DTIC FILE COPY

Final Report
for the period
December 1983 to
June 1988

AFAL-TR-88-096

AD:

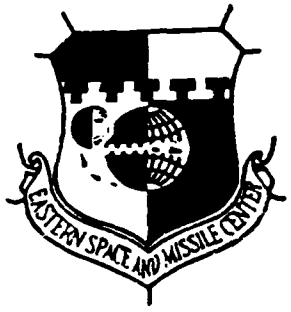
AD-A203 204

October 1988

Space Propulsion Hazards Analysis Manual (SPHAM)

Volume I







Authors:
D. C. Erdahl
D. W. Banning
E. D. Simon

Martin Marietta Corporation
Space Systems Company
P. O. Box 179
Denver, CO 80201

MCR-88-590
F04611-84-C-0003

Approved for Public Release

Distribution is unlimited. The AFAL Technical Services Office has reviewed this report, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

DTIC
ELECTE
DEC 1 9 1988
S D
E

Prepared for the:

Air Force Astronautics Laboratory

Air Force Space Technology Center
Space Division, Air Force Systems Command
Edwards Air Force Base,
California 93523-5000

88 12 19 103

NOTICE

When U.S. Government drawings, specifications, or other data are used for any purpose other than a definitely related Government procurement operation, the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise, or in any way licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may be related thereto.

FOREWORD

This is Volume 1 of the Space Propulsion Hazards Analysis Manual submitted by Martin Marietta Corporation on completion of contract F04611-84-C-0003 with the Air Force Astronautics Laboratory (AFAL), Edwards AFB, CA. AFAL Project Manager was John Marshall.

This report has been reviewed and is approved for release and distribution in accordance with the distribution statement on the cover and on the DD Form 1473.

JOHN W. MARSHALL
Project Manager

FRANCISCO Q. ROBERTO
Chief, Propellant Development Branch

FOR THE COMMANDER

DAIVD P. KING, Lt Col, USAF
Deputy Director
Propulsion Division

SECURITY CLASSIFICATION OF THIS PAGE

ADA203204

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S): MCR-88-590	5. MONITORING ORGANIZATION REPORT NUMBER(S): AFAL-TR-88-096
6a. NAME OF PERFORMING ORGANIZATION: Martin Marietta Corporation; 6b. OFFICE SYMBOL (If applicable):	7a. NAME OF MONITORING ORGANIZATION: Air Force Astronautics Laboratory
6c. ADDRESS (City, State, and ZIP Code): Space Systems Company, P. O. Box 179, Denver, CO 80201	7b. ADDRESS (City, State, and ZIP Code): AFAL/RKPL, Edwards Air Force Base, CA 93523-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION; 8b. OFFICE SYMBOL (If applicable):	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER: F04611-84-C-0003
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO	WORK UNIT ACCESSION NO.
62302F	5730	00	GM

11. TITLE (Include Security Classification): Space Propulsion Hazards Analysis Manual (SPHAM) (U)

12. PERSONAL AUTHOR(S): Erdahl, David C., Banning, Douglas W., and Simon, Elvis D.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Final	FROM 83/12 TO 88/6	88/10	499

16. SUPPLEMENTARY NOTATION: This is Volume 1 of a two volume report. This report was prepared under the technical guidance of the Eastern Space and Missile Center (ESMC) Patrick AFB FL

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP
21	08	

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number): Hazards, Hazards Analysis, Accident Scenarios, Post Accident Environments, Risk Assessment, Safety Program, Probability Modeling, Blast, Fragmentation, Acoustics, Thermal, Toxicity, Hazardous Materials

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Space Propulsion Hazards Analysis Manual (SPHAM) is a compilation of methods and data directed at hazards analysis and safety for space propulsion and associated vehicles, but broadly applicable to other environments and systems. It includes methods for compiling imposed requirements and deriving design requirements. It describes in detail the steps to constructing accident scenarios for formal risk assessment. It discusses the approaches to developing probabilities for events in scenarios, and probabilities for scenarios. It illustrates data analysis from experience data for the purpose of probability modeling. The SPHAM provides methods for predicting blast, fragmentation, thermal, acoustic and toxicity post-accident environments. The SPHAM describes in overview fashion a large number of qualitative and quantitative analytical methods available to perform hazards analysis complete with guidelines for application. Examples are FMEA, Fault-tree and Energy Analysis. It describes methods to organize analysis by type, phase, or subsystem. Examples are interface hazards analysis, preliminary hazards analysis, and ordnance hazards analysis. Qualitative and quantitative risk assessments are described. The formal processes for hazards analysis and safety for various

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☒ DTIC USERS	UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code)	22c. OFFICE SYMBOL
John W. Marshall	(805) 275-5642	RKPL

DD Form 1473, JUN 86 — Previous editions are obsolete. — SECURITY CLASSIFICATION OF THIS PAGE

Block 19 (continued): agencies and departments of the government and DOD are described. The appendices to SPHAM contain voluminous data on available references in the form of an annotated bibliography, summary of the hazardous nature of 27 commodities common to space propulsion, and system description for a variety of space launch vehicles, upper stage vehicles, and spacecraft. (AR)

Accession For	
NTIS GRA&I	X
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	



PREFACE

This Space Propulsion Hazards Analysis Manual was prepared by Martin Marietta Astronautics Group, Denver, Colorado, under contract F04611-84-C-0003. It was sponsored jointly by the Air Force and the National Aeronautics and Space Administration. Program management and contract administration were provided by the Air Force Astronautics Laboratory, Edwards Air Force Base, California. Technical direction was provided principally by both the Astronautics Laboratory and the Eastern Space and Missile Center, Patrick Air Force Base, Florida. The project manager was Mr. John W. Marshall, Air Force Astronautics Laboratory.

This manual is intended to be a source of information, methods and data useful to hazards analysis for space propulsion and space vehicles. It is not intended to be used as a regulatory document, nor is it to be construed as a complete, definitive and authoritative work.

The complete Space Propulsion Hazards Analysis Manual (SPHAM) consists of these two volumes that are bound separately to facilitate their handling and use as reference material:

Volume I SPHAM Technical Chapters
Volume II SPHAM Appendices

ACKNOWLEDGEMENTS

This manual reflects the work of many dedicated individuals from industry and government. We wish to give special recognition to those people whose contributions helped to make this manual a first of its kind:

Mr. Louis J. Ullian, ESMC, Patrick AFB, FL
Mr. John W. Marshall, AFAL, Edwards AFB, CA
Mr. Bill Riehl (retired), NASA-MSFC, Huntsville, AL
Mr. John Atkins, RTI, Cocoa Beach, FL
Mr. Robert Fletcher, NASA-JSC, Houston, TX
Mr. Tom Kerr (retired), NASA-HQS, Washington, DC
Mr. Wayne R. Frazier, NASA-HQS, Washington, DC
Mr. Bobby R. Quisenberry, GDC, San Diego, CA

We also wish to acknowledge the following people for their contributions as Martin Marietta employees:

Mr. Bob Lomax
Mr. Doug Banning
Ms Gloria Bradway
Ms Kate McCarthy
Mr. Rich Barthelow
Mr. Ed Kirk
Mr. Art Major
Mr. Joe Mangino

SPHAM Table of Contents

SPHAM TABLE OF CONTENTS

Chapter 1	- Introduction	Volume I
Chapter 2	- Requirements and the Hazards Analysis Process	Volume I
Chapter 3	- Accident Scenarios	Volume I
Chapter 4	- System Failure Probabilities	Volume I
Chapter 5	- Post Accident Environments	Volume I
Chapter 6	- Hazards Analysis Methods	Volume I
Chapter 7	- Risk Assessment	Volume I
Chapter 8	- Hazards Analysis and Safety Approval	Volume I
Chapter 9	- Index, Glossary, Acronyms and Conversion Factors . . .	Volume I
Appendix A	- Annotated Bibliography	Volume II
Appendix B	- Summary of Hazardous Materials	Volume II
Appendix C	- System Descriptions	Volume II

Chapter 1
Introduction

CHAPTER 1
INTRODUCTION

TABLE OF CONTENTS

Section	Title	Page
1.0	INTRODUCTION	1-1
1.1	Purpose	1-2
1.2	Scope	1-2
1.3	User Orientation	1-3
1.3.1	Accident/Loss Model	1-3
1.3.2	Hazards Analysis Program Elements	1-6
1.4	SPHAM Summary	1-9
1.5	User Guide	1-15

LIST OF FIGURES

Figure No.	Title	Page
1-1	Generic Accident and Loss Model	1-16
1-2	Accident Model - Independent Failures	1-17
1-3	Accident Model - Common Cause	1-18
1-4	Accident and Loss Scenario - Hazards Analysis Model	1-19

LIST OF TABLES

Table No.	Title	Page
1-1	Appendix C Vehicles	1-14
1-2	SPHAM Roadmap to Major Topics	1-15

CHAPTER 1
SPHAM INTRODUCTION

1.0 INTRODUCTION

The Space Propulsion Hazards Analysis Manual (SPHAM) has been developed under contract F04611-84-C-0003 with the Air Force Rocket Propulsion (now Astronautics) Laboratory, Edwards Air Force Base. The project was jointly sponsored by the Air Force and NASA. The major tasks completed during the project were:

Phase 1

Task 1A - Conduct Literature Search and Field Survey

Task 1B - Prepare Comprehensive Annotated Bibliography

Phase 2

Task 2A - Review Analysis Protocols; Prepare Technical Report and Synoptic Outline

Task 2B - Prepare Final Synoptic Outline and Revised Program Plan

Phase 3

Task 3A - Develop SPHAM Initial Draft

Task 3B - Develop SPHAM Final Draft

Phase 4

Task 4A - Prepare Final Camera Ready SPHAM

Task 4B - Prepare SPHAM Presentations and Deficiencies/Limitations Report

Task 4C - Prepare SPHAM Electronic Record

1.1 PURPOSE

The purpose of SPHAM is to provide a single comprehensive source of available methods and data useful for hazard analysis in space propulsion applications. A related objective is to identify specific areas where the available methods and data applicable to space propulsion are deficient, so that directed efforts can be made to improve them. Ideally those efforts would result in a SPHAM update.

The principal function of SPHAM is to serve as a reference for system safety practitioners, as well as other individuals or agencies dealing with hazardous material or subsystems. The SPHAM may also be used as a source of contractual requirements for hazards analysis. It is intended for use by agencies and representatives of the DOD, NASA and aerospace contractors for both existing and future space vehicle programs. However, SPHAM does have utility for non-space and non-flight systems. As a result, the SPHAM may have the effect of standardizing DOD and NASA safety program elements and methods.

1.2 SCOPE

The scope of SPHAM includes methods and data of the annotated bibliography and other references which are applicable or otherwise useful to hazards analysis in the space propusion hazards environment. Methods include:

(1) Analytical techniques (qualitative and quantitative) to identify and assess hazards and their controls.
(2) Methods to organize analysis, such as by program phase or by subsystem.
(3) Methods to document and report analysis data.
(4) Examples which are illustrative of the methods.

Hazards analysis data includes:

(1) System and subsystem data for existing vehicles.
(2) Hazards analysis data for existing systems and subsystems
(3) Data for specific hazards which can be anticipated for the space propulsion environment, including hazardous materials.

The scope of SPHAM also includes assessments of the methods and data and application recommendations or guidelines.

The scope of this initial SPHAM excludes new data and methods. It would be appropriate for later versions of SPHAM to incorporate methods and data developed for SPHAM to eliminate current deficiencies (see Technical Report - Deficiencies and Limitations).

1.3 USER ORIENTATION

The principle purpose of this Introduction is to orient the user of SPHAM to the methods and data presented in the manual, in a manner most aligned with his potential needs. Section 1.3.1 establishes a generalized model or convention for the key events and condition involved in an accident. Ideally the elements of a Hazards Analysis Program, the purpose of which is to control accident risk, are directed at identifying, assessing, and controlling those key events and conditions. Section 1.3.2 therefore, is intended to orient the user to key elements or functions of a Hazards Analysis Program. Section 1.4 provides a brief summary of the purpose and content of each chapter of SPHAM. These sections lead to the users Guide of Section 1.5 which provides traceability to the Chapters of SPHAM by the topics developed in this section.

1.3.1 Accident/Loss Model

The data and methods of the Annotated Bibliography items which form the SPHAM data base do not adhere to a uniform convention for the meanings of terms. The term "hazard," for example is often used to mean a functional failure mode, an accident, a source of energy or toxicity, an environment created by an accident such as fire, etc. "Hazard risk," although a meaningless term, is often used in place of "accident risk" or "expected loss." In addition, the literature does not present their data and methods in a common framework or convention representing the sequence and relationship of events and conditions which lead to an accident and result in a loss. An example is the distinction between the accident and the consequence of the accident, or loss. Accident consequence is generally used only as a means to categorize the threat presented by a hazard, i.e., its severity. As a result, there is little distinction made between hazard control functions or margins which reduce the risk of an accident and those which reduce the effects of an accident. The lack of an accepted convention may not present difficulty to individual users of selected references who are very familiar with the parochial convention within. It is a potentially major difficulty for the user of the compiled data and methods of SPHAM (see Technical Report - Deficiencies and Limitations).

The organization, content (methods and data) and use of the SPHAM derive in part from the events and conditions that lead to an accident and result in a loss. A summary of the accident and loss model used to develop SPHAM, along with the definitions of key terms, are presented as an aid to the user of SPHAM. The conventions presented here and elsewhere in the manual are arbitrary in that they are not consistent with those of any one reference in the SPHAM data base. First order of precedence was given to those both available and adequate from military and government documents (e.g., Mil-Std-882B, Mil-Std-1574A). Second order of precedence was given to most common usage.

An effort was made to "fit" the methods and data extracted from the references and incorporated into SPHAM to the conventions summarized here. Completion of this effort is outside the scope of this version of SPHAM (see Technical Report - Deficiencies and Limitations).

For the purposes of SPHAM it is presumed that accidents are caused by:

(1) The loss of a human, hardware or software function (or functions performed outside of tolerance) which results in the loss of control of a hazard existent in the system.

(2) An unplanned human action within the system which creates an uncontrolled hazard, defeats the control of an existing hazard or subjects the system to operation or environment outside of limits.

(3) An unplanned event in the environment of the system, e.g. the release of a natural hazard, another accident, etc.

Figure 1-1 is a generalized model of the SPHAM convention for the events of (1) and their sequence and relationship that can lead to an accident and result in a loss. Key definitions pertaining to this model are as follows:

Failure Mode - A unique hardware, software or human malfunction, which constitutes loss of function or functional performance outside of specified limits.

Failure Mode Cause - The immediate or accumulated hardware, software or human state(s) or action(s) which leads directly to or precipitates a failure mode.

Failure Mode Effect - The state(s) or event(s) within the boundaries of the system which result directly or indirectly from the occurrence and propogation of a failure mode.

Local -	The immediate or initial effect.
Intermediate -	The effect propagated from the local effect.
System -	The highest, last or end effect within the boundaries of the system.

Hazard - A source toxicity, energy, or incompatibility which must be controlled in order to preclude major injury, death or other loss exceeding prescribed limits.

Hazard Control Function - A hardware, human or software function the purpose of which is to control a hazard.

Event - The occurrence or realization of any definable, distinct state or condition of interest of a system or its environment within its boundaries.

Accident - An unplanned event which results directly in damage and loss to the system and/or to the environment of the system and which is caused by an uncontrolled hazard.

System Damage - Death, major injury, equipment or property damage beyond prescribed limits within the boundaries of the system.

Environmental Damage - Death, major injury, equipment or property damage beyond prescribed limits to the environment of the system outside the boundaries of the system.

Major Injury - Any injury which results in admission to a hospital and prolonged treatment such as a bone fracture, second or third degree burns, severe lacerations, internal injury, severe radiation exposure, chemical or physical agent toxic exposure or unconsciousness.

Accident Loss - The total death, major injury, equipment or property damage beyond prescribed limits from damage to the system and/or its environment that results directly from the occurrence of an accident.

Program Loss - The total loss to a program which results from a single accident, such as the cost of schedule modification, lost security, etc.

The accident model of Figure 1-2 is a variation from Figure 1-1. In this model two independent failures are necessary to precipitate the accident, one failure propagating to the system level in combination with a second failure propagating to the subsystem level. An example is the high velocity impact of a launch vehicle loaded with liquid bipropellant resulting from (1) loss of flight control, and (2) loss of the range safety destruct subsystem function.

The accident model of Figure 1-3 is one of particular concern in hazards analysis, the accident resulting from multiple failures which have a common cause.

The accident and loss scenario model of Figure 1-4 and the definitions which follow represent the SPHAM convention for the meaning, sequence and relationship of the events and conditions used to model an accident and loss for the purpose of hazard analysis identification, control and control of hazards. The definition of new terms is as follows.

Scenario - A unique set of events and conditions leading to and including an event of interest.

Accident Scenario - Any scenario leading to and including a defined accident.

Loss Scenario - Any scenario leading to and including a defined loss.

Post-Accident Environment - The conditions (e.g., blast, thermal, radioactive, fragmentation, toxicity) resulting from the accident which, in part or in total, cause the damage to the system and/or its environment and the accident loss.

For the purpose of hazard analysis, the accident and the environment of the system at the occurrence of the accident from the model of Figure 1-4 are generally postulated. Unique sequences of events leading to the accident are deduced to form accident scenarios. The definitions of accident and system environment lead to predictions of the post-accident environment (e.g., toxicity, thermal) which leads in turn to prediction of damage to the system and its environment and loss from the accident.

Accident risk and expected loss are significant measures of risk of retaining an identified hazard in the system. Accident risk is the probability that the accident of interest will occur on one mission of the system. Expected loss (accident loss) is generally the predicted loss from the accident multiplied by the accident risk. Program accident risk is the probability that the accident of interest will occur in the life of a program, and expected program loss is the predicted loss from one accident multiplied by the program accident risk.

1.3.2 Hazards Analysis Program Elements

The organization, content and use of the SPHAM derive not only from the events and conditions that lead to an accident and result in a loss, but also from the functions and activities of the hazards analysis program. The overall purpose of a hazards analysis program is to ensure that the risk of an accident and the resulting loss are managed to acceptable levels. The specific objectives of the hazard analysis program are, in order of precedence:

(1) To preclude or eliminate those hazards which unnecessarily or unacceptably compromise the system design or operations concepts.

(2) To verify or incorporate adequate control of hazards where hazards necessarily exist in the system design or operations concept.

(3) To verify or establish adequate control of potential loss from credible accidents.

(4) Coordinate the functions and maintain the data necessary for risk management.

The Hazards Analyses Program elements are not totally distinct in that they are overlapping and iterative in nature. As well, not all elements are found in individual programs due to the nature of those programs. These elements can be summarized as follows:

(1) Develop Hazard Compliance Requirements - Associated with each program are the known or anticipated requirements for hazard avoidance, minimum control of hazards, and loss prevention or mitigation. The objective of this element is to compile the requirements in a useful and manageable format to guide or direct the design effort up-front to ensure that the requirements are met or accommodated early. The checklist is a common format for the compilation of program requirements. The checklist format provides traceability to the detailed requirements of the program compliance documents and enables early compliance definition from the responsible project personnel.

(2) Develop Hazard Design Criteria and Derived Requirements - In the view of experienced safety practitioners, program compliance requirements do not (and probably cannot) adequately constrain or guide the design effort up front such that the hazard avoidance and control objectives are met. Safety design criteria and derived requirements are often developed to supplement the program requirements. These criteria anticipate hazards which may appear in the system

design or operations concept as it evolves, and defines potential alternatives and minimum controls for the anticipated hazards and other measures and features to mitigate loss from an accident. The Preliminary Hazards Analysis (PHA) is often the means used to develop criteria where it is imposed as a safety program task requirement.

(3) Identify Existing Hazards and Control - Following the initial effort to guide the design to avoid hazards where possible and to implement adequate control, the system, subsystem, component and operational designs are analyzed to:

(a) Define the hazards which exist in the concepts or designs.

(b) Determine the measures and features which exist in the concepts or design to maintain control of the identified hazard and to prevent or mitigate the loss which may result from loss of control of the hazard.

(c) Identify additional or alternative measures to the design effort where the need or opportunity exists.

The early compilation of requirements and criteria form the principal basis for this evaluation of the design. Experienced practitioners, however, indicate that a significant number of hazards of concern identified during the detailed evaluation of the design were not covered by the earlier requirements and criteria.

(4) Verify Compliance to Requirements/Criteria - Although somewhat inherent in the effort to identify and evaluate hazards and their control, the verification of compliance to program requirements and criteria is an essential element. Compliance verification establishes the status of compliance of the system and operations design to all known requirements and criteria. It is also the first risk assessment "gate," since all hazards and their controls which have met the requirements and criteria are presumed to have an acceptable associated accident risk. The result of compliance verification also forms an important basis for the final assessment of overall program risk.

Those hazards-of-concern and their associated controls which later attract increasingly greater attention and more detailed analysis are predominantly those which do not comply with program requirements and criteria, or those which were not covered or constrained by the requirements.

(5) Develop Accident Scenarios - Accident scenarios are formally developed to:

(a) Establish and reach consensus on the credibility of an accident and the necessary or possible events leading to an accident.

(b) Provide a basis to analytically define and test the effectiveness of hazard controls.

(c) Provide the definition of events for which qualitative and quantitative probabilities can be developed and accident risk assessed.

(d) Provides the basis for the definition of the possible system environments for post-accident environment and loss predictions.

The development of accident scenarios is critical to sound program decision to accept risk.

(6) Predict Post-Accident Environment - Formal predictions of post-accident environment are often not included or developed for the assessments of risk and loss. Where used post-accident environment prediction:

(a) Verifies that the conditions necessary for the release or realization of a hazardous material or condition are met.

(b) Establishes the nature and magnitude of those effects of an accident which threaten the system and its environment. Examples of these conditions are blast, thermal effects, fragmentation, toxicity, etc.

(c) Provides the basis for assessing the potential damage and loss resulting from an accident.

Although the post-accident environment predictions are quantitative and often straightforward, they are often not developed because worst-case effects from accidents are assumed and because of the difficulty in assessing loss from the post-accident environment.

(7) Assess Accident Risk and Loss - Accident risk is a common measure of acceptability of a hazard and its associated control(s). Formal assessments of accident risk and loss are normally done only for those few identified hazards and accident scenarios which elude successful implementation of corrective action and remain a hazard of concern. These assessments can be qualitative or quantitative in nature, and together with the design trade study data and the risk acceptance criteria form the substantiation for major program decisions. It should always be understood that managing accident risk to acceptable levels is the purpose of a hazards analysis program.

(8) Coordinate Review and Disposition - Successful management of accident risk and therefore risk to the program is contingent on (1) visibility to the essential data and analysis developed to support the concern or acceptance for a hazard and potential accidents, (2) the involvement of all affected procurement and contractor personnel, and (3) adequate time to evaluate risk and make changes where necessary. The purpose of this element of a hazards analysis program is to ensure that these factors are satisfied.

1.4 SPHAM SUMMARY

Chapter 2.0, Requirements and the Hazards Analysis Process, discusses the topics of requirements in hazards analysis (i.e., requirements which implement hazards analysis, imposed compliance requirements for hazard avoidance and control, and derived requirements) and the hazard analysis process. These topics are inseparable and are integrated in the discussion.

The purpose of Chapter 2 is to establish the purpose, objective and general nature of the hazard analysis process and to establish it's relationship to the overall System Requirements effort. The specific element discussed include:

(1) Responsibility, authority and requirements to implement hazards analysis.
(2) Preliminary hazards analysis
(3) System/Safety Checklist
(4) System, Subsystem and operational hazards analysis
(5) Hazard cataloging and reporting
(6) Hazard Analysis by development phase

Chapter 3, Failure Scenarios, provides a summary of post-accident environment considerations for solid and liquid propellants as they relate to types of accidents, such as High Velocity Impact (HVI) and Confined By Ground Surface (CBGS). Chapter 3 includes a general discussion of Flight Termination Systems (FTS). This discussion establishes time-to-function and inability-to-function as necessary considerations in developing accident scenarios. Chapter 3 describes and illustrates the development of accident definitions as a key pre-requisite to credible accident scenarios. It illustrates the derivation of accident definitions from the risk assessment goal. Establishing the risk assessment goal and deriving accident definitions are the initial steps in developing accident scenarios. The steps in developing accident scenarios are described as follows:

(1) Establish or verify the Risk Assessment Goal.
(2) Develop Accident Definitions
(3) Identify Triggering Events
(4) Assess possible Accidents
(5) Identify Triggering event causes
(6) Review FMEA/Fault-Tree Data

Chapter 3 also includes several analytical scenarios developed for an expendable launch vehicle for the in-flight phase.

The date of Chapter 3 is intended to be used to aid development of analytical accident scenarios for formal risk assessment. It is not intended to constrain the less rigorous informal accident scenario normally considered during the course of hazard identification and control assessment.

Chapter 4, System Failure Probabilities, provides methods and data to quantify the probabilities of scenario events and the purpose of Chapter 4 is to provide means to develop quantitative assessments for use in risk assessment scenario end events. Chapter 4 discusses discretely the process of:

(1) Developing probability models and probabilities for individual events in a scenario (scenario events), and

(2) Modeling the probability of the scenario end event (usually an accident).

Included in (1) is a treatment of the analysis of historical data. Emphasis is placed on the importance of applying historical experience to the development of probabilities for scenario events. The use of weibull for this purpose is illustrated. Empirical system failure probabilities for Program 624A, and analytical system failure probability results from the J. H. Wiggins Co. for the STS are presented. These data are limited in applicability to existing and new programs due to the age of the data for Program 624 and the optimistic methods used by J. H. Wiggins for the STS. The STS system failure events discussed include:

Liftoff through MECO

1. Tipover on Pad
2. Loss of Control/Tumble
3. Inadvertent Separation, SRB/ET Aft Attachment
4. Inadvertent Separation, SRB/ET Forward Attachment
5. Corkscrew (SRB TVC Failure)
6. ET Punctured
7. ET Intertank/LOX Tank Failure
8. SRB Recontact at Separation
9. Loss of ME Propulsion

MECO through Payload Separation

10. ET Punctured
11. Loss of Maneuverability Orbiter Tumbles
12. Loss of Maneuverability Orbit Decay
13. ME Fire/Explosion

Many quantitative methods to evaluate system failure probabilities rely on component and failure mode probability data. For this reason Chapter 4 includes component and known reliability data derived from the WASH-1400 Reactor Study.

The system failure events of Chapter 4 do not correspond with the failure scenarios of Chapter 3. This is because of vehicle differences and limitations of the data.

The data and methodology of Chapter 4 can be used principally to determine probability or risk of system level events of interest where the hardware or human failure modes and effects can be determined.

Chapter 5 presents and discusses data bases, data and methods for predicting the post-accident environments of

1. Blast (Overpressure)
2. Fragmentation
3. Thermal/Fire
4. Toxicity
5. Acoustics

where emphasis is given to those environments associated with complete destruction of the vehicle. A principal conclusion of Chapter 5.0 is post-accident environments can be reasonably well defined, but more work must be done in certain areas, principally fragmentation and solid propellant fire and thermal effects.

Stepwise blast determination procedures are provided for LO_2/LH_2, LO_2/RP-1, and hypergolic (A-50/N_2O_4 and MMH/N_2O_4) liquid propellants and class 1.3 solid propellants for different failure scenarios. Similarly stepwise procedures are provided to evaluate the critical parameters of a solid or liquid propellant fireball. the release and concentration of toxic chemicals, and acoustic power levels mainly in large rocket motors. Chapter 5 can be used as a source or source reference for data and procedures to evaluate the consequence of mishaps or failure scenarios defined by the hazards analysis methods and data of Chapters 3, 4 and 6.

Chapter 6 provides detailed discussion and guidelines for application for many important methods to identify and assess hazards. These include:

<u>Qualitative</u>

1. Change Analysis
2. Contingency Analysis
3. Critical Incident Technique
4. Criticality Analysis
5. Energy Analysis
6. Flow Analysis
7. Interface Analysis
8. Job Safety Analysis
9. Maximum Credible Accident
10. Naked Man
11. Operational Hazards Analysis
12. Preliminary Hazards Analysis
13. Prototyping
14. Scenario Brainstorming
15. Software Safety
16. Subsystem Hazard Analysis
17. Systematic Inspection

<u>Quantitative</u>

18. Cable Failure Matrix Analysis
19. Event Tree
20. Failure Modes and Effects Analysis
21. Fault Tree Analysis
22. Management Oversight/Risk Tree Analysis
23. Network Logic Analysis
24. Pin Fault/Pin Short Analysis
25. Sneak Circuit Analysis
26. Statistical Analysis

In addition to the analytical methods, Chapter 6 discusses methods which pertain to specific types of hazards, or hazardous subsystems. Examples are propellants, pressure, RF, radiation, etc.

To illustrate methods and reporting, and to provide data on generic space vehicle hazards, hazard causes, controls, and verification methods, Chapter 6 also includes twelve hazard reports for generic hazards associated with typical space vehicle subsystems. These are applicable to STS payloads only

Chapter 7, Risk Assessment, presents alternative (qualitative and quantitative) methods to assess the mishap risk (probability of occurrence) and cost risk associated with identified hazards. Chapter 6 describes and illustrates methods to establish risk acceptability criteria. The emphasis of Chapter 7 is first the identification and control of risk factors, and the subsequent assessment of risk level for decision-making. An important conclusion of Chapter 7 is that risk acceptability is strictly program-unique and is driven by mishap effect on program cost, schedule, personnel injury, and system loss/damage. Chapter 7 can be used as a source of guidelines for defining and managing the program risks associated with the hazards identified in the course of the overall safety program.

Chapter 8, Hazard Analysis Approval, summarizes and contrasts the technical and administrative approaches of DOD, USAF, NASA, INSRP and the National Ranges in implementing, monitoring and approving the safety program elements and products for space programs. Key guideline documents include:

(1)	Mil-Std-822B	- DOD
(2)	Mil-Std-1574A	- USAF
(3)	SRD-127-4	- USAF
(4)	NHB 1700.7A	- NASA
(5)	SAMTO HB S-100/KHB 17007	- NASA/USAF
(6)	JSC 13830A	- NASA
(7)	ESMCR, WSMCR 127-1	- ESMC, WSMC

Chapter 8 also clarifies the authority of the Range Commander for safety of systems and operations which will utilize a National Range.

Chapter 8 can be used as a source or source reference to alternative approaches to implementing the hazards analysis process and managing the accuracy and completeness of results.

Chapter 9, Index, Glossary, Acronyms and Conversion Factors provides a detailed topical reference to SPHAM excluding the appendixes. The Index is detailed covering major and minor topics. The Glossary establishes uniform definitions for key terms used in SPHAM. Inconsistencies may exist between the glossary definitions and the use of the terms in SPHAM where they were derived from the reference literature. A list of acronyms and a table of conversion factors are included in Chapter 9.

Appendix A, Annotated Bibliography identifies the 457 technical reports, manuals, texts, etc., which were reviewed and assessed for appropriate data and methods for SPHAM. The bibliography summarizes the major topic of each bibliography item, identifies hazardous materials discussed in each item, identifies specific principal failure scenarios and post-accident environments included in each item, and identifies the principal methodologies as qualitative or quantitative. Where known, the Annotated Bibliography also identifies the current source of the reference. References to the Annotated Bibliography items within SPHAM are made by Annotated Bibliography reference number.

Appendix B, Summary of Hazardous Materials, identifies the physical and hazardous properties of common propulsion and other hazardous materials in space vehicle applications. It also summarizes accepted storage, handling, transportation, transfer and operational practice for those materials. They include ammonia, high-pressure gaseous nitrogen and helium (5000 psig), liquid helium, mercury, carbon dioxide, carbon monoxide, Freons, hydrazine, liquid hydrogen, hydrogen peroxide, liquid fluorine, nitrogen tetroxide, monomethylhydrazine, liquid methane, nitrogen trifluoride, liquid oxygen, solid propellants (classification 1.1 or 1.3), and radioisotope thermoelectric generators used for the Galileo mission.

Appendix C, System Description and Mission Scenarios, provides physical and functional descriptions of the launch vehicles, upper stage and satellite vehicles identified in Table 1-1. The descriptions include system, subsystem, operations and mission data. The vehicle descriptions highlight hazardous materials and conditions, design and operational features to control or mitigate known hazards and potential failure modes of particular interest to each vehicle. The data can be used as a source for known space propulsion hazard conditions and controls, or as supporting information for the more detailed discussions of hazards, failure modes, and failure scenarios of subsequent chapters of SPHAM.

Table 1-1 Appendix C Vehicles

Launch Vehicles

- Space Transportation System
- Titan T34D
- Atlas F (HGM16F)
- Atlas/Centaur
- Delta
- Titan II
- Scout
- Titan IV

Upper Stage Vehicles

- Centaur G-Prime
- Inertial Upper Stage (IUS)
- Minuteman II (Stages 1 and 2) Motors
- Orbit Transfer Vehicle (OTV)
- Payload Assist Module - Delta (PAM-d)
- Transtage

Satellite Vehicles

- Defense Satellite Communications Systems (DSCS)
- Defense Systems Program (DSP)
- Global Positioning System (GPS)
- Multi-Mission Modular Spacecraft (MMS)
- Tracking and Data Relay Satellite (TDRS)
- P80-1 (Ion Engine)
- Galileo Spacecraft
- Ulysses Spacecraft

1.5 USER GUIDE

The data incorporated into the SPHAM includes both hazards analysis methods and hazards analysis data. The data presented serves both to illustrate the methods and to provide reference data useful for hazards analysis of new and existing systems. Table 1-2 provides a user roadmap to the data and methods of SPHAM for the principal topics developed in Section 1.3.

Table 1-2 SPHAM Roadmap to Major Topics

Hazard Analysis Topics	Methods Capter	Data Chapter
1. Hazards	6	6, Appendix C
2. Failure Modes, Causes, Effects	3,6	3, Appendix C
3. Accident Scenarios	3,6	3
4. Post-Accident Environments	5	5, Appendix B
5. Loss (Damage)	4,7,3	3
6. System Environments	Appendix C	Appendix C
7. Accident Risk Assessment	4,7	7
8. Accident Risk Acceptance Criteria	7	7
9. Requirements	2	2
10. Criteria	2	2
11. Hazard Identification Assessment	6	6, Appendix C
12. Hazard Control	2,6	6, Appendix C
13. Hazard Reporting	6,2	6
14. Data Maintenance	2,6	2,6
15. Review/Approval	2,8	8
16. Hazardous Materials	Appendix B	Appendix B

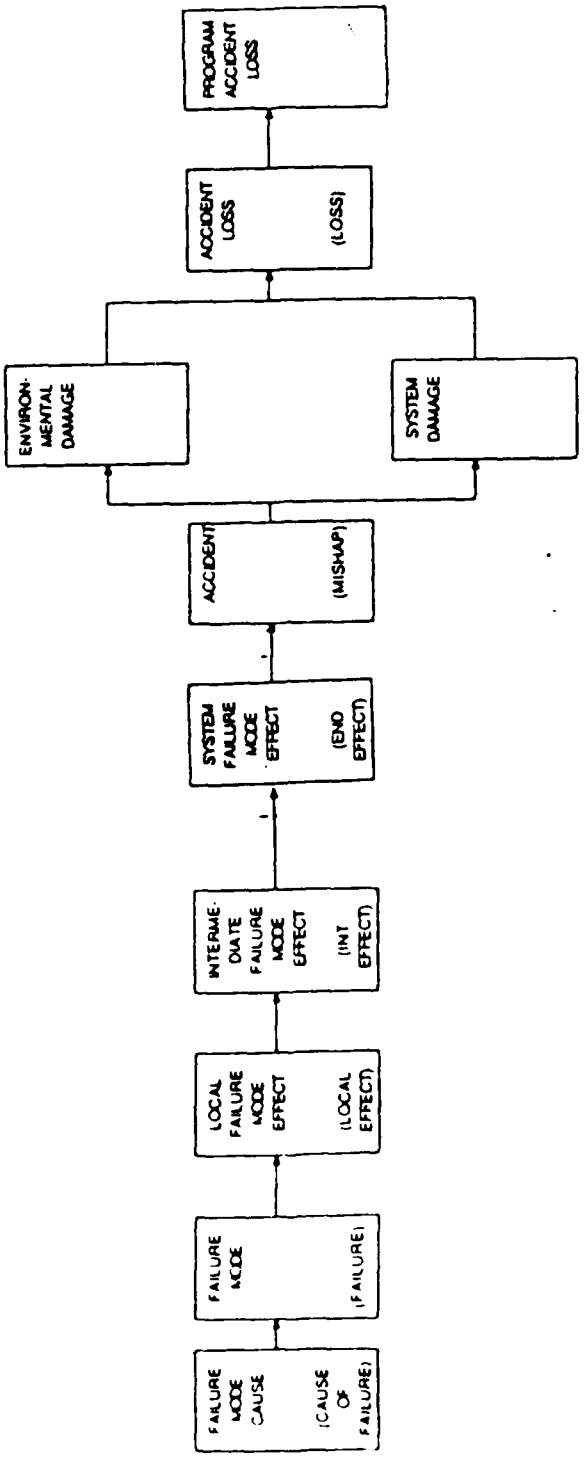


Figure 1-1 Generic Accident and Loss Model

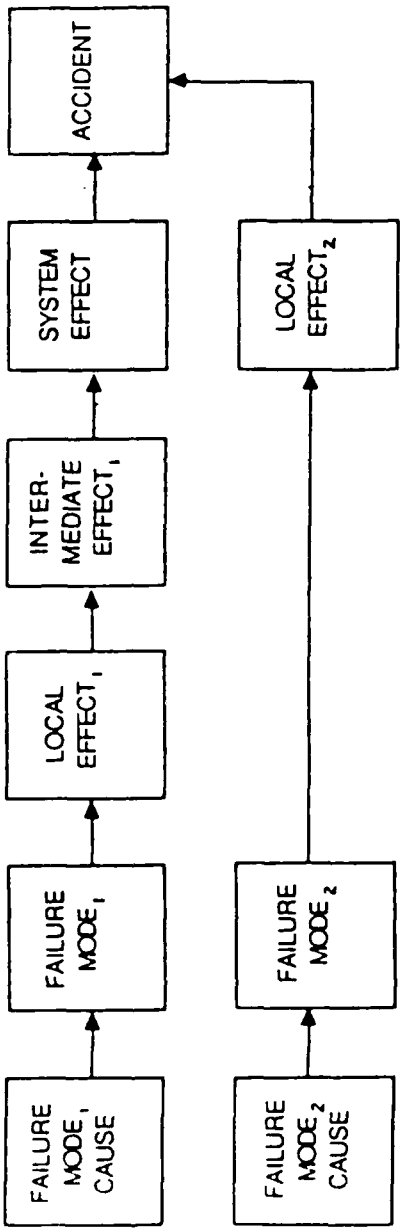


Figure 1-2 Accident Model Independent Failures

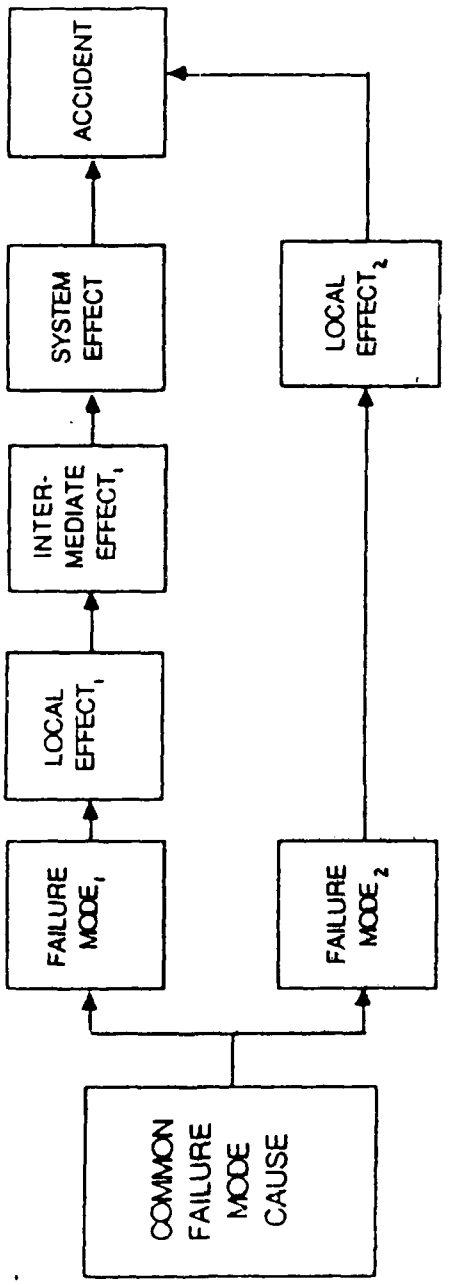


Figure 1-3 Accident Model - Common Cause

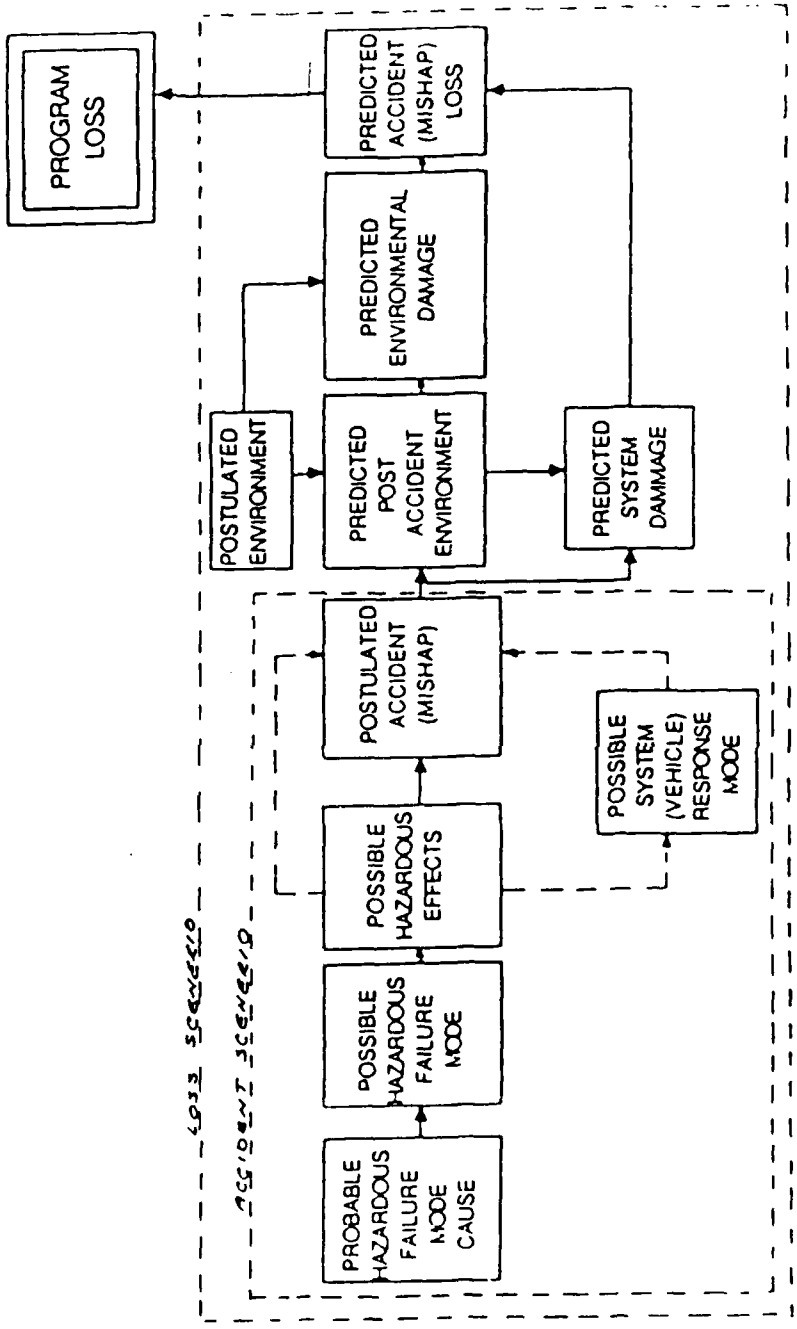


Figure 1-4 Accident/Loss Scenarios

Chapter 2
Requirements and the Hazards Analysis Process

CHAPTER 2
REQUIREMENTS AND THE HAZARDS ANALYSIS PROCESS

TABLE OF CONTENTS

Section	Title	Page
2.0	Introduction	2-1
2.1	Implementing Hazards Analysis	2-1
2.2	The Hazards Analysis Process	2-2
2.2.1	Hazards Analysis Objectives	2-3
2.2.2	Hazards Analysis Responsibilities	2-4
2.3	Hazards Analyses Approach	2-5
2.3.1	Preliminary Hazards Analysis	2-6
2.3.2	System Safety Checklist	2-8
2.3.	Accident Risk Analysis/Assessment	2-8
2.3.3.1	Subsystem Hazard Analysis	2-9
2.3.3.2	System Hazard Analysis	2-10
2.3.3.3	Interface Hazard Analysis	2-14
2.3.3.4	Operating and Support Hazard Analysis	2-15
2.4	Instructions - Hazard Analysis Documenation	2-18
2.4.1	Hazard Analysis Sheets	2-18
2.4.2	System Safety Checklist	2-21
2.4.3	Hazard Catalog	2-28
2.4.4	Hazard Analysis Report	2-29
2.4.4.1	Identifying/Classifying/Describing Hazards	2-30
2.4.4.2	Identifying/Potential Causes	2-30
2.4.4.3	Propose/Track Controls	2-31
2.4.4.4	Verifying/Finalizing Controls	2-31
2.4.4.5	References and Resolution	2-32
2.5	Project Interfaces	2-32
2.6	Program Phases and Tasks	2-35
2.6.1	Conceptual	2-35
2.6.2	System Definition	2-36
2.6.3	System Development	2-37
2.6.4	Manufacture/Test	2-38
2.6.5	System Use	2-39
2.7	Summary of Accident/Risk Assessment in Requirement Definition	2-39
2.8	References	2-44

LIST OF FIGURES

Figure No.	Title	Page
2-1	The Hazards Analysis Process	2-45
2-2	The Hazards Analysis Flow	2-46
2-3	Hazard Identification Checklist (Page 1)	2-47
	Hazard Identification Checklist (Page 2)	2-48
	Hazard Identification Checklist (Page 3)	2-49
	Hazard Identification Checklist (Page 4)	2-50
2-4	Example Potential Hazard Matrix Form	2-51
2-5	Example Hazard Analysis Sheet Format	2-52

LIST OF FIGURES - continued

Figure No.	Title	Page
2-6	Example System Safety Checklist (Master File)	2-53
2-7	Example System Safety Checklist (Project)	2-54
2-8	Example System Safety Master Checklist Coding System (Page 1)	2-55
	Example System Safety Master Checklist Coding System (Page 2)	2-56
	Example System Safety Master Checklist Coding System (Page 3)	2-57
	Example System Safety Master Checklist Coding System (Page 4)	2-58
2-9	Example Hazard Catalog Format	2-59
2-10	Hazard Report Form (DOD STS)	2-60
2-11	Sample Hazard Report Data	2-61
2-12	Concept Phase	2-62
2-13	System Definition Phase	2-63
2-14	System Development Phase (Page 1)	2-64
	System Development Phase (Page 2)	2-65
2-15	Manufacture/Test Phase	2-66
2-16	System Use Phase	2-67

LIST OF TABLES

Table No.	Title	Page
2-1	Source Document Code Listings	2-22

CHAPTER 2
REQUIREMENTS AND THE HAZARDS ANALYSIS PROCESS

2.0 INTRODUCTION

Requirements are essential to hazards analysis and the hazard analysis process in several ways:

(1) Requirements implement the hazard analysis process,

(2) Top level operational requirements drive the system functional and physical characteristics and thereby create inherent potential hazards,

(3) Imposed compliance requirements establish mandatory criteria or acceptability parameters for controlling hazards in the system design or the operational constraints,

(4) Derived requirements which result from hazards analyses define additional design and operational controls necessary to adequately control system hazards,

(5) Integration of the hazard control requirements into the system requirements data base is necessary to fully ensure implementation and verification of the hazard control requirements,

(6) Verification of compliance with imposed and derived hazard control requirements is essential for accident risk management.

In practice the hazards analysis process implements requirements, yields requirements to the system and operational design efforts, and provides documented traceability to the design implementation and the verification of requirements. For this reason, the topic of requirements and the topic of hazards analysis process are inseparable. This chapter discusses both in an integrated fashion.

2.1 IMPLEMENTING HAZARDS ANALYSIS

The hazard analysis process is the primary technical means to implement the system safety program. NHB 1700.1 (V7), "System Safety," (Reference 1) and DOD Instruction 5000.36, "System Safety Engineering and Management," (Reference 2), and other policy documents establish the requirement for a system safety engineering and management program for NASA and the Department of Defense programs. The policy for both NASA and DoD is to ensure the optimum degree of safety and occupational health by the application of system safety engineering and management practices to all systems and facilities, beginning at the program concept formulation phase, and continuing throughout all phases of the system life cycle. The authority to enforce this policy during system development and manufacture lies with the Program Sponsor. For systems which use a National Range or test facility, DOD Directive 3200.11, "Use, Management and Operation of Department of Defense Major Ranges and Test Facilities," (Reference 3) establishes the Range Commander's responsibility to:

(1) Determine policies and enforce safety procedures for range utilization,

(2) Coordinate safety plans and procedures, and

(3) Establish allowable ground and flight safety conditions and take appropriate action to ensure that test articles do not violate these conditions.

These top level policies are implemented by various directives, regulations, standards and handbooks to become a tailored system safety program for each specific system. For example, the Peacekeeper system safety program is derived from DODI 5000.36. At the Air Force level 5000.36 is implemented by AFR 800-16, "USAF System Safety Programs," (Reference 4) which imposes MIL-STD-882, "System Safety Program Requirements" (Reference 5). MIL-STD-1574, "System Safety Program for Space and Missile Systems," (Reference 6) tailors the requirements of MIL-STD-882. SAMSO STD 79-1, "Integrated System Safety Program for the MX Weapon System," (Reference 7) tailors the requirements of MIL-STD-1574 and invokes more detailed design criteria, including the design requirements of Western Space and Missile Center regulation (WSMCR) 127-1 (Reference 8).

All space and missile system programs which utilize a National Range, either for test or mission operations, must meet the design, operations, analysis and data requirements of the National Range, either WSMCR 127-1 or ESMCR 127-1 (Reference 9). It is important to note that although these requirements are invoked by the Progam Office during development, it is the Range Commander who approves their implementation and authorizes operation on the Range. By illustration, the development requirements for a military space launch system which will operate at the Eastern Space and Missile Center (ESMC) will likely include both MIL-STD-1574A and ESMCR 127-1. The Accident Risk Assessment Report developed to satisfy the requirements of MIL-STD-1574A is often submitted to the range to obtain approval for pre-launch processing, in lieu of the ESMCR 127-1 requirements for a Missile Systems Prelaunch Safety Package (MSPSP). This is acceptable only to the extent that the ARAR satisfies the ESMCR 127-1 MSPSP requirements. An ARAR which does not satisfy the range MSPSP may lead to a delay of approval for pre-launch processing, by authority of the range commander.

2.2 THE HAZARD ANALYSIS PROCESS

Figure 2.1 illustrates the relationship of the Hazard Analysis process to the "Project Design," "Program Office" and "Range Operations" functions and data. In practice the hazard analysis process starts with the initial program concept. The initial system requirements and criteria are established from the system concept, development requirements and established range safety requirements (No. 1). These system requirements form the basis for design concepts and initiate the hazard analysis (No. 2). The hazards analysis process identifies and documents all potential hazards and then establishes requirements to control the hazards (No. 3 and 4). These requirements may be imposed compliance requirements such as the National Electric Code or they may be derived from detailed system analysis. In either case these requirements are levied on the design effort for implementation (No. 5). As shown by number 6, the next step is a review of the design to assess compliance with the hazard control requirements. Concurrently, as shown by numbers 7, 8 and 9 the system, range safety and facility/site

requirements are verified and approved. Then (10, 11 and 12) the iterative process of reviewing the hazards lists and identified controls to assure completeness and incorporation of requirements takes place. As the design is finalized, the compliance assessment and other design details are used to prepare an Accident Risk Assessment (No. 15). This assessment (16) along with approved requirements (13), and Flight Plan Analysis (14), are used to support final design approval. The approved design data and accident risk assessment lead to system certification (19). Concurrently, the Flight Plan, Pad Safety Plan and SOPs are used to obtain procedure approval (17). The approved procedures, favorable test results and system design certification are used to obtain range safety approval for launch (18 and 19). It is essential that hazards, hazard control requirements and range safety requirements are identified as early as possible to ensure effective implementation in the system's design and operational concepts.

2.2.1 Hazards Analysis Objective

The overall objective of hazard analysis is to effectively manage accident risk by identifying and controlling all hazards resident in the system. Hazards are sources of danger and are inherent where they are required for operational capability. Hazard Analysis is performed as part of the system conceptual design, development, testing, production, and operational phases and consists of a continuously iterative process of systematic accident risk identification and analysis of each safety related hardware or software element in all operational modes. Hazards Analysis will:

(1) Identify all energy and toxic sources existing in the system, evaluate safety critical aspects, and identify potential safety problems and accident risk factors early in the life of the subsystem or system.

(2) Identify undesired events that could occur if the hazard is not adequately controlled.

(3) Identify controls over the energy and toxic sources to prevent their propagation. Identify the design criteria and/or operational constraints to eliminate or control accident potentials caused by human error, environment, deficiency/inadequacy of design, and component malfunction that could result in major injury or fatality to personnel.

(4) Identify potentially hazardous environments. Examine flight and ground systems/subsystems through all system phases and consider all planned and contingent operations including maintenance, repair, transportation, handling, storage, training, testing, assembly, checkout, launch, modification, deployment, retrieval and return.

(5) Identify criteria for environmental control.

(6) Establish safety design criteria that provide the degree of hazard (energy or toxin source, or environment) control required to reduce the accident risk to an acceptable level. Consider generic hazards as well as the interaction of procedures, personnel, and equipment.

(7) Specify the means by which hazard control implementation is to be verified and provide traceability of the actions taken to control the identified hazard(s).

(8) Document verification of hazard control implementation.

2.2.2 Hazards Analysis Responsibilities

The specific functions in the hazards analysis process are never contained within a single functional element of a program organization. There are no rules for allocation of function within the organization. However, typical responsibilities of Program Management, System Safety and Engineering elements may include the following functions.

Program Management

(1) Establish a System Safety Program Plan in accordance with mission requirements.

(2) Review, approve and deliver Hazard Analyses per contractual requirements.

System Safety

(1) Establish the technical requirements for the project/system hazard analysis Process in accordance with the terms of the System Safety Program Plan.

(2) Perform independent System Safety evaluation of the system's design and operations concepts to identify potential accident risks.

(3) Evaluate each potential accident risk.

(4) Coordinate the accident risk assessment with the responsible engineering function and provide a report to program management.

(5) Ensure that hazard control requirements are met. Develop design or operational requirements where necessary for adequate control. Alert program management to safety problem areas.

(6) Establish the hazard classification as required by contract or by the System Safety Program Plan.

(7) Prepare System Safety design and operations hazard control requirements checklists.

(8) Maintain all hazard analysis documentation.

(9) Provide safety problem identification and status to appropriate management. Near the end of the program, as specified in the contract, prepare a program safety report approved by program management.

(10) Evaluate design changes for hazard control.

(11) Submit hazard analysis reports in accordance with the contract.

Engineering Elements

(1) Develop and provide current design and operation/test data for hazards analysis.

(2) Develop system/subsystem analysis data such as Failure Mode and Effects Analysis (FMEA), Single Failure Point (SFP), and Fault-Tree Analysis data.

(3) Develop other supporting data analyses, such as maintenance task analysis, where required.

(4) Assess hazard analysis and accident risk assessments. Provide additional technical detail to complete the analysis where required.

(5) Coordinate problem resolution and the elimination or control of hazards.

(6) Incorporate safety design criteria and design and operations hazard control requirements into the system requirements data base and the appropriate specifications, plans, or procedures.

(7) Evaluate and confirm the Safety checklists.

2.3 HAZARDS ANALYSIS APPROACH

The hazards analysis approach illustrated in this section can be used for a system or a system element. The scope may vary as a function of complexity, the type of hazard sources, and project requirements. The hazard analysis approach and methods used will always require tailoring to meet the specific needs of the program.

Various terms are used throughout the literature and safety profession to describe safety concerns (hazards) and their causes (action events). Selection of the terms to describe the hazard is a matter of preference. In most cases specific terms such as contamination, radiation, etc., are used to describe a general hazard (energy or toxic source), and an action sentence is used to describe the mishap to be avoided by adequate hazard control. A hazard is a static, ever-present threat to a system. When a hazard (source of danger) is released and becomes dynamic, it is no longer a hazard, it is a mishap. The objective then is to control the source of danger to keep it in the static mode. When hazard control fails, control of the energy source is lost creating a mishap potential. The primary purpose of system safety analysis activity is to determine how and why control of the hazard can be lost or what can trigger the hazard to change from its static state to its dynamic state. When the hazard and accident or mishap are described, the cause(s) can be determined and acceptable controls can be defined.

Example:

HAZARD	MISHAP TO BE AVOIDED
1) Contamination	Clogging of fuel or oxidizer cavitating venturi filter results in shut down of gas generator, and turbine.
2) Toxicants	Release of UDMH/Hydrazine or N_2O_4 vapors during propellant loading. Exposure of personnel.

The hazard analysis flow of Figure 2-2 illustrates these relationships.

The hazard analysis (hazard identification and control) is a continuing, iterative process which is performed throughout the program/project life cycle, beginning with concept definition and ending with deployment/operation. Although the analysis is a continual process, there are three major phases: (1) the Preliminary Hazard Analysis (PHA), (2) the System Safety Checklist, and (3) Accident Risk Analysis and Assessment.

2.3.1 Preliminary Hazard Analysis (PHA)

The (PHA) is performed as early as possible in the life of the program/project. The PHA identifies the hazards resident in the system based on the energy and toxic sources, environment, and system operational requirements, and the accident risks associated with each identified hazard. It provides the basis for future analyses and Accident Risk Assessment Report (ARAR)/Safety Compliance Data as required by DOD or NASA customers.

In the hazard identification process, it is necessary to consider two major hazard characteristics: (1) Severity, or the potential effect on the system/subsystem if lack of hazard control causes damage or injury, and (2) the probability (credibility) that a particular hazard will, in fact, occur or be released. Significant consequences or effect are generally classified by severity and are best described as either critical or catastrophic.

To systematically perform the PHA certain steps must be accomplished:

(1) Divide the system into the elements for which a responsible design engineer can be identified so that a rapport can be established between the system designers and the safety engineers.

(2) Define the development, test, production and operational (by mode) life cycle of the system via the hardware/system functional flow diagrams and mission timelines, as appropriate. The intent is to segment the system life cycle into sequential phases that can be logically analyzed for accident risks.

(3) Identify Safety Critical aspects of systems and phases (e.g., payload mate and checkout, propellant transfer, test, launch, etc.).

(4) Identify all hazards and hazard severity categories. A hazard identification checklist similar to the example of Figure 2-3 is very helpful (Reference 10). Select those hazards that apply to the system being analyzed and document them on a Potential Hazard Matrix (PHM). An example is shown in Figure 2-4. The PHM combines a given operational phase (functional flow or mission timeline) with hardware or system elements. These factors and the related man/machine interface establish hazard identification. Document the hazards on Hazard Analysis Sheets as shown in Figure 2-5.

Hazard Analysis Sheets form the basic hazard analysis control documentation for the hazards analysis process. They document the identified hazard, the assessment of the hazard with respect to potential accidents and accident consequences, and the probability or risk that the hazard will be released to produce an accident, and ultimately the disposition. Once a hazard has been identified, it is tracked through the system life cycle until it is disposed of or "resolved." Hazard resolution is a management function and is accomplished through coordination between each affected design element and Project/Program management. It should be noted that the information contained in Figures 2-3 and 2-4 is not all inclusive and may require significant modification to meet the requirements of a specific program.

(5) Define initial requirements to control the hazard to maintain accident risk at an acceptable level. The imposed requirements or the project safety design criteria may be adequate. Where additional/alternative controls are needed, requirements should be established using an order of precedence similar to the following:

- Design - Reduce or eliminate hazards or increase functional control via increased factors of safety, redundancy, back-up functions, etc.

- Safety Devices - Accident risks that cannot be acceptably maintained through functional design requirements shall be controlled through the use of safety devices such as relief valves, current limiters, mechanical internal barriers or inhibiting mechanisms.

- Warning Devices - When functional design and safety devices do not reduce the probability of accident to an acceptable level, warning devices should be considered.

- Procedures - When an accident risk cannot be reduced to an acceptable level through design, protective or warning devices, procedures should be established to limit or control initiation of hazardous sequences, where possible.

The Potential Hazard Matrix, and related Hazard Analysis Sheets provide the basis for the Preliminary Hazard Analysis (PHA) and should be completed before the system Preliminary Design Review (PDR). This analysis also provides the basis for future detailed analyses of the system; it provides the basis for a preliminary system accident risk assessment and/or the Safety Compliance Data as necessary. In addition, it aids the identification of areas where additional safety related guidance and criteria are required. It may set forth specific design criteria or operational constraints.

2.3.2 System Safety Checklist

The system safety checklist is a requirements document. Its purpose is to compile the applicable hazard avoidance and hazard control requirements into a manageable (traceable, verifiable) format. Although distinct from the Preliminary Hazards Analysis, the effort to compile the checklist is concurrent with the PHA. The initial checklist should be completed prior to PDR and maintained throughout the program.

The system safety checklist can be developed from the applicable compliance requirements imposed on the program by contract or by program direction. It can also be developed from the derived requirements for hazard control identified through system analysis and the hazards analysis process, as well as the imposed compliance requirements. In the first case the checklist will generally stand alone; it will be used by the safety and design functions to document the verification of compliance to imposed requirements. In the second case, it can be developed as a distinct or non-distinct element of the System Requirements Data Base. This will be its strongest function.

Figures 2-6, 2-7 illustrate example System Safety Checklists. These checklists are most manageable and useful when they are automated. A properly coded checklist enables any user to sort, search and retrieve, from the computer, a matrix of all of the items addressing a specific subject, without having to read the entire checklist.

2.3.3 Accident Risk Analysis/Assessment

The PHA is updated, refined, and evaluated throughout the program/project life cycle until all identified hazards and hazard control issues have been resolved. As system development progresses, more and more data becomes available to the hazard analysis process. These data and related analyses are used to update, refine and modify the Hazard Analysis Sheets produced in the PHA, and then develop the hazard reports. When the Critical Design Review (CDR) is complete, development of the design-related Hazard Analysis Sheets normally ceases. The hazard analysis process is then directed toward verification of each identified hazard control. During the fabrication and production phase, the System Safety engineer must review all Engineering Change Summaries (ECS) for possible safety impact. Most design related hazards are resolved prior to or during the CDR. Operational test and procedural hazard controls are normally verified later in the system life cycle.

The Hazard Catalog (Figure 2-9) is often used to summarize and maintain the hazards analysis status late in the development effort. The Hazard Catalog should be produced immediately following the CDR and continually updated throughout the program/system life cycle.

The hazards analysis process following PHA can be illustrated by the following discussions of Subsystem Hazards Analysis, System Hazards Analysis, Interface Hazards Analysis, Operating and Support Hazards Analysis.

2.3.3.1 Subsystem Hazard Analysis - A Subsystem Hazard Analysis (SSHA) is performed to identify hazards associated with hardware and software component failure modes.

This analysis identifies all components and equipment whose performance, performance degradation, functional failure, or inadvertent functioning could result in a mishap. It includes a determination of the modes of failure, including all single point failures, and the effects on safety when failures occur in subsystem components. Many techniques may be used to support the SSHA (Reference Chapter 6). Examples are:

(1) Fault Hazard Analysis
(2) Fault Tree Analysis
(3) Sneak Circuit Analysis
(4) Cable Failure Matrix Analysis

The SSHA and its reporting should include the following:

(1) Component(s) Failure Mode(s) - All component failure modes which can result in a hazard.

(2) System Event(s) Phase - The phase of the mission the system is in when the hazard is encountered.

(3) Hazard Description - A complete description of the hazard.

(4) Effect on Subsystem - The detrimental results an uncontrolled hazard source could inflict. Possible upstream and downstream effects shall also be considered.

(5) Risk Assessment - An assigned risk assessment for each hazard.

(6) Recommended Action - The recommended requirements to eliminate or control the hazard. Include alternatives where appropriate. Provide sufficient technical detail in order to permit the design engineers and the customer to adequately develop and assess design criteria resulting from the analysis.

(7) Implementation Verification - How the requirements are actually implemented in design or controlling procedures. As a design progresses from concept through Critical Design Review, the verification would identify the implementation successively in the System Requirements Analysis, equipment specification, and finally, in the design drawings.

(8) Effect of Recommended Action - The effect of the recommended action on the assigned risk assessment.

(9) Any information relating to the hazard not previously covered; for example, applicable documents, previous failure data in similar systems, or administrative directions.

2.3.3.2 System Hazard Analysis - A System Hazard Analysis (SHA) is performed to determine the safety problem areas of the total system. This analysis includes a review of subsystems interrelationships for:

(1) Compliance with safety requirements.

(2) Possible independent and dependent failures that could present a hazardous condition, including failures of safety devices.

(3) Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.

(4) Changes that occur within subsystems so that the System Hazard Analysis can be updated accordingly.

(5) Support equipment interface with the primary system.

(6) Facility requirements for system operation and maintenance.

(7) Inherent safety problems with system employment.

(8) Expected human error cause factors.

Techniques used for the SHA are similar to those used for the SSHA. The general criterion which a good SHA should meet is to clearly show the degradation in the safety of a given subsystem and the total system from normal and abnormal operation of another subsystem.

The SHA and reporting includes all subsystem failure modes which can result in a hazard. These descriptions are similar to the component failure mode descriptions provided in the SSHA. However, emphasis is now placed on failures affecting interfacing subsystem operations.

The following is an example of analysis results for one hazard identified in a subsystem. The hazard is identified, accident scenarios are postulated, accident controls are identified, and controls implementation are proposed. In addition, status of compliance with safety requirements is presented and verifications of accident controls are described.

STRESS CORROSION HAZARD ANALYSIS EXAMPLE

1. Summary of Assumptions and Results

   The risk factor of stress corrosion is considered catastrophic or critical based on the potential accident scenarios. However, it will be acceptable based on a Stress Corrosion Analysis Report and documented safety procedures which show that:

   a. Safety critical components are made from materials which are not stress corrosion susceptible (MSFC-SPEC-522A Table 1) or parts are manufactured and assembled to ensure that sustained tensile stresses are well below the crack initiation/growth levels and inspection/test ensures detection of unacceptable flaws.

   b. The Spacecraft will not be subjected to corrosion inducing environments at any time from manufacture through launch.

   c. Drawings/drawing changes of safety critical parts require sign-off by System Safety and Mechanical Systems Engineering.

2. Potential Accident Scenarios

   Factory - During assembly, checkout and preparation for transport to launch site, stress corrosion cracking could lead to a failure of a load carrying structural member. This type of failure, if undetected at the factory, could lead to a catastrophic accident during later ground or flight operations. The causal factor for stress corrosion cracking is the use of stress corrosion susceptible material under sustained tensile stress in a corrosion inducing environment. Contributing factors which might induce stress corrosion cracking include over-torquing bolts and the use of corrosive cleaning solvents.

   Ground Operations - Checkout - A stress corrosion initiated crack could propagate during ground operations resulting in a structural failure of the Spacecraft. The resulting accident could cause damage to other cargo element systems, Airborne Support Equipment, Orbiter, Aerospace Ground Equipment, facility, or personnel injury. A structural failure could also result in a hydrazine leak/fire. Causal factors are the same as at factory.

Ground Operations - Transportation - During transport, a structural failure could occur with resulting damage to the transport container and/or possible personnel injury if failure is undetected prior to removing the Spacecraft from the transport container. Causal factors same as at factory with expected stress loads from transport aiding in crack propagation.

Launch through STS Orbit Insertion - If there is stress corrosion cracking of the Spacecraft structural elements, the expected high g-loading during STS launch/ascent to orbit could cause a structural failure resulting in a Spacecraft collision with the Orbiter cargo bay interior. Such a collision could result in loss of payload and Orbiter/crew.

Payload Deployment from Orbiter - Enroute to geosynchronous orbit, a structural failure induced by stress corrosion could cause loss of the Spacecraft. Existing cracks could propagate from normal flight loads.

Abort - During reentry/landing, a structural failure of the Spacecraft could occur if stress corrosion cracking had weakened structural elements. The structural failure could lead to a collision with the interior of the cargo bay causing loss of Orbiter/crew.

3. Accident Controls/Verification

   a. The Spacecraft has been thoroughly analyzed to identify all safety critical parts. The safety critical parts have been evaluated, and materials which are not highly resistant to stress corrosion cracking, i.e., materials not listed on Table 1 of MSFC-SPEC-522A have been identified. Material Usage Hazard Analyses (MUHAs) have been prepared to justify the use of non-Table 1 materials for Spacecraft safety critical components. The Stress Corrosion Safety Analysis Report (SCSAR) provided the detailed screening of safety critical parts, the rationales for use of non-Table 1 materials, and the specific safety controls for each stress corrosion susceptible part.

   b. Techniques for controlling the risk factor of stress corrosion cracking which will be implemented include specification of grain direction, shot peening, special assembly procedures, and/or nondestructive evaluation such as dye penetrant or X-ray inspection.

The specific controls for each safety critical stress corrosion susceptible part is identified in the SCSAR. The verification of the controls will be provided by System Safety and Mechanical Systems Engineering sign-off of safety critical drawings/drawing changes.

c. Manufacturing planning will provide detailed instructions to prevent improper assembly. System Safety will provide inputs to manufacturing planning which will be signed off and approved by the design and quality assurance engineers. Spacecraft assembly operations are witnessed and inspected by Quality Control (QC) to ensure that calibrated and certified tools are used to assemble the Spacecraft according to drawings, and that assembly procedures are followed exactly.

d. The manufacture of parts, assembly of the Spacecraft and all ground operations through installation in the STS Orbiter cargo bay are performed in a temperature/humidity controlled environment. The Spacecraft STS environmental controls are delineated in the Stress Corrosion Safety Analysis Report.

4. Compliance/Noncompliance/Deviation

NHB 1700.7A

Paragraph 200	Compliance - Worst case environments analyzed
Paragraph 208-3	Compliant - Safety critical parts materials selected for resistance to stress corrosion in accordance with intent of MSFC-SPEC-522A
Paragraph 214	Compliant - Verification of Safety Controls

MSFC-SPEC-522A

Section 3	Compliant - General Requirements
Section 4	Compliant - Material Usage Requirements, modified for the Spacecraft Program
Section 5	Compliant - Material Selection Criteria used to evaluate material resistance to stress corrosion cracking

Subsystem and system hazard analysis reports should include detailed descriptions of the physical and functional characteristics of the system components. The capabilities, limitations and interdependence of these components need to be expressed in terms relevant to safety. The system and components need to be addressed in relation to mission and operational environment. System block diagrams and/or functional flow diagrams may be used to clarify system descriptions.

2.3.3.3 Interface Hazard Analysis - The Interface Hazard Analysis (IHA) is specifically intended to identify all physical and functional incompatibilities between adjacent/interconnected/interacting elements of a system which, if allowed to persist under all conditions of operation, would generate hazards which could result in mishaps. The objectives of an IHA are to identify the requirements to control or eliminate all accident risk factors that may be present as the consequence of integrating the system. Several inductive analysis techniques and formats may be used to perform an IHA. The key advantage of the IHA over other analyses which also consider interfaces between subsystems is the thoroughness of the IHA in considering more than simple operating states.

A missile system comprised of propulsive stages from several manufacturers may have an ordnance system provided by another contractor and an ordnance arming and firing control system provided by yet another manufacturer. Although each of these contractors will perform hazard analyses for the separate elements and to some extent analyze potential hazards resulting from simple interfaces, these analyses would not ordinarily consider potential hazards unique to the integrated system. The IHA is the tool used by the analysis integrator that will consider all interfaces and potentially hazardous interactions among all elements of the integrated system. Missile ordnance systems used to initiate propulsive stages generally use signals that begin as digital logic, are decoded and changed to analog signals that initiate an explosives chain in which a pyroshock signal is transmitted to the propellant igniter resulting in ignition and propellant burn.

Each of these signals originates, terminates or crosses interfaces in a separate element of the system. The IHA, if properly executed, will deal with the complex interactions of all the signals, including all safety interlocks, and identify potential interface hazards and any controls required in addition to those identified in the separate element hazard analysis.

The well-performed interface hazard analysis should have considered all likely physical, functional, and flow relationships across each interface.

A look at the physical layout of subsystem components is necessary to determine if a problem exists such as inadequate clearance between components which may dissuade proper maintenance or result in damage during maintenance or operation.

Functional relationships across interfaces must be looked at in detail in the IHA. These are the most commonly analyzed relationships such as zero output, degraded output, erratic output, excessive output, and inadvertent output effects across each subsystem interface.

Finally, an analysis of the flow between subsystems of energy or physical substances should be done to identify possible hazards. Security of interconnections between subsystems must be evaluated along with the effects of a partial or total failure of these interconnections. Some possible effects might be shock, flammability, or toxicity.

2.3.3.4 Operating and Support Hazard Analysis - Operating and Support Hazard Analysis (O&SHA) is the final task in the analysis sequence, it is a task that continues for the life of the system. It is performed to ensure a systematic and complete evaluation of all of the functional aspects of the system.

Conducting an O&SHA - The initial task is similar to that in our initial discussion on system analysis. It involves the same acceptability parameters developed during the formulation of the analysis goals.

The first thing to do is to examine the mission goals keeping the procedural sequences in mind. Based on the analyses of the system during the design phase, how safe is the system design? What residual risk controls have been left for the operational sequences? Again, we go back and look at transportation and handling equipment, software, operational and industrial environment, storage or processing facilities, and support equipment. However, this time these items are looked at in relation to the way they were designed to operate, and their operational relationship with all other aspects of the system. Furthermore, we need to know all the ways we can get into trouble operating the system in the manner it was designed to operate.

The first step is to learn from the design analysis: "What are the energy sources and what was done in the design to control them?" This should also include those conditions not totally controlled by design. Typically, additional controls are delegated to procedural action.

The second step is to determine where in the operational phase these conditions can become critical. To do this, all operations are segmented into groups of sequenced events, each of which can be examined for mishap risk. Whether a mishap can occur, and whether that mishap can cause mission inhibiting damage, can be determined from the original analysis. The time at which the condition is critical varies with the system configuration, its location, and the time that a failure or error occurs. For example, a relief valve on a hydrazine tank freezes shut. This situation is not critical until there is hydrazine in the tank and the system is pressurized. Therefore, any evaluation of danger, damage, and risk must include a time analysis. This analysis is put into matrix form that lists: 1) the operational phase (e.g., manufacturing, in-plant testing, transportation launch processing, launch deployment, reentry, landing, refurbishing, etc.); and, 2) potential conditions in each of these phases that can cause a mishap (e.g., inadvertent ignition of ordnance device, inadvertent actuation or deployment of solar panels, antennas, staging devices, shrouds, system overpressurization, fire, flight termination, etc.) for each safety critical system, subsystem, or component.

Using this approach, the points at which a specific hazardous sequence will begin or end can be shown. From this point, much information can be derived. Improper sequencing of hazardous events and events following the initiation of an undesired event can be easily noted. When there is an indication that inadvertent activation can result in a mishap and design controls are not sufficient, special safeguards are incorporated into operational procedures to minimize occurrence or minimize subsequent effects.

This brings up the third, and most important step: task or procedural analysis. Procedural safety analysis is conducted to find out in advance what can go wrong. Some tasks are inherently more hazardous than others. Task accomplishment procedures need to be analyzed in detail.

A task analysis is performed to identify which equipment, procedures, or process operations have mishap potential. An analysis of the procedures used in those tasks determines where the hazardous steps are and where procedural controls on the triggering mechanisms should be inserted. A task analysis will determine which tasks can be done simultaneously, and which must be done sequentially. This analysis will also ensure that the overall operations can be conducted under conditions that are the worst foreseeable and still have a margin of safety. Uncertainties of system and component characteristics during the initial operations necessitate rigid controls and contingency planning. By the time a system is operational, hazards have been evaluated and system characteristics have been defined, and hazard control becomes routine. Changes to proven procedures without adequate risk assessment often times are disastrous. For example, it was critical that an Atlas ballistic missile be launched at precisely 11:00 a.m. Problems in the launch preparation process caused a reassessment of the earliest possible launch time. The new time was set for 11:30 a.m. This time was unacceptable due to other test conditions. An analysis of the times involved in the remaining launch preparation tasks revealed that there was one task that required exactly one-half hour to complete. The task was to spin up the guidance system gyros and physically check them to assure they were all functioning properly. Inquiry revealed that in the past several launches no problems were found with these gyros. Therefore, it was proposed this test be deleted to makeup the lost one-half hour. Against the advice of the guidance system engineers, this decision was made. The missile was launched precisely at 11:00 a.m. A pitch gyro did not function and the missile looped and had to be destroyed. The people making the decision to delete the gyro test made that decision without full knowledge of why the test was being conducted. They altered a procedure that was specifically written to control a known hazardous condition. They were also not aware the gyros were due to be replaced by a new model with the deficiency corrected.

Contingency Planning - O&SHAs will identify points at which contingency planning needs to be applied. As long as a hazard exists, there is a possibility that loss of control will occur. The only thing that is uncertain is the time and exact circumstances. The actions taken during the first few seconds after a hazard is identified may determine whether control can be re-established and a mishap avoided. Under these circumstances, emergency and back-out procedures are planned and prepared long before the system is put into operation. Often times when an emergency arises, there is no time to assess the situation, determine what is wrong, determine the corrective action, and carry out the action. Emergency procedures are prepared to handle the immediate crisis. Back-out procedures are then

implemented to put the system in a less dangerous configuration from which there is time to regain control of the hazards. Optimum actions necessary to recover control need to be determined long before the emergency situation arises. Wherever possible, system design should permit recovery without danger to operating personnel. In some cases, after "backing" the system away from the emergency, it will become apparent that planned actions cannot handle the situation. Contingency planning should take this into account and carefully establish a "point-of-no-return." Without a firmly established point, persons involved in the emergency are so wrapped up in efforts to save the system that they do not have time to determine the optimum point when to abandon the recovery attempt and salvage whatever is left of the mission or system. Conversely, efforts may be abandoned prematurely, long before it is necessary. The analysis of operational contingencies should include all operations listed in the operational timelines including system installation, checkout, and modification as well as mission operations. Particular attention should be paid to operations that interface with operational support equipment and the needs of the operators.

Evaluation Criteria - O&SHAs can be evaluated against three types of criteria: scope, technical validity, and accountability. Each is discussed below.

(1) Scope - The O&SHA listing of operations/tasks must be related to whatever system is being used on the contract for system function accountability; e.g., it should track the systems requirements analysis when one is being performed. As a method of auditing this aspect of the evaluation criteria, all person-performed tasks in the Operational Requirements Analysis (ORA), Test Safety Analysis (TSA), and Logistics Support Analysis (LSA) should be represented in the O&SHA. Eventually, all tasks/subtasks in Technical Orders and in test procedures should also be accounted for. When used for production, deployment, and similar contractor-performed operations, the O&SHA should be related to the plans for those operations, and then to the actual controlling media. The planned sequence of tasks should be followed in the O&SHA to provide analysts the capability of evaluating the potential for hazards induced by that sequence.

(2) Technical Validity - Evaluation of technical validity in an O&SHA considers four independent concerns: was there a sufficient understanding of the tasks to identify the potentially hazardous effects?; were the risks associated with each identified hazard properly evaluated?; were desired solutions identified for implementation, and did they satisfy specified criteria?; were the required solutions effectively implemented? The analyst's rationale and/or supporting data for each line item in the O&SHA must provide the technical basis for such evaluations. Safety requirement checklists developed as part of, or in conjunction with the Potential Hazard Analysis (PHA), should be utilized. So should any personnel hazard data developed in subsystem or system-level safety analyses. When the use of analytical tools is insufficient to identify the specific nature of a hazard, or the effects of implementing a chosen safety requirement, the O&SHA must establish the

requirement for development of empirical data (test, Verification and Validation, etc.) and use that data dispositioning the hazard.

(3) Accountability - The O&SHA must specifically detail acceptance by the analyst(s) of the implemented solution to each identified hazardous condition which is coded with a hazard risk/level deemed unacceptable under the requirements of the contract, or as applicable under Government regulatory requirements.

Each potential accident risk is considered to be an open problem and resolution efforts are continued until the accident risk is resolved by one of the following actions: (Generally these actions do not occur until after CDR, at which time all engineering is subject to formal configuration control.)

(1) The accident risk has been eliminated by design and design accomplishment has been confirmed, or;

(2) The accident risk has been reduced to an acceptable level (controlled hazard reduction precedence sequence), and the reduction has been verified by means of a successful completion of those verification processes identified in the end item specification verification matrix as well as in test procedures, analytical studies, and/or training programs, or;

(3) The accident risk has been assessed and the risk has been accepted.

2.4 INSTRUCTIONS - HAZARD ANALYSIS DOCUMENTATION

The documentation of data and analysis resulting from hazard analysis is extremely important to risk management. The following guidelines for completing the forms typically used in hazard analysis must be adapted to the program requirement.

2.4.1 Hazard Analysis Sheets (Figure 2-5)

Each identified potential hazard is analyzed to assess the accident potential. The analysis includes a definition of how the hazard can propagate into an accident, the potential effects, the assumptions and rationale, the hazard level classification in accordance with the definitions of the SSPP, and the design and/or operational requirements to eliminate or control the hazard with references to specifications. This section provides guidelines for completing the hazard analysis sheets of Section 2.3.1. The guidelines are keyed to the item numbers of the example hazard analysis sheet format of Figure 2-5.

Item 1: Enter the unique analysis number.

Item 2: Page numbers shall be 1 of 1, 1 of 2, etc.

Item 3: Enter the date the analysis or revision is completed.

Item 4: Enter the hazard classification as determined by the analysis or revision in accordance with the categories defined in the System Safety Program Plan (SSPP).

Item 5: Enter the status as one of the following:

a) Open for unresolved problem or incomplete analysis.
b) Closed for items when analysis determines hazard is not valid, hazard eliminated by design, or residual hazard accepted by management and customer.

Item 6: Enter the project phase when analysis was completed or revised, such as:

a) System study
b) Pre-PDR
c) PDR Review, etc.

Item 7: Enter the system title.

Item 8: Enter the appropriate subsystem nomenclature.

Item 9: Enter the Operation/Phase considered in the analysis, as discussed in paragraph 6.1 Item 4.

Item 10: Enter the hazard title (Hazard Group).

Item 11: Enter any applicable reference to source data used in the analysis.

Item 12: Describe the hazard in clear, concise terms.

Item 13: Describe the worst case potential effects of the hazard under consideration.

Item 14: Provide all pertinent facts or assumptions used as the basis of analysis; hazard causes, calculations, reference data and analysis performed to develop the rationale for classification of the hazard and disposition actions.

Item 15: Enter the requirements established by the analysis to eliminate or reduce the hazard. There should be a control for each hazard cause. Examples:

a) Design
b) Operational Constraints
c) Other

Item 16: Enter the reference to other project documentation that incorporates the requirement of Item 15, e.g., the paragraph of specification that defines a design requirement.

Item 17: Enter how incorporation of the hazard control is verified (test, analysis, inspection, demonstration).

Item 18: Same as Item 16 but for verification.

Item 19: Status of control or verification such as: planned, implemented, completed, resolved, etc.

Item 20: Enter remarks on the hazard. In most cases, this will be progressive entries, i.e., referred to design, eliminated by design change, entered in Hazard Catalog, risk accepted, etc.

Item 21: Enter analyst's name, location and telephone number.

Item 22: Signatures attesting to report completion.

2.4.2 System Safety Checklist (Figures 2-6 and 2-7)

A properly developed System Safety Checklist Data Base is a master file of non-tailored system safety requirements extracted verbatim from various government and industry source documents, such as design handbooks, Military Standards and and Regulations, NASA Standards, National Fire Protection Association, OSHA, etc.

The systems safety checklist illustrated and discussed in this section was derived from the Martin Marietta Peacekeeper program. The discussion of the checklist is limited to imposed compliance requirements, it does not include derived requirements, nor does it illustrate the link to the SRDB (System Requirements Data Base). It should also be noted that this is an automated system for peacekeeper. The software is Martin Marietta proprietary.

Checklists are maintained in the computerized System Safety Master Data File by document title/code and are available for copying by project level System Safety organizations. The project level organization tailors the Master Data Checklist copy to meet project contractual requirements (individual document checklist requirements may be integrated into a single checklist at the project level). The same checklist form is used for both the System Safety-Master Text and the project checklist. The Checklist format consists of seven items of header information and eight columns for additional data entry. Master checklists contain information in the header and in Columns 1, 2, and 3 only. When checklists are project tailored and engineering has responded to each requirement, Columns 4, 5, 6, 7, and 8 will be completed.

Figures 2-6 and 2-7 illustrate checklists for System Safety-Master Text and Project, respectively. The circled numbers on the figures refer to the data entry items that are discussed in the following. See also the notes at the end of this section.

Item 1: Enter either
"System Safety Master Text" or
System Safety "X" Project

Item 2: Enter identification number of the source document and its effective date.

Item 3: Enter title of the source document.

Item 4: Leave blank for master checklist. For project level checklist, enter the name of the engineer, or lead, responsible for determining the degree of actual compliance to the requirements.

Item 5: Enter date of the checklisting of the source document.

Item 6: Enter date if the last minor revision to the source document checklisted.

Item 7: Enter page number of the checklist.

Item 8: Column 1. Enter checklist item number. These numbers herein consist of a twelve character document, revision, and checklist item number code. The first three digits match the three-digit source document code (Ref. Table 2-1) assigned to the checklist. The next two digits indicate the document revision number and the last five digits are the sequential checklist item number. For example:

354.01-00924

354	Document code, matching the document code developed from Table 2-1.
01	Indicates revision Number 1 to the source document.
00924	Indicates the 924th checklist item.

Note: The period after the third digit and the hyphen after the fifth digit are required; they are part of the checklist item number. Once the checklist item number is established in a master checklist, that number is not changed.

Table 2-1 Source Document Coding Listing

Number	Document Category
001 thru 050	System Safety Management
051 thru 100	Public Law (other than Title 29 OSHA Part 1910)
101 thru 200	MIL Standard and Specifications
201 thru 225	USAF Design Handbooks
226 thru 255	USA Design Handbooks
256 thru 350	USAF Regulations and Standards
351 thru 425	USAF Manuals
426 thru 450	USAF Pamphlets
451 thru 500	USA Regulations
501 thru 525	USA Manuals
526 thru 575	USN Regulations
576 thru 600	USN Manuals
601 thru 700	NASA Safety Requirements
701 thru 725	ERDA Safety Requirements
726 thru 775	Industry Standards
776 thru 799	Title 29, OSHA Part 1910
800 thru 850	Miscellaneous

Item 9: Column 2 (Criterion). This column in the Master Checklist contains the paragraph by paragraph requirements extracted verbatim from the source document. In the Project Checklist, this column contains single checklist items (requirements) that can stand along. See Note 1 at the end of this section.

Item 10: Column 3; Criterion - A 2 to 7 character alpha/numeric code is used in this column to identify the system against which the criteria are to be applied.

Item 11: If the design is in compliance, an "X" will be placed adjacent to the requirement in Column 4, "Compliance".

Item 12: If the design does not comply with the requirement, an "X" is placed adjacent to the requirement in Column 5, "Non Compl".

Item 13: If the design requirement is not technically applicable, an "X" is placed adjacent to the requirement in Column 6, "Not Appl".

Item 14: Column 7. Enter a concise description of the method of compliance, the rationable for noncompliance or justification for imposition of operational constraints in lieu of design, or a technical discussion on why the requirement does not apply.

Item 15: Column 8. Enter an exact description of the drawing, test method, operations procedure etc., wherefrom compliance/control or non applicability to the requirement, can be verified. Design related noncompliance items will normally result in a formal deviation request. When a deviation to the requirement is proposed, the unique number assigned to the deviation request shall be entered. Proposed deviations must be identified as early in the program as possible to permit the customer time to adequately evaluate the deviation and its technical justification. Presenting the deviation request at the Critical Design Review (CDR) may result in a surprisingly costly redesign effort.

Notes:

1. Tailored checklists for project level applications are developed as follows. The safety engineer generating the checklist must make sure he has the current master checklist document, or if required, the contract designated issue thereof, before he begins project level checklisting. He should read the entire document before he begins.

   a. The System Safety engineer will select each definitive System Safety requirement from each pertinent section within the document and retain it on the checklist form. Philosophy, background, and other nondefinitive type information will be eliminated.

b. System Safety requirements that are written in clear and concise language shall be retained verbatim on the checklist. If the language is not in a checklist style, paraphrasing of requirements may be necessary. When paraphrasing a requirement, it is important for the checklist requirements to match the source document requirements in spirit and intent. Each checklist item shall be written to stand alone. For example, if a checklist item makes reference to another paragraph in a source document, or any document, always identify the reference document number or title and the paragraph.

c. Each checklist item will include its reference paragraph from the source document. References will be in parentheses following each checklist item.

d. If a source document paragraph or paragraph with subparagraphs contains more than one System Safety requirement, a separate checklist item will be made for each. An example of source-to-checklist conversion follows for AFR-122-10, Paragraph 1-2b(2)(b):

Source Document

(b) The weapon system design will keep the prearming function totally separate and distinct from the authorization or enabling function. Design features will preclude prearming in the absence of the intent command signal, and will also prevent any bypass of the prearming device(s) that would permit final arming without prearming.

Checklist Format

280.00-00008	The weapon system will be designed to keep the prearming function totally separate and distinct from the authorization or enabling function. (Para. 1-2b(2)(b)
280.00-00009	The weapon system design features will preclude prearming in the absence of the intent command signal. (Para. 1-2b(2)(b)
280.00-00010	The weapon system design will prevent any bypass of the prearming device(s) that would permit final arming without prearming. (Para. 1-2b(2)(b)

e. After the master checklist document has been converted to a project level checklist, a reviewing System Safety engineer will compare the draft project checklist with the master document and provide comments to the checklist author. Corrections to the draft will be incorporated as appropriate. The project checklist then will be entered into the computer system and printed in hard copy.

The code is developed from Figure 2-8: System Safety Master Checklist Coding System.

2. There are prerequisites that need to be met before coding a checklist. The individual who will be coding the checklist should have the source safety document, from which the System Safety Checklist to be coded was derived, and a work copy of the System Safety Checklist to be coded, with the "System" column left blank. The coder must review and be familiar with the titles, headings, and subheadings of the source safety document, so that these can be translated into the various codes. The System Safety Master Checklist Coding System (Figure 2-8) is the document from which the example codes are derived. The coder must be very familiar with the codes appearing on this list. Finally, the coder must know and understand how the coder checklist will be used to save time in document searching and reading. The following guidelines are designed to assist the checklist coder in assigning the proper codes:

   a. Each item of a checklist must receive a code.

   b. Code each item to the greatest degree possible.

   c. Individual codes for one element of any item must not be more than seven (7) digits long.

   d. The words "shall" and "will" denote a specific requirement to be met and must be coded as such. (F3)

   e. The code must appear in the following order: Type - System - Subsystem - Component.

   f. Use the titles, headings, and subheadings of the source safety document as a guide to assist in assigning the most appropriate code, but do not code the title, heading, or subheading itself.

   g. Use the reference code (F2), when the document referred to is the same document that is being coded.

   h. When using the management administration Type Code (F), place the applicable number for the kind of management administration, after Type (F) and before the system or subsystem code being used. (Example: F3G or F2JA)

   i. When absolutely necessary, a System need not be preceded by a Type.

   j. A code may not be made up of two (2) Types or two (2) Systems used together. The code is divided into two (2) separate codes. (Example: (DF3) for operations requirements is incorrect; (D) and (F3) as separate codes is correct.)

k. Subsystems need not be followed by a Component, if the information to be coded is of a general rather than a specific nature.

l. A Subsystem shall not be used as a code by itself; it must be preceded by a Type or System.

m. A Component shall not stand alone as an item code, it must be preceded by a Subsystem and at least a System.

n. When using codes that are subdivided into additional code segments, the letter or number should not be preceded by itself. (Example: facilities vehicle should be coded as 'JC', not 'JJC'.)

o. When coding a definition, use (F5).

p. Individual acronyms shall be coded each time they appear in a specific checklist.

q. A reference shall be coded as a reference each time it appears in the checklist, even if the code (F1) has been used as an all encompassing Management Administration code.

r. Additions should not be made to the Subsystem and Component sections of the Master Safety Checklist Coding System list without prior approval of the System Safety managing authority. See Note 8.

s. Deletions may not be made to any part of the System Safety Master Checklist Coding System. See Note 8.

3. Once the safety requirements have been checklisted and coded, the checklist is subdivided by System or discipline and the resulting condensed checklists are distributed to the appropriate engineering elements. Each element is responsible for responding to the checklist by completing Columns 4, 5, 6, 7, and 8 of the checklist. At, or before, the Preliminary Design Review, the design should be sufficiently defined to permit the design responsible engineer to determine whether the design is in compliance with the contractual requirement, whether a deviation will be sought, whether control will be developed by application of operational constraints, or the requirement is technically not applicable.

4. Test or operations related checklist requirements are frequently not resolved until after the CDR. Here again, closure should occur as soon as practicable.

5. When each item on a given checklist is completed, the design responsible, or lead, engineer will affix his/her signature adjacent to the header titled "Completed By". This signature certifies to the accuracy of the data provided in response to the requirements.

6. It is generally necessary for the responsible System Safety Engineer to interface with the design responsible engineer on a frequent basis to assure the checklist is being kept up to date and to permit verification of compliance as the engineering is completed. The same is true for test and operations related activities. Waiting for the last minute to perform the verification activities will leave the System Safety Engineer an insurmountable task.

7. One, if not the most important, facet of checklisting requirements is the necessity for project level management to recognize the overall time and cost savings realized by the use of checklists and to openly support and direct their use and proper completion. If management does not support their use, they become nothing more than costly and futile exercise for System Safety.

8. Master Checklist Changes - When there are changes or revisions to the source document from which a Master System Safety Checklist was generated, a System Safety Engineer will be assigned the task of determining the effect of the changes against the Safety requirements in the master checklist.

   a. Major Revisions to Source Document - A major source document revision will require the generation of a new master checklist. The checklist item numbers will also reflect the revision. For example: Revision 1 to ESMC 127-1, will begin with 352.01-00001 (see Figure 2-7). Note that the previous version of the checklist is not deleted from the master file as contractual compliance to earlier versions may continue for years.

   b. Minor Changes to Source Document - Minor changes to a source document which has been checklisted and affects Safety requirements must be incorporated into the master checklist. Note that the original criterion items cannot be changed.

      1. A symbol $A for example, will be used in column one to tag items added, deleted or changed by the first revision. $B for the second, etc. $A, plus the source document change date, will be entered in the header following Last Revision Date:. ($B plus change date will follow $A.)

      2. Additions - Checklist items may be inserted between two existing items. For example;

Checklist Item #1	005.02-00001
New Item	005.02-0001a
	$A
New Item	005.02-0001b
	$A
Checklist Item #2	005.02-00002

3. Deletions - If checklist items are deleted by a revision, the checklist item will be retained and tagged in Column 1. "Deleted" will be entered in the criterion column. For example:

Checklist Item	Criterion
005.02-00130	Minimizing the use of flammable...
005.02-00130 $A	"deleted"

4. Changes - When a criteria item must be changed, the item in Column 1 is tagged and the correct data is inserted in Column 2. For example:

Checklist Item #1:	005.02-00001
corrected Item #1:	005.02-00001 $A

If the item should change again with a second change notice, it would be tagged $B. It would not replace the original item or the change 1 item.

c. Once a project has copied a master checklist into its own files, the checklist copy can be tailored to fit the individual needs of the program.

2.4.3 Hazard Catalog (Figure 2-9)

The hazard analysis can be summarized in the Hazard Catalog to provide current status of all identified hazards. The catalog provides for hazard tracking, management visibility, and may be submitted in accordance with contract data requirements. The Hazard Catalog consists of two parts; Hazards List and Residual Hazards.

(1) Hazards List - Each identified hazard is recorded and statused on the format shown. The information shown in the Hazard List shall reflect the current status of the detailed hazard analysis. The following instructions refer to the item numbers of Figure 2-9 and are to be used in preparing the Hazard List, Part I of the Hazard Catalog.

Item 1: Enter the appropriate system as described in paragraph 2.4.1, Item 7.

Item 2: Page numbers shall be 1 of 1, 1 of 2, etc.

Item 3: Enter the hazard number as defined in paragraph 2.4.1, Item 1.

Item 4: Give a brief description of the hazard.

Item 5: Check this column if hazard has been eliminated.

Item 6: Check this column if residual hazard remains to be resolved.

Item 7: Check this column if the hazard is controlled.

Item 8 and 9: Check appropriate column indicating whether risk has been accepted (with or without waiver) or hazard remains open.

(2) Residual Hazards - Each residual catastrophic or critical hazard is recorded and described on the format shown. The following instructions refer to the item numbers of Figure 2-9 and are to be used in preparing Residual Hazards, Part II of the Hazard Catalog.

Item 1: Enter the appropriate item number as described in paragraph 2.4.1, Item 7.

Item 2: Enter the hazard level as described in paragraph 2.4.1, Item 4.

Item 3: Enter the date the hazard was first identified or the report was last revised.

Item 4: Enter the system title as described in paragraph 2.4.1, Item 7.

Item 5: Enter the appropriate subsystem nomenclature.

Item 6: Enter the appropriate component nomenclature.

Item 7: Describe the hazard and its effects in clear concise terms.

Item 8: Enter the recommended action to be taken, in sufficient detail for management visibility and understanding.

Item 9: Enter the disposition of the hazard, including rationale for retention of the hazard, or the actions accomplished to reduce or eliminate the hazard.

2.4.4 Hazard Analysis Report

A well documented Hazard Report contains a description of the potential problem and what is being done about it. The Hazard Report is the most important document of all safety documentation discussed during a safety review. Each hazard should be documented on a hazard report and should: a) show potential causes, b) identify controls, c) relate results of verification, and d) provide traceability. The data should be brief and concise with enough back up data supplied so that each Hazard Report can be a "stand-alone" document. Summarize referenced detailed analysis, tests, and

test results in order to provide enough facts to allow the Safety Review Team (SRT) to make a value judgment.*

2.4.4.1 Identifying/Classifying/Describing Hazards - Ideally speaking, all hazards should be revealed during the Phase 0 or Phase 1 Safety Review time period. Obviously, the further downstream a hazard is discovered, the greater the potential for cost and schedule impact to the program. Typical sources used to identify hazards are risk factor matrices, safety analyses, other related analyses, and checklists. As each hazard is identified, it should be documented on a uniