AD-A129 603

METHODOLOGY FOR SYSTEM SAFETY ANALYSIS(U) SPACE AND  
MISSILE SYSTEMS ORGANIZATION LOS ANGELES CA 11 AUG 77  
SAMSO-STD-68-88

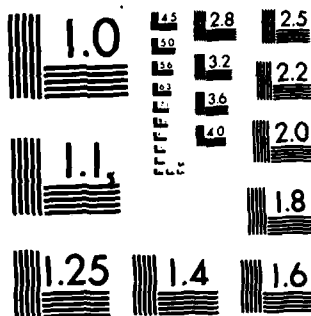
1/1

UNCLASSIFIED

F/G 22/2

NL

END  
DATE  
FILMED  
DTIC



MICROCOPY RESOLUTION TEST CHART  
NATIONAL BUREAU OF STANDARDS-1963-A

ADA 129003

Approved for Public Release;  
Distribution Unlimited

SAMSO STD 68-8B  
11 August 1977

SUPERSEDING  
SAMSO STD 68-8A  
10 May 1974

SAMSO STANDARD

METHODOLOGY FOR

SYSTEM SAFETY ANALYSIS

Accession For	
DTIC GUST	
EMIS TAB	
Unannounced	
Distribution	
<i>will m p te</i>	
By	
Distribution/	
Availability Group	
Dist	Avail and/or Special
<i>A</i>	

DTIC  
ELECTE  
JUN 21 1983  
S A D

SAMSO STD 68-8B

SPACE AND MISSILE SYSTEMS ORGANIZATION

El Segundo, California

Methodology for System Safety Analysis

SAMSO STD 68-8B

1. This SAMSO standard is approved for use by the Space and Missile Systems Organization (AFSC)
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.

## CONTENTS

		<u>Page</u>
Paragraph 1.	SCOPE . . . . .	1
2.	REFERENCED DOCUMENTS . . . . .	1
2.1	Issues of documents . . . . .	1
3.	DEFINITIONS . . . . .	1
3.1	Safety concern . . . . .	1
3.2	Closed safety concern . . . . .	1
3.3	Accepted risk . . . . .	1
3.4	Additional definitions . . . . .	1
3.5	Definition of acronyms used in this standard . . . . .	2
4.0	GENERAL REQUIREMENTS . . . . .	3
4.1	System safety analyses . . . . .	3
4.1.1	Responsibility for analyses . . . . .	3
4.1.2	Compatibility of analyses . . . . .	4
4.1.3	Hazard level categories . . . . .	4
5.	DETAILED REQUIREMENTS . . . . .	6
5.1	Preliminary hazard analysis (PHA) . . . . .	6
5.1.1	Purpose . . . . .	6
5.1.2	Documentation . . . . .	6
5.2	Operating hazard analysis (OHA) . . . . .	6
5.2.1	Purpose . . . . .	6
5.2.2	Documentation . . . . .	7
5.3	Fault hazard analysis (FHA) . . . . .	7
5.3.1	Purpose . . . . .	7
5.3.2	Schedule . . . . .	7
5.3.3	Format . . . . .	8
5.3.4	Documentation . . . . .	8
5.4	Cable failure matrix (CFM) . . . . .	8
5.4.1	Purpose . . . . .	8
5.4.2	Documentation . . . . .	8
5.5	Fault tree analysis (FTA) . . . . .	8
5.5.1	Purpose . . . . .	9
5.5.2	Procedure . . . . .	9
5.5.3	Integration . . . . .	9
5.5.4	Schedule . . . . .	9
5.5.5	Documentation . . . . .	10
5.6	Software hazardous effects analysis (SHEA) . . . . .	10

## CONTENTS - Continued

		<u>Page</u>
Paragraph 5.6.1	Purpose . . . . .	10
5.6.2	Documentation . . . . .	10
5.7	Accident risk assessment report . . . . .	10
5.7.1	Purpose . . . . .	10
5.7.2	Content . . . . .	11
5.7.3	Format . . . . .	11
5.7.4	Documentation . . . . .	12
6.	NOTES	12
6.1	Data requirements . . . . .	12

## FIGURES

		<u>Page</u>
Figure 1	System Safety Analyses Events and Milestones . . . . .	5
2	Fault Hazard Analysis Format . . . . .	14
3	"Lambda-tau" Combination . . . . .	25
4	Simplified Cable Failure Matrix . . . . .	30
5	Connector Pin Short Potentials . . . . .	30
6	Multiconnector Cable Diagram . . . . .	33
7	Cable Wire Table . . . . .	34
8	Modified Interface Control Drawing (ICD) and Cable Wire Run List . . . . .	35
9	Complex Cable Failure Matrix . . . . .	36
10	Software Hazardous Effects Analysis Format . . . . .	39

## APPENDICES

		<u>Page</u>
APPENDIX A - FAULT HAZARD ANALYSIS		
Paragraph 10.	GENERAL . . . . .	13
10.1	Purpose . . . . .	13
20.	REFERENCED DOCUMENTS . . . . .	13
30.	DEFINITIONS . . . . .	13
40.	GENERAL REQUIREMENTS . . . . .	13
50.	DETAILED REQUIREMENTS . . . . .	13
50.1	Format . . . . .	13
APPENDIX B - FAULT TREE ANALYSIS		
Paragraph 10.	GENERAL . . . . .	19
10.1	Purpose . . . . .	19
10.2	Application . . . . .	19
20.	REFERENCED DOCUMENTS . . . . .	19
30.	DEFINITIONS. . . . .	19
30.1	Failure event . . . . .	19
30.2	Primary failure event . . . . .	19
30.3	Secondary failure event . . . . .	20
30.4	Commanded failure event . . . . .	20
40.	GENERAL REQUIREMENTS . . . . .	20
50.	DETAILED REQUIREMENTS . . . . .	20
50.1	Graphic symbology . . . . .	20
50.1.1	Events . . . . .	20
50.1.2	Logic . . . . .	21
50.1.3	Special symbols . . . . .	22
50.2	Mathematics . . . . .	23
50.2.1	General . . . . .	23
50.2.2	Computation . . . . .	23
50.2.3	Simulation . . . . .	24
50.3	Data . . . . .	24
50.3.1	Data types . . . . .	24
50.3.2	Data sources . . . . .	26
60.	NOTES . . . . .	27



## APPENDICES - Continued

		<u>Page</u>
APPENDIX C - CABLE FAILURE MATRIX		
Paragraph 10.	GENERAL . . . . .	29
10.1	Purpose . . . . .	29
20.	REFERENCED DOCUMENTS . . . . .	29
30.	DEFINITIONS . . . . .	29
40.	GENERAL REQUIREMENTS . . . . .	29
50.	DETAILED REQUIREMENTS . . . . .	29
50.1	Connector fault modes . . . . .	29
50.2	Connector matrices . . . . .	29
50.3	Wire bundle fault modes . . . . .	31
50.4	Additional considerations . . . . .	31
APPENDIX D - SOFTWARE HAZARDOUS EFFECTS ANALYSIS		
Paragraph 10.	GENERAL . . . . .	37
10.1	Purpose . . . . .	37
20.	REFERENCE DOCUMENTS . . . . .	37
30.	DEFINITIONS . . . . .	37
40.	GENERAL REQUIREMENTS . . . . .	37
40.1	Nuclear safety . . . . .	37
40.2	Analysis approach . . . . .	37
50.	DETAILED REQUIREMENTS . . . . .	38
50.1	Format . . . . .	38

## 1. SCOPE

This standard tailors and interprets certain requirements of MIL-STD-1574 and defines the methodology to be used to satisfy the analytical requirements imposed by that MIL Standard.

## 2. REFERENCED DOCUMENTS

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

### Military Standards

MIL-STD-1574

System Safety Program for Space  
and Missile Systems

(Copies of specifications, standards, drawings and publications required by suppliers in connection with specific procurement functions should be obtained from the procuring activity or as directed by the contracting officer.)

## 3. DEFINITIONS

3.1 Safety Concern. An accident risk factor/hazard that is considered credible and of such significance that it be identified to program management. All safety concerns are documented in the Accident Risk Assessment Report and are tracked to resolution.

3.2 Closed Safety Concern. A safety concern can be closed in one of two ways.

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

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

3.4 Additional definitions. Additional definitions are contained in MIL-STD-1574.

- | -

3.5 Definition of acronyms used in this standard. The following acronyms listed in this standard are defined as follows:

A&CO	- Assembly and Checkout
ARAR	- Accident Risk Assessment Report
AVE	- Airborne Vehicle Equipment
CI	- Configuration Item
CFM	- Cable Failure Matrix
FHA	- Fault Hazard Analysis
FMEA	- Failure Modes and Effects Analysis
FTA	- Fault Tree Analysis
MSE	- Maintenance Support Equipment
NSCCA	- Nuclear Safety Cross Check Analysis
OSE	- Operating Support Equipment
OHA	- Operating Hazard Analysis
PA	- Procuring Activity
PHA	- Preliminary Hazard Analysis
RFI	- Radio Frequency Interference
SAIC	- Safety Analysis Integrating Contractor
SDR	- System Design Review
SHEA	- Software Hazardous Effects Analysis
SSEP	- System Safety Engineering Plan
SSPP	- System Safety Program Plan
SSWG	- System Safety Working Group
SSAR	- System Safety Analysis Report

#### 4. GENERAL REQUIREMENTS

4.1 System Safety analyses. The system safety analyses required by MIL-STD-1574 normally take the form of (1) Preliminary Hazard Analysis (PHA), (2) Operating Hazard Analysis (OHA), (3) Fault Hazard Analysis (FHA), (4) Fault Tree Analysis (FTA), (5) Software Hazardous Effects Analysis (SHEA), and (6) Cable Failure Matrix (CFM). The conduct of these analyses provides for the identification of hazards and safety requirements to be considered by the contractor during all phases of equipment design, development and operation. These analyses shall be conducted in a manner to provide sufficient sub-system documentation to facilitate the performance of integrated system safety analyses by a Safety Analysis Integrating Contractor (SAIC) and the summarization of specified safety concerns in an Accident Risk Assessment Report (ARAR). They shall provide the required documentation for post-design evaluation and numerical assessments. The contractors participating on a particular program shall be members of a System Safety Working Group (SSWG) for the purpose of reviewing integrated System Safety Analyses Data. Participation at SSWG meetings is not limited to SSWG members; other concerned agencies or personnel may attend as their duties require.

4.1.1 Responsibility for analyses. The associate contractor responsible for design and development of a Configuration Item (CI) will perform the PHA and the OHA to identify safety requirements; i.e., the analyses shall be utilized to establish the safety design requirements, constraints, warnings, cautions, etc., before the equipment and/or related procedures are designed. The contractor shall provide a closed-loop tracking system for insuring that all identified safety deficiencies have corrective action implemented in a timely and cost effective manner. The intent and objective of the above analyses are primarily to optimize safety by establishing optimum design requirements within the constraints of operational requirements, schedules and resources, and to accomplish this objective prior to Critical Design Review (CDR). The FHAs will be accomplished to monitor and control the design process with regard to system safety. They shall be accomplished during the hardware design phase and shall utilize established failure modes, failure rates, failure effects and shall establish resulting hazard categories. These elements shall be continually assessed by the contractor in a manner which assures that design attention is directed toward minimizing the hazardous effects of failures in the design solutions presented at Preliminary Design Review (PDR) and CDR. Thus, to be effective, the FHA must proceed concurrently with design to provide a basis for design safety assurance. Therefore the FHA must be completed by CDR. Finally, each associate contractor shall perform FTAs on category I or II events identified in the PHA and approved by the procuring activity (PA) at PDR and selected events relative to his CI that are required by the SAIC to complete the system level fault trees.

4.1.1.1 Review of analyses. System level safety analyses will be reviewed and integrated by the SAIC. These analyses include the six types of analyses indicated in 4.1 and consider the integrated weapon system to include all interfaces between the individual associate contractors' subsystems. The hazard events to be analyzed by the fault tree technique will be those specified by contract and those identified as Category I or II by the SAIC and approved by the PA.

4.1.2 Compatibility of analyses. It is essential that the fault hazard and fault tree analyses of each contractor be compatible with those of the other associate contractors so that the systems analyses can be performed without reaccomplishing the subsystem level analyses. The format, definitions and ground rules specified in this standard shall be followed to provide the necessary standardization. MIL-STD-1574 specifies the orderly progression of analyses to support design reviews. Figure 1 presents the analyses in calendar format to be performed toward the goal of completion by CDR. All analytical effort should be complete by that time to support production release. The SAIC performing overall system safety analysis integration should have all data by the CDR with the exception of those design changes resulting from CDR actions.

4.1.3 Hazard Level categories - The method of categorizing hazard levels required by MIL-STD-1574 shall be as follows:

- a. Category I - Conditions resulting from design deficiency/inadequacy, component failure/malfunction, or personnel error where the worst case potential effect is loss of life or major system loss such as loss of missile/launch vehicle. The category includes the nuclear safety undesired events such as inadvertent programmed launch, accidental motor ignition, inadvertent nuclear detonation, and faulty launch.
- b. Category II - Conditions resulting from design deficiency/inadequacy, component failure/malfunction or personnel error where the worst case potential effect is major injury or system damage (major subsystem loss or loss of mission).
- c. Category III - Conditions resulting from design deficiency/inadequacy, component failure/malfunction or personnel error where the worst case potential effect is less than the above.

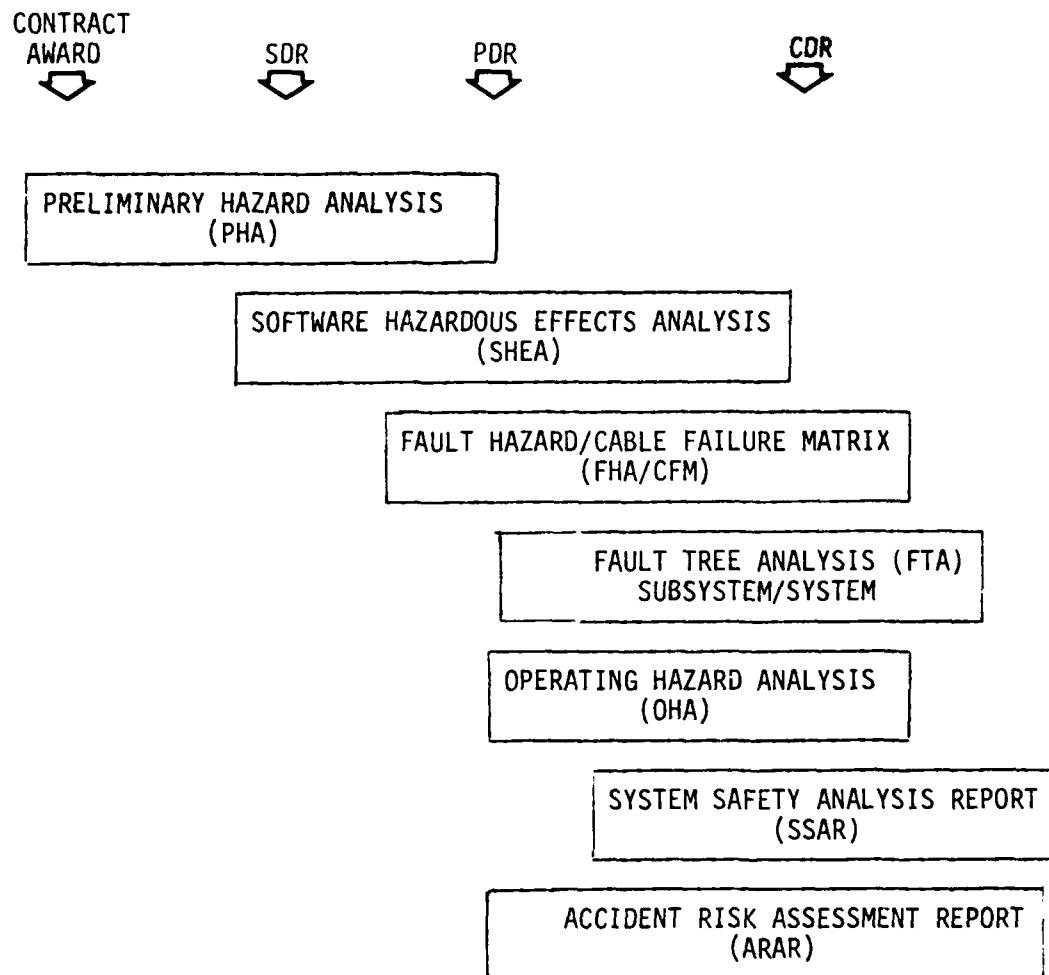


Figure 1. System safety analyses events and milestones

## 5. DETAILED REQUIREMENTS

### 5.1 Preliminary Hazard Analysis (PHA)

5.1.1 Purpose. The primary purpose of the PHA required by MIL-STD-1574 is to identify system/subsystem hazards for the purpose of establishing safety requirements for inclusion in the CI specification. The PHA shall be performed on each new system, subsystem, major hardware modification, or major additive to a program. It shall be initiated during the contractor's initial efforts in the conceptual phase or feasibility studies and shall continue up to the PDR. This analysis shall be used to identify and document, in a qualitative manner, the hazards recognized by the contractor, and the design and/or procedural constraints which are imposed upon an end item to eliminate, control or minimize the hazard. The analysis shall indicate all the hazards identified by the contractor for each CI, the hazard category per 4.1.3 of this standard, and the actions that must be taken to eliminate or control Category I or II hazards. The action taken shall normally result in design and/or procedural constraints. Those Category I or II hazards remaining at PDR, will be submitted to the PA for determination of those which shall be subjected to FTA. The conduct of PHA and its use throughout design is delineated in the contractor's system safety program plan and must be an integral part of his engineering management effort. As such, no format is specified for the documentation of this effort. The contractor shall be free to utilize the format which best fits his organization and (1) provides a closed-loop system of identifying and resolving safety problems, (2) provides documentation of the efforts accomplished and the hazards considered, (3) provides traceability from the identification of the hazards to the resulting corrective action in the design or procedures and (4) facilitates review by the PA at System Design Reviews (SDRs) and PDRs.

5.1.2 Documentation. The results of the PHA will be presented at the SDR and PDR. The means of control, for any identified Category I or II hazards that are not to be quantitatively analyzed, will be presented at CDR, with accompanying rationale. The documentation of the analysis shall be maintained in the contractor's facility and updated as required.

### 5.2 Operating Hazard Analysis (OHA)

5.2.1 Purpose. The primary purpose of the OHA required by MIL-STD-1574 is to provide the basis for the preparation of procedures for:

- a. Rendering the subsystem/system safe under normal and emergency conditions
- b. Emergency escape or egress and rescue operations

- c. Ground handling and transportation operations and environments.
- d. Operating and maintenance operations, including warning and caution notes.
- e. Identification of a hazardous period time span and actions required to control the identified hazard(s).
- f. Recovery procedures for potential accidents.

To assure maximum effectiveness of this analysis, it shall be initiated as early in the program as possible. Whereas the PHA is normally Airborne Vehicle Equipment/Operating Support Equipment (AVE/OSE) oriented, the OHAs are personnel, procedure, and Maintenance Support Equipment (MSE) oriented and, therefore, must consider all the elements of the operation and maintenance functional flows. These analyses shall define the operating hazards considered by the contractor, the control, reduction, or elimination of which are to be reflected in the equipment and/or procedures developed for the CI. The analyses shall include all functions and equipment documented in the CI functional flows. The contractor shall be free to utilize the format which best fits his organization and follows good engineering documentation practices. The results of the OHA will be presented at the CDR for the affected hardware. The documentation of the analysis shall be maintained at the contractor's facility for review and updated as required.

5.2.2 Documentation. Formal submittal of the OHA shall be in accordance with the Contract Data Requirements List (CDRL). The OHA shall list all known or suspected hazards against each function or procedure with an associated hazard category, as defined in 4.1.3 with instruction on how to eliminate, reduce or control each hazard. In addition the analysis will define the potential accident and detail the recovery measures.

5.3 Fault Hazard Analysis (FHA). The FHA shall be conducted in accordance with Appendix A of this standard.

5.3.1 Purpose. Each associate contractor responsible for a CI shall conduct a FHA on the CI. On complex systems, this analysis may be made up of several analyses accomplished on units which make up the CI. The purpose of the analysis, in addition to that indicated in 4.1.1, is to document all primary, command and significant secondary failure modes of a CI design, and to provide additional information required for fault tree construction and numerical assessment.

5.3.2 Schedule. The FHA shall be initiated concurrent with the design of each CI and shall continue until the CDR is completed. The contractor shall insure that necessary management and administrative



actions are invoked to compare the results of the FHA with hazards identified in the PHA and OHA and the constraints identified in the CI specification. This iterative process shall continue until the CDR. Such iteration shall be described in the contractor's System Safety Program Plan (SSPP).

5.3.3 Format. The FHA shall be documented in a manner which facilitates the construction of fault trees required of both the associate contractor and SAIC with minimum requirements for additional data. The level of detail of the FHA report will be based on a PA-approved component breakdown supplied by the contractor which best describes his CI within the following minimum requirements:

- a. The analysis shall contain a hardware oriented flow diagram, i.e., by subassembly which indicates to the fault tree analyst the functions performed by the CI and the command flow. On complicated CIs composed of multiple major subassemblies, indented flow diagrams shall be used to the extent required to accomplish the FHA objectives.
- b. The FHA format described in Appendix A shall be used for each indenture of the functional flow diagram and each component listed in the column provided.

5.3.4 Documentation. Formal submittal of the FHA shall be in accordance with the CDRL.

5.4 Cable Failure Matrix (CFM). The CFM shall be developed in accordance with Appendix C of this standard.

5.4.1 Purpose. In lieu of performing a complete FHA on the inter-connecting cables and connectors within a CI, and because the functions and failure modes of these elements are generally well established, a CFM shall be developed for each cable assembly within a CI. These matrices form a part of the FHA report although they may be provided in a separate document. The predominant failure events depicted from the cable failure matrix, affecting the desired output of a cable, will be added to the command and/or secondary failure columns of the FHA for the associated CI.

5.4.2 Documentation. Formal submittal of the FHA, including the CFM, shall be in accordance with the CDRL, normally a sufficient period after CDR to allow changes and the incorporation of comments resulting from the CDR presentations and review.

5.5 Fault Tree Analysis (FTA). The FTA shall be conducted in accordance with Appendix B of this standard.

5.5.1 Purpose. Each associate contractor responsible for the design and development of a CI shall perform subsystem FTAs on that end item, as directed by the PA. The purposes of the FTA are twofold. First, they provide the means for determining and graphically presenting the events or combinations of events which will cause a defined undesired event. Secondly, they provide a basis for assessing the probability of occurrence of those events, either by statistical or simulation methods.

5.5.2 Procedure. The Category I and II hazards identified by the contractor's PHA at PDR shall be the basis of the PA designation of the events to be subjected to subsystem FTA for each CI. Additional hazards resulting from the FHA will also be reported to the PA for determination if FTA shall be required. Each associate contractor shall be responsible for the development and assessment of fault trees for the PA approved events within the bounds of his CI.

5.5.3 Integration. The SAIC shall develop the system level top trees to identify the additional events to be required from each associate contractor to support the system level trees. The FTA development of these events, upon PA approval, shall also be a requirement of the appropriate associate contractor within the bounds of his CI. The SAIC shall be responsible for those portions of the FTA that extend beyond the associate contractor's CI interface.

5.5.4 Schedule. The FTA is initiated concurrent with the design effort. Associate contractor FTAs, insofar as possible, are completed prior to CDR. Upon review by the SSWG they will be informally submitted to the SAIC for use in the system level analysis. Subsequent to CDR they will be updated to reflect any changes or actions directed at CDR and then be formally submitted as required by the CDRL. It is intended that the associate contractors subsystem FTAs be adequate for approval at CDR for direct application to the system level trees. Close liaison and technical interchange between the PA, the SAIC and the associate contractors is required to meet this goal. The SAIC will complete the system level fault trees utilizing to the maximum practicable extent the trees submitted by the associate contractors. The SAIC will be responsible for completing the system level fault trees for specific safety critical events which extend across associate contractor interfaces. The system level FTAs should be ready for SSWG final review approximately 90 days following the last CDR. Subsequent to this review the results will be documented in the System Safety Analysis Report (SSAR) and formally submitted to the PA for approval as required by the CDRL. The contractor shall closely monitor the development of his FTAs for early identification of problem areas. The contractor shall exercise necessary management control to assure early identification of those undesired events whose likelihood of occurrence must be minimized in design to attain maximum safety consistent with operational requirements and to minimize post-CDR change action.

5.5.5 Documentation. Formal submittal of the FTA shall be in accordance with the CDRL. Normally, a sufficient period after the CDR is allowed for incorporation of changes and comments resulting from the CDR presentation and review.

5.6 Software Hazardous Effects Analysis (SHEA). The SHEA shall be conducted in accordance with Appendix D of this standard.

5.6.1 Purpose. The SHEA is to be performed on all software having any direct interface with the operational weapon system. The SHEA is to be performed by the software development contractor during software design. 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 skips causing illegal entry into critical routines). All routines and functions of the software program are to be examined. The analysis will be based on the assumption that one illegal computer skip may occur at any time. Possible hazardous configurations will be determined by noting the effect of one illegal computer skip, as well as all legal program branches, program transfers, and computer restarts. For purposes of this analysis, the software program under development and the computer in which the program will reside are to be considered an entity. The results of the SHEA will:

- 1) affect the design of the software system wherever practical to assure control of possible system hazards.
- 2) identify to the SAIC, for inclusion in the integrated weapon system analysis, those potential hazards introduced or impacted by the software system.

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

#### 5.7 Accident Risk Assessment Report

5.7.1 Purpose. The Accident Risk Assessment Report required by MIL-STD-1574 is a summary of the safety critical accident risk factors/hazards which have been identified during the safety analysis process and the manner in which they are being controlled. The report provides management visibility of the risk being assumed in all system operational modes and the actions taken or remaining to be taken to reduce the risk. It provides the basis for management decision on the adequacy of the controls or acceptability of the residual risk and the data for any tradeoffs involving risk versus operational requirements.

5.7.2 Content. The Accident Risk Assessment Report is limited to those accident risk factors/hazards which have been designated as safety concerns (see 3.1). This would normally include all Category I and many Category II hazards, although a Category III hazard could be listed where a significant cost tradeoff requiring a management decision was involved. Contractors shall draw up a proposed list of hazards to be designated as safety concerns. PA concurrence/non-concurrence on the designation will be given at safety working group meetings. Associate contractors shall list those safety concerns where the postulated accident is initiated by the component/subsystem for which they have design responsibility. The Safety Analysis Integrating Contractor shall list the overall system concerns, work the associate interface concerns and compile the integrated system accident risk assessment report which will include the associate contractor reports as appendices.

5.7.3 Format. The report shall be made in narrative style and as a minimum will contain a Table of Contents, a short Introduction, a Statement of Purpose and Scope and explanatory material as deemed necessary for reader orientation. Following this will be a listing of open safety concerns and accepted risks by short title, with a paragraph reference to the main body of the report. The main body of the report shall contain the detailed assessment of the safety concerns separated into a logical sequence of subsystem, operation or event with which they are related. As an example, safety concerns involving a certain subsystem shall be grouped under that subsystem with paragraph headings and subheadings as follows:

Example:

#### 4.3 Subsystem Nomenclature

4.3.1 Subsystem description. (Provide enough detail so that the safety concern can be understood and evaluated).

4.3.2 Analysis Summary. (List the gross hazards associated with the subsystem and state which ones are considered credible).

#### 4.3.3 Safety Concerns

4.3.3.1 Safety Concern #1 (Descriptive short title).

Concern Description (Brief statement of the potential hazard).

Discussion (More detail on the potential hazard, its probability of occurrence, steps which have been taken to reduce the hazard, results of any analyses which have been accomplished and any tradeoffs which are available).

Closure Rationale (State whether item is still open, whether the risk has been accepted, giving rationale for acceptance, or if the concern is closed, state how hazard has been controlled).

#### 4.3.3.2 Safety Concern #2

Appendices to the report may be utilized as needed to summarize special analyses or provide other reference information useful for management actions or decisions.

5.7.4 Documentation. Formal submittal of the Accident Risk Assessment Report shall be in accordance with the CDRL, however incremental reviews will be made at Safety Working Group meetings.

## 6. NOTES

6.1 Data requirements. Data requirements of this standard shall not be prepared or delivered to the purchasing office unless specified by the Contractor Data Requirements List (CDRL). The data normally required under this standard includes:

- a. (U)S-716(SAMSO), Accident Risk Assessment Report
- b. DI-S-3581 Subsystem Design Analysis Report
- c. DI-H-3278 Preliminary Hazards List and/or Analysis

APPENDIX A  
FAULT HAZARD ANALYSIS

10. GENERAL

10.1 Purpose. The Fault Hazard Analysis (FHA) is the tool used to define the effects of various component failure modes and categorize these effects on system equipment or personnel in conformity with 4.1.3 of this document. This indicates which subsystem effects must be further analyzed during system analysis and includes, but is not restricted to, all effects in Category I and II. The analysis considers all the CIs in the system and, therefore, all the interface effects due to CI internal failures. Analyzing at the CI level allows all identifiable hazards to be found because each hazardous event must terminate in a subsystem major component.

20. REFERENCED DOCUMENTS (Not applicable)

30. DEFINITIONS (Not applicable)

40. GENERAL REQUIREMENTS (Not applicable)

50. DETAILED REQUIREMENTS

50.1 Format. The format shown in figure 2 shall be used in performing the FHA. The FHA may be combined in the Failure Modes and Effects Analysis (FMEA) as long as the pertinent data required is listed. The following paragraphs provide instructions in the use of this format by reference to column heading.

- a. Major component - Components are defined, at the discretion of the analyst, by their physical or functional significance to the CI or its design concept. Alpha numeric indexing with indentures may be used to facilitate identification and referencing. A guide for defining the major components is included to facilitate understanding of the types of natural separations to consider. It is not intended to be exhaustive.

- (1) Electronic logic circuits - Many CIs are made up from a small number of basic circuit designs which perform an

MAJOR COMPONENT	COMPONENT FAILURE MODE	COMPONENT FAILURE PRIMARY	SYSTEM OPERAT'L MODE	EFFECT OF COMPONENT ON CI	PRIMARY FAILURE	FACTORS THAT MAY CAUSE SECONDARY COMPONENT FAILURE	UPSTREAM COMPONENTS OR INPUTS THAT MAY COMMAND THE UNDESIRE STATE	HAZARD CATE- GORY	REMARKS

Figure 2. Fault hazard analysis format

identifiable purpose. These are used as building blocks for larger circuits designed to perform the required logic functions to the CI. To minimize the analysis required, the basic circuits can be defined as major components, and an analysis made of each logic function.

- (2) Mechanical devices - Mechanical devices can be either a single part or an assembly of parts which perform one function. For an FHA, a major mechanical component can be defined as either. The use in the system will dictate to what level of detail mechanical parts should be considered. Single parts which can be considered major components are: solid drive shafts, engine blocks, primary structure, etc. The majority of mechanical devices will be assemblies of many parts and it is more reasonable to treat the assemblies as major components; for example: relays, pumps, motors, mechanical safety devices, etc. This permits the majority of vendor supplied mechanical devices to be analyzed as major components, thus avoiding the requirement for vendors to provide an FHA of their subsystems.
  - (3) Electrical systems - Major components can be basic components of a circuit or combinations of components used to perform one single function such as amplifiers, rectifiers, or regulators. The level of analysis should be based on the importance of the part as a functional element in the design.
  - (4) Chemical systems - In systems containing chemical compounds, the chemicals should be considered as major components if these compounds can cause failures of other components through chemical reaction or release of chemical energy. Examples of chemical components are: fuels, pressurants, coolants, and preservatives.
  - (5) Safety devices - Safety devices will always be considered as major components since they are used primarily to protect against undesired events.
  - (6) Wiring - Interconnecting wiring of major components will be considered a major component. Internal wiring will be considered as a part of a major component. Physical characteristics of cables which prevent failures between wires should be stated in the cable analysis.
- b. Component failure mode - Failures of major components consisting of one part require a listing of the modes in which that



part may fail. Failures of major components consisting of more than one part or circuits containing more than one component will require a failure mode and effects analysis to determine how the failure modes of each part or component affect the components' or circuit output. These effects will be the failure modes of the major component listed in the FHA. All failure modes of the component must be listed.

- c. Component failure rate - The predicted failure rate computer from actual field data of primary failures should be tabulated in this column for each major component in each of its modes of failure. These data can be used in evaluating the probability of the fault event or in selecting which safety critical events should be analyzed if the decision is made not to analyze all those in Category I and II. It also serves as a data bank for future reference when the need arises to analyze other undesired events as a result of system changes.
- d. System operational mode - Many major components are repeatedly activated during the system's operational life. The level of stress of these components will change from one system mode to another. The effect of a failure in each mode can be different; for example, components supplied with power only during a test can create a fault hazard only while a test is performed. Failures existing in one mode of system operations can also adversely affect the system when the mode is changed. Therefore, each major component failure mode must be analyzed for possible effects on all system operational modes.
- e. Effects of primary component failure on configuration item (CI) The effect of the major component's abnormal output on the CI's operation is listed in this column. The effect will be of the immediate functional output on the most proximate downstream components. No secondary considerations are necessary. A description of the functional effect on normal CI operation will supply the required information. This data can be extracted from information used to provide the maintenance engineering fault matrix. Some failures can initiate a normal chain of events within the CI. Those sequences that are inherent to the design can also be reported as a primary effect. The description of this effect should be identified by its particular CI oriented function and also by form and magnitude of output energy. This information is necessary when using the completed Fault Hazard Analysis for construction of fault trees. Once an undesired event has been defined, all primary failure modes can be found by scanning this column.

- f. Factors that may cause secondary component failure - Any major component operating in a system is subject to out-of-tolerance and abnormal inputs. There may be no source of such conditions within the subsystem under analysis, but once integrated into a system, abnormalities can arise. To insure detection of the hazardous secondary conditions which can cause equipment failure, the limits beyond which failure occurs will be listed. This information is very significant, because a failure causing an out-of-tolerance condition can affect many critical system functions simultaneously and may degrade the system's safety.

The following items are examples of information which should be included in this column when applicable.

- (1) Effect of power reversals
- (2) Effect of high and low power
- (3) Temperature limits
- (4) Shock limits
- (5) Vibration limits
- (6) Radio Frequency Interference (RFI) limits
- (7) Electromagnetic limits
- (8) Transient effects
- (9) Chemical effects
- (10) Any other source of energy which, if supplied in a sufficient quantity, will cause the primary failure rate to increase.

- g. Upstream components or inputs that may "command" the undesired state - The analysis cannot be continued unless it is known how the undesired event could occur due to improper inputs being furnished to the major component. It has been shown that a fault effect on a CI may be caused by a primary or secondary failure of a major component. This column shows how the fault effect on the CI may be caused by having improper input signals applied to the major component. This is termed a "Commanded Failure" and describes the specific subsystem oriented functions and their energy level and shape

required to command the specific failure mode being analyzed. Improper outputs of the most proximate upstream components will be listed.

- h. Hazard level category - This column provides an estimate of the severity of the effect on the CI (see 4.1.3 for definitions of hazard level categories).
  - (1) MARGINAL FLAG (P) - A marginal flag designation shall be used to identify a potential system level Category I or II hazard that is not present on the individual equipment, but may be a potential integrated system hazard (Category I or II) with the individual equipment item combined into the system. This is used to flag the attention of the SAIC to this potential problem.
- i. Remarks - This column is used to include additional information needed to clarify or verify information in the other columns, or to provide a permanent note of recommended future actions. A few examples of usage are given below:
  - (1) Describe the number and type of monitors on this major component failure mode, if known.
  - (2) Show the recommendations for further system analysis as a permanent note.
  - (3) Explanation of a major component definition in doubtful cases.
  - (4) Any agreements not to analyze a Category I or II event and reference.
  - (5) A coding to show data source on the primary failure rates.
  - (6) A discussion of time sequencing of fault tree events entered in the "Command" column No. 7.
  - (7) Rationale on hazard category if the category assigned is doubtful.
  - (8) When applicable, a statement that the major component is an interface component and requires an input from another subsystem or can provide the abnormal output in the "Effect of primary failure on CI" column.

## APPENDIX B

### FAULT TREE ANALYSIS

#### 10. GENERAL

10.1 Purpose. A Fault Tree is a graphic representation of the various parallel and series combinations of subsystem and component failures which can result in a specified system failure. The fault tree, when fully developed, may be mathematically evaluated to establish the probability of occurrence of the ultimate undesired event as a function of the estimated probabilities of occurrence of identifiable contributory events.

10.2 Application. The development of a Fault Tree begins with the definition of the end system fault condition ("undesired event"). The system is then analyzed and all the logical combinations of functional fault events which can cause the end event are determined. Such an analysis is wholly dependent upon a thorough knowledge of the system functions and equipment. Each of the contributory fault events is further analyzed to determine the logical interrelationships of subsystem fault events which can cause them. Analysis is facilitated if the fault events are systematically classified according to failure cause. It is pertinent to consider each fault as the possible result of primary, secondary, and commanded failures. In this manner a tree of logical relationships among fault events is developed. The development is continued until all input fault events on the tree are defined in terms of basic, identifiable faults which can be assigned known probability values.

#### 20. REFERENCED DOCUMENTS (Not applicable)

#### 30. DEFINITIONS

30.1 Failure event. A condition of a device whereby the output state is erroneous, or not normal for the system condition, i.e., the Safe and Arm (S&A) device is in the armed state with the system in Strategic Alert.

30.2 Primary failure event. A failure of a device, in and of itself, while operating with normal inputs and within design constraints, i.e., autoignition of the squibs in the S&A device.

30.3 Secondary failure event. A failure of a device, not in and of itself, but caused by other than normal inputs, or operation outside design constraints, i.e., the squibs in the S&A device are activated by severe shock.

30.4 Commanded failure event. An erroneous, or abnormal output for the system condition, from a correctly operating device, as a result of an erroneous or abnormal command input, i.e., the S&A device arms in Strategic Alert as a result of power applied erroneously to the S&A Motor.

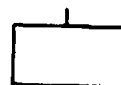
#### 40. GENERAL REQUIREMENTS (Not applicable)

#### 50. DETAILED REQUIREMENTS

50.1 Graphic symbology. The following graphic symbology shall be used in preparing the Fault Tree.

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

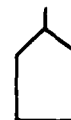
- a. The RECTANGLE identifies an event in a Fault Path that results from a combination of fault events.



- b. The CIRCLE identifies a primary failure of a device.



- c. The HOUSE indicates an event or state which is normal for the system.



- d. 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.

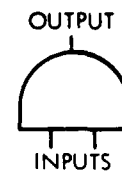


- e. The DOUBLE DIAMOND terminates a branch which has not been fully developed due to lack of information.



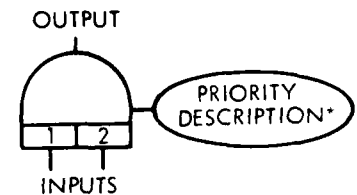
50.1.2 Logic. The logic operators required to develop the fault trees are defined and symbolized as follows:

- a. The AND gate describes the logical operation which requires the co-existence of all inputs to cause the output.

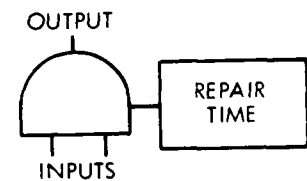


- b. The PRIORITY AND gate performs the same function as the AND gate except that the inputs must occur in the sequence stipulated.

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



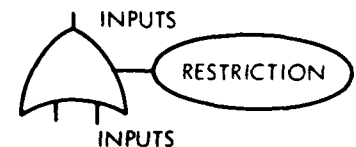
- c. The CONSTANT REPAIR AND gate performs the same function as the AND gate except that the repair time of the output event is not dependent on the repair times of the inputs, but is as stipulated.



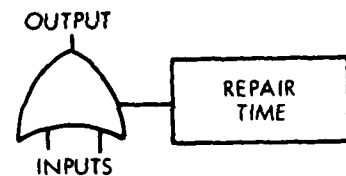
- d. The OR gate describes the logical operation whereby the output is caused by the occurrence of any of the inputs.



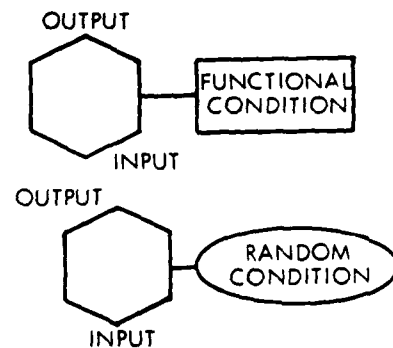
- e. The EXCLUSIVE OR gate performs the same function as the OR gate except that specified inputs cannot coexist.



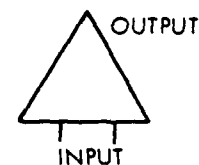
- f. The CONSTANT REPAIR OR gate performs the same function as the OR gate except that the repair time of the output event is not dependent on the repair times of the input, but is as stipulated.



- g. 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.

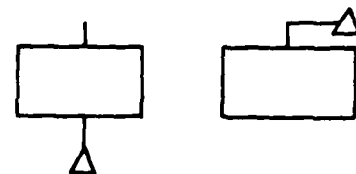


- h. The MATRIX gate is used to describe a situation in which an output event is produced for certain combinations of events at the inputs. A matrix showing the event combinations that produce the output event will accompany each usage of this symbol.

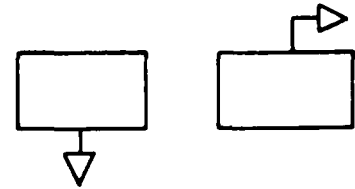


50.1.3 Special symbols - Special symbols are used in order to simplify the graphic representation of fault tree construction. These special symbols are shown below:

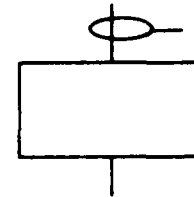
- a. The TRANSFER symbol is used to show continuity between two parts of the tree. A line into the side of the triangle transfers everything below to another area identified by the triangle with a line drawn from the apex.



- b. The INVERTED TRANSFER symbol is used to show similar type tree construction. The only difference being designations or pin numbers.



- c. An ELLIPSE with a line extending out along the major axis is used when a component appears several times at the same place (e.g., a 10-stage counter). Only one of the inputs is drawn and the ellipse is drawn to encompass the output. This indicates that the failure rate of that event is to be multiplied by the given factor for an OR gate or raised to a given power for an AND gate.



## 50.2 Mathematics

**50.2.1 General.** There are two basic approaches used to quantify fault tree probabilities. The two approaches are calculation and simulation. The calculation or deterministic approach will be considered first. For fault trees where every basic input is nonrepairable, classical probability can be used. In this case each gate merely represents the operation to be performed (i.e., union for OR gates and intersection for AND gates). The classical probability approach, while simple and efficient, is not adequate for fault trees where the effect(s) of a basic failure can be eliminated before the defined mission length is achieved (e.g., a failed component is located and repaired). A basic failure whose effect can be removed is called repairable; however, the usage of the word "repairable" is irregular because the effect may be terminated without actually repairing or replacing the failed item. The analysis of repairable systems requires special statistical techniques.

**50.2.2 Computation.** One such technique is the "lambda-tau" (" $\lambda - \tau$ ") method. To use the " $\lambda - \tau$ " method to evaluate fault trees, failure rates must be small, and the redundant inputs must be removed. Redundancies that are not removed may lead to serious unbounded errors in the answer. The fault tree is usually expressed algebraically and operated on by Boolean algebra theorems to remove redundancies. The " $\lambda - \tau$ " method can be evaluated by hand or by digital computer. However, as the fault trees get larger in size, the task of hand calculation becomes time consuming, laborious, and error prone. The " $\lambda - \tau$ " method was programmed for the digital computer. The computer program also



writes the algebraic expression and uses Boolean algebra to remove the redundancies. However, computer core storage limits the size of the fault tree solvable by this method. Nevertheless, smaller fault trees can be calculated accurately by hand or computer using " $\lambda - \tau$ " methods. " $\lambda - \tau$ " combinations are given in Figure 3.

**50.2.3 Simulation.** In the simulation approach, a fault tree is represented on a computer and the failures are simulated over a given mission length. The computer prints out the fault path which leads to the undesired event and produces an estimate of its probability of occurrence. The information and probability estimate derived from the computer simulation is no substitute for rigorous manual quantitative analysis once the dominant fault paths have been qualitatively identified. The simulation approach has all the advantages of the calculation approach except for the greater amount of computer time needed to simulate fault trees with small probabilities. Simulation offers several additional advantages i.e., the dominant paths are listed and the computer can solve larger fault trees (10 times larger than " $\lambda - \tau$ "). Simulation has gone through many stages of development. In its early stages, the amount of computer time required became prohibitive; however, special Monte Carlo techniques (importance sampling) have reduced greatly the computer time needed. The importance sampling technique distorts the true failure distribution to make events occur more rapidly. Thus, the number of trials (a trial represents the predefined mission length of the system) required for an acceptable statistical confidence is reduced. Overall, simulation offers better potential and has proven to be more effective in identifying critical areas in the system than the computation method.

### 50.3 Data

**50.3.1 Data types.** Several types of numerical data are required for a mathematical fault tree evaluation by the " $\lambda - \tau$ " method or simulation method. In the succeeding paragraphs are listed the types of data needed and some of the possible sources.

- a. Major component failure data - The basic fault tree inputs are the primary and secondary failures of major components. This data, symbolized by " $\lambda$ ," is in the form of failure rates, mean time between failures, or failures per trial.
- b. Event data - Event data is data concerning system function other than failures or malfunctions. This data is sometimes required because major component failure rates can be affected by normal system functions. An example of this is changes in a component stress level as the system changes from a "quasi-static" to a dynamic state. The fault tree must be structured to account for these effects and probabilities assigned to these events for mathematical evaluation.

		2 INPUTS	3 INPUTS	n INPUTS
AND	$\tau_s$ UNEQUAL	$\lambda_n$	$\lambda_1 \lambda_2 \lambda_3 (\tau_2 \tau_3 + \tau_1 \tau_3 + \tau_1 \tau_2)$	$\lambda_1 \lambda_2 \dots \lambda_n (\tau_2 \tau_3 \dots \tau_n + \tau_1 \tau_3 \dots \tau_n + \tau_1 \tau_2 \dots \tau_{n-1})$
		$\tau_n$	$\frac{\tau_1 \tau_2 \tau_3}{\tau_2 \tau_3 + \tau_1 \tau_3 + \tau_1 \tau_2}$	$\frac{1}{\frac{1}{\tau_1} + \frac{1}{\tau_2} + \dots + \frac{1}{\tau_n}}$
	$\tau_s$ EQUAL	$\lambda_n$	$3 \lambda_1 \lambda_2 \lambda_3 \tau^2$	$n \lambda_1 \lambda_2 \dots \lambda_n \tau^{n-1}$
		$\tau_n$	$\frac{\tau}{3}$	$\frac{\tau}{n}$
OR	$\tau_s$ UNEQUAL	$\lambda_v$	$\lambda_1 + \lambda_2 + \lambda_3$	$\lambda_1 + \lambda_2 + \dots + \lambda_n$
		$\tau_v$	$\frac{\lambda_1 \tau_1 + \lambda_2 \tau_2}{\lambda_1 + \lambda_2} \quad \frac{\lambda_3 \tau_3}{\lambda_1 + \lambda_2 + \lambda_3}$	$\frac{\lambda_1 \tau_1 + \lambda_2 \tau_2 + \dots + \lambda_n \tau_n}{\lambda_1 + \lambda_2 + \dots + \lambda_n}$
	$\tau_s$ EQUAL	$\lambda_v$	$\lambda_1 + \lambda_2 + \lambda_3$	$\lambda_1 + \lambda_2 + \dots + \lambda_n$
		$\tau_v$	$\tau$	$\tau$

Figure 3. " $\lambda - \tau$ " combination

- c. Conditional data - The occurrence of some events may be contingent upon the existence of certain system conditions. Inhibit gates are used in fault trees to depict such a situation. A probability value must be assigned to the conditional inputs of inhibit gates and these are termed conditional data.
- d. Repair data - The repair times used in fault tree evaluation represent fault duration times, that is, the time the system is exposed to the fault effects before it is terminated by repair or some other change in the system state. This data, symbolized by "tau," is associated with the failure data assigned to each major component failure in the fault tree and is vital to the mathematical evaluation.

50.3.2 Data sources. Data for fault trees and fault hazard analyses are derived from the following sources:

- a. Achieved data - The most useful source of major component failure data for fault tree evaluation is achieved reliability data obtainable from the associate contractors and Air Force agencies. Examples of these are AFM 66-1 Maintenance Management reports, and the data summaries obtainable from the SAIC contractor.
- b. Component data - If no reliability information is available for major components, it is frequently possible to synthesize it through a failure modes and effects analysis from component part reliability data. Component reliability data can be obtained from such sources as MIL-HDBK-217A, Reliability Stress and Failure Rate Data for Electronic Equipment. Another source of reliability data is Assembly and Checkout (A&CO) and operational field reports. The principal shortcoming of this type of data is that there is no way to distinguish between primary and secondary failure modes.
- c. Laboratory tests - In some instances major component reliability data is not available or cannot be generated from component part data. In these cases, it is sometimes feasible to develop this information by laboratory tests. These tests and physics of failure analyses provide the necessary data to compute the best reliability estimate.
- d. Reliability predictions - Some data cannot be found within the regular data sources. Limited usage and lack of data can make precise calculations of failure rates impossible. This lack of information will require failure rate values to be estimated and each case must be handled individually. One aid in

making estimates of this kind is to obtain data for similar components operating in comparable environments and adjust the values accordingly. Estimates should be substantiated by laboratory tests or research into similar problem areas.

#### 60. NOTES

The following references were used in the preparation of this appendix.

- a. Nagle, P.M., "Importance Sampling in System Simulation," Annals of Reliability and Maintainability, Volume 5, Society of Automotive Engineers, New York, AIAA, 1966.
- b. Vesley, W. E., "Analysis of Fault Trees by Kinetic Tree Theory," IN-1330, Idaho Nuclear Corporation, Oct. 1969.
- c. Vesley, W. E., and Narum, R. E., "Prep and Kitt: Computer Codes for the Automatic Evaluation of a Fault Tree," IN-1349, Idaho Nuclear Corp., Aug 1970.

(This page intentionally left blank)

## APPENDIX C

### CABLE FAILURE MATRIX

#### 10. GENERAL

10.1 Purpose. The cable failure matrix is a shorthand method used to concisely represent many of the possible combinations of failures which can occur within the cable assembly and should prove to be a useful tool in executing the analysis for cable assemblies.

20. REFERENCED DOCUMENTS (Not applicable)

30. DEFINITIONS (Not applicable)

#### 40. GENERAL REQUIREMENTS

A cable assembly consists of one or more connectors and one or more wire bundles. In the example shown in figure 4, cable W107 has two 7-pin connectors and one wire bundle consisting of seven wires. There are three areas of failure matrices associated with this cable assembly, one area for each of two connectors are depicted as being identical, they have not been developed separately. In a more general case, the two connectors would not be identical, and a separate class of matrices would be required for each connector.

#### 50. DETAILED REQUIREMENTS

50.1 Connector fault modes. There are two major fault modes in which a short may occur within a connector: (1) 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 pin-to-pin shorts caused by bent pins. Pin-to-pin shorts from bent pins are considered adjacent only if the pin can directly bend to immediately adjacent pins or between adjacent pins to outer pins (see figure 5); (2) pin-to-case shorts, which can be caused by a bent pin. (This is shown in the matrix of figure 4 by case short (CS) designation).

50.2 Connector matrices. Connector matrices shall be developed for individual pin shorts caused by bent pins. These matrices will also include connector pin-to-case shorts caused by bent pins. Connector pins size 8 gauge or larger are not considered capable of bending over to contact another pin; but, the other pins, if less than size 8 gauge, are capable of bending over to the larger gauge pin. Connector matrices need not be developed for pin-to-pin shorts caused by foreign material. The following ground rules will be used in the development of a connector matrix:

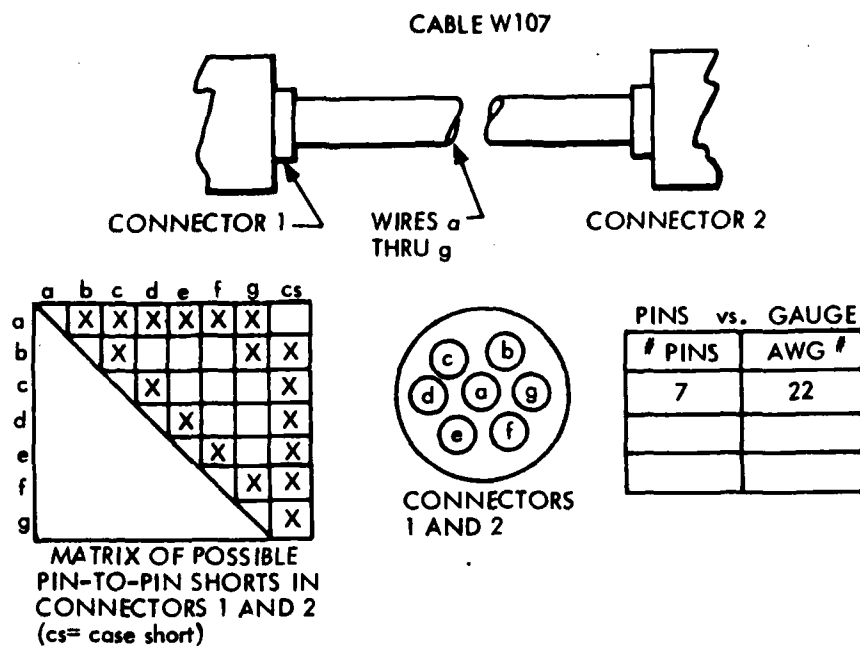


TABLE 1. CABLE ASSEMBLY W107		
COMPONENT	FAILURE MODE	FAILURE RATE
CONNECTORS 1 & 2 (NAS NO.)	PIN-TO-PIN SHORTS PIN-TO-CASE SHORTS	
CABLE W107	WIRE-TO-WIRE SHORTS WIRE-TO-SHIELD SHORTS OPEN WIRE FAULT	

Figure 4. Simplified cable failure matrix

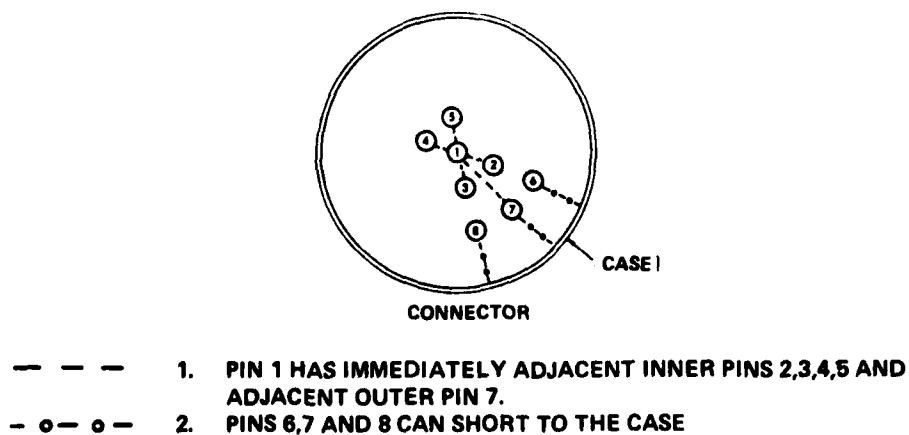


Figure 5. Connector pin short potentials

- a. Each connector matrix shall be contained on one drawing and will have the connector representation on that sheet.
- b. Nonconductive connector cases shall be noted on the matrix sheet.
- c. Pin-to-pin shorts shall consist of only geometrically possible faults that can occur from bent pins.
- d. To preclude constructing connector matrices more than once for a particular connector, a cross reference table of cable numbers and connectors shall be prepared (not illustrated). This will result in a summary of connectors that will provide an instant cross reference of like connectors for future use.

The case shown in figure 4 requires the development of one fault matrix for both connectors. The failure rates are the same for all pins in a specific failure mode. This data is entered in table 1 of figure 4. Note that all the possible combinations of shorts should be included in only the top half of the matrix.

50.3 Wire bundle fault modes. There are three major modes in which a fault can occur within a wire bundle. These are: (1) wire-to-wire shorts; (2) wire-to-shield shorts; (3) open wire faults. It is necessary that all combinations of failures be presented. Of course, if two wires do not run together in any section of the bundle, they need not be included. (figure 6 clearly illustrates this case.) It is assumed that a wire in a cable bundle can short to any other wire within that bundle. Each wire in the cable assembly should be identified and recorded (as in the table of figure 7). A brief description of the function of the wire, e.g., issue ordnance ignition discrete, 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 run list (see figure 8). The pin and connector assignments of both ends of the wire shall be placed in the From and To columns of the table in figure 7. The routing in a cable will be shown for branched cables to establish the possible wire-to-wire shorts. The wire type, size and shielding shall be noted in the last column. Available wire lists that specify this information will satisfy this requirement.

50.4 Additional considerations. Two more considerations must be made before the Cable Failure Matrix is complete: (1) if the wires within the cable are insulated by different materials or some of the wires are shielded (see figure 8), the potential of wire-to-wire shorts



will be different for the different combinations, and (2) if the pins within a connector are of different dimensions (figure 9), then the potential of different combinations of pin-to-pin shorts will be different. Both of these considerations must be made and noted whenever applicable for the validity of the analysis.

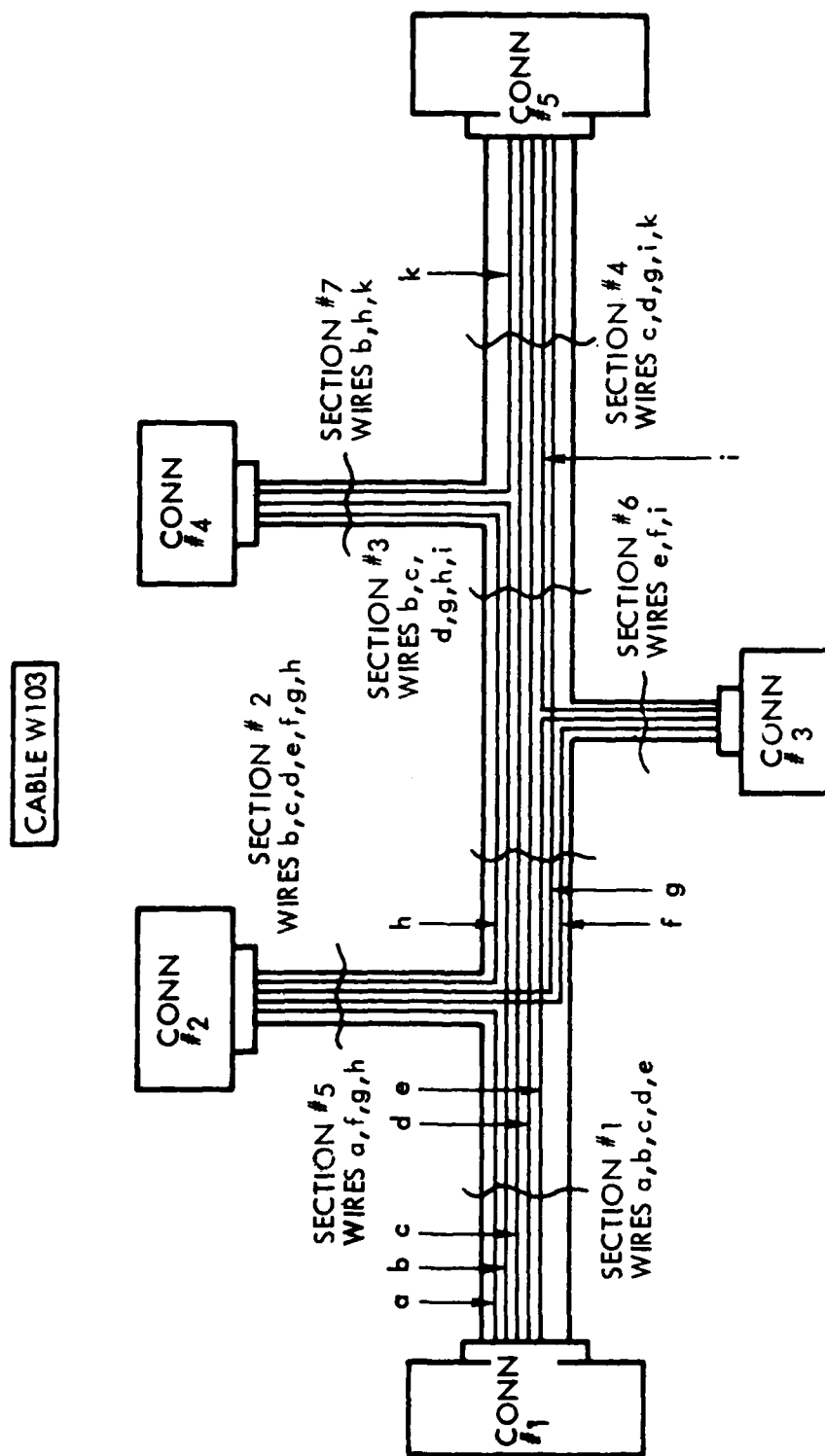












Figure 6. Multiconnector cable diagram

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	$\pm 28\text{vdc}$ $10\text{ma}$	CONN 2 PIN a	CONN 5 PIN i	5,2,3,4	 16 GA	SSC
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 7. Cable wire table

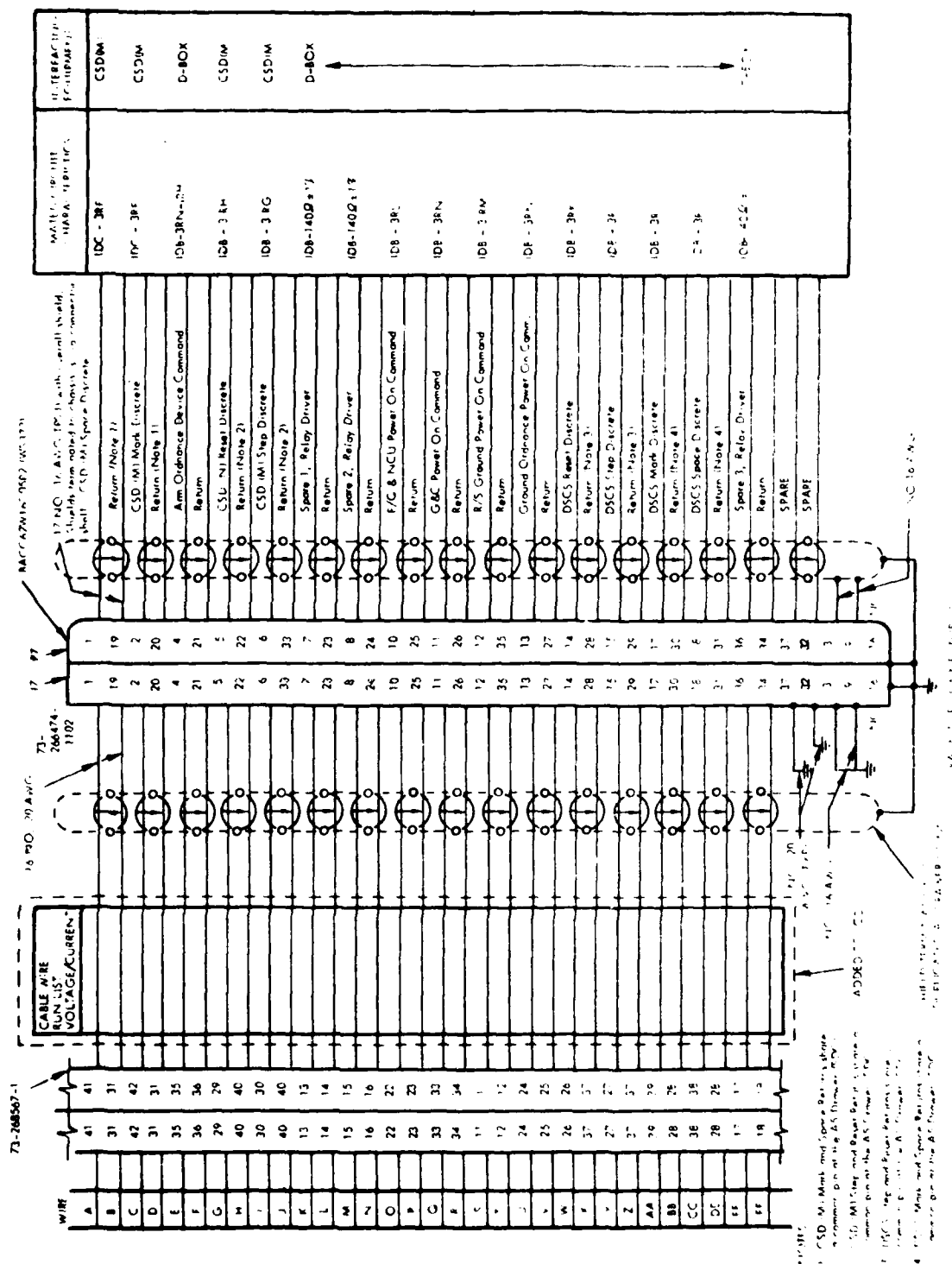


Figure 8. Modified interface control drawing (ICD) and cable wire run list

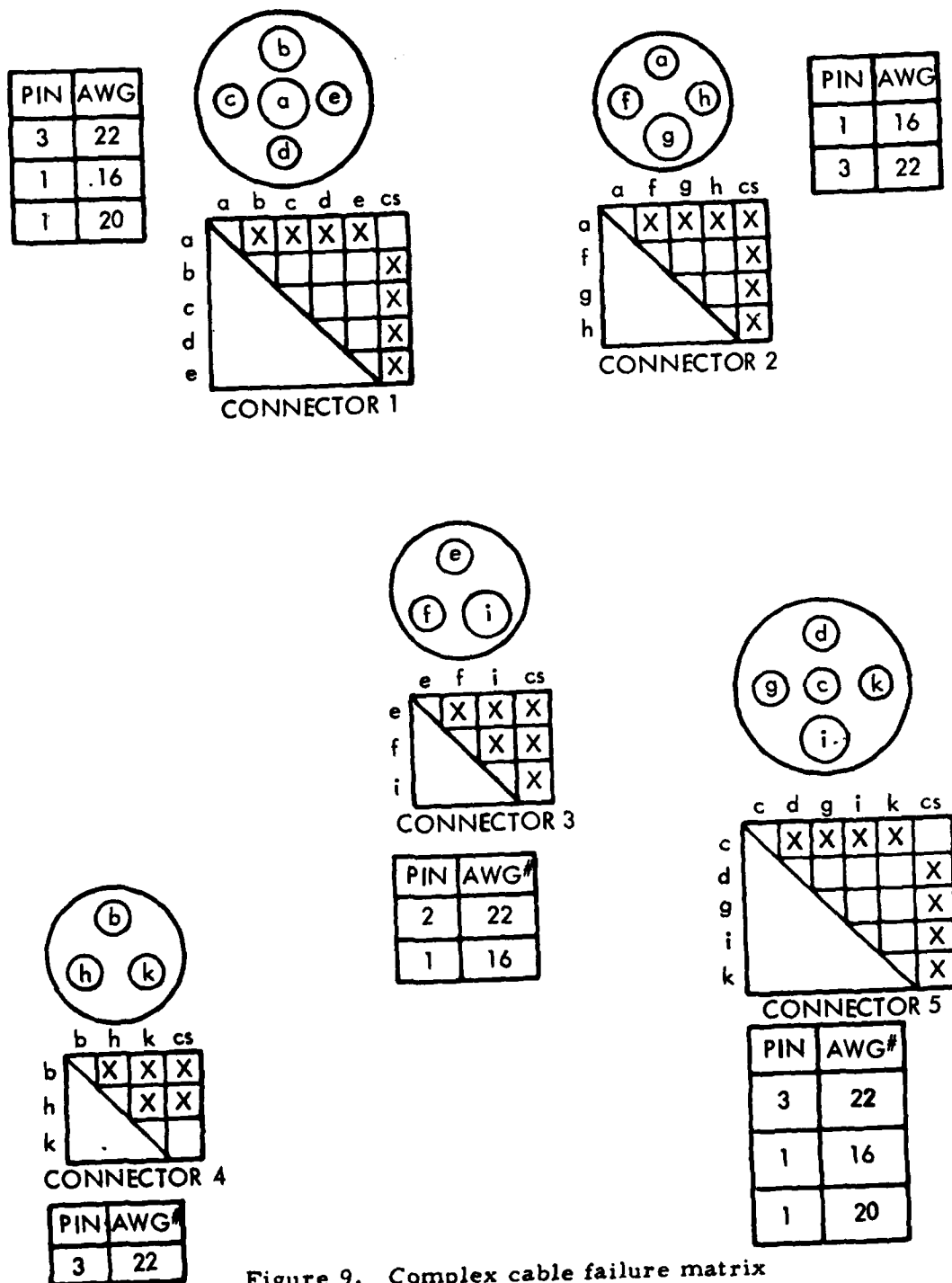


Figure 9. Complex cable failure matrix

## APPENDIX D

## SOFTWARE HAZARDOUS EFFECTS ANALYSIS

## 10. GENERAL

10.1 Purpose. The Software Hazardous Effects Analysis (SHEA) is performed to insure that potential hazards are identified during the software design such that appropriate design requirements can be derived to eliminate, control or minimize the hazards. All potential hazards will be identified to the SAIC for inclusion in weapon system level analysis.

## 20. REFERENCE DOCUMENTS:

AFR 122-10

Nuclear Weapon Systems Safety  
Design and Evaluation Criteria

## 30. DEFINITIONS (Not applicable)

## 40. GENERAL REQUIREMENTS

40.1 Nuclear Safety. The SHEA must identify hazards affecting the nuclear safety criteria of AFR 122-10, chapter 4.

40.2 Analysis approach. For purposes of this analysis, the software program and computer are considered an entity. Each function (e.g. a Command function) which affects system safety must be specifically analyzed in the SHEA. All functions of the program must be analyzed to determine their effect on the safety of the system. All legal program branches and transfers will be considered. Computer restarts during critical routines and one illegal computer skip (which can occur at any time) will also be considered in establishing what, if any, hazardous configurations may occur. The analysis will include:

- a. Internally, what modes the software may branch into, and
- b. What commands/loss of monitoring may occur externally at improper times.

Hazards occurring internally to the software system will be categorized in accordance with this standard. Effects of an error/malfunction at the output interface of the software system will be identified to the SAIC for hazard identification across the interface.

## 50. DETAILED REQUIREMENTS

50.1 Format. The format shown in figure 10, shall be used in performing the SHEA. The following paragraphs provide instructions in the use of this format by reference to column heading.

- 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) (see FHA) 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.

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

Figure 10. Software Hazardous Effects Analysis Format



FIL  
7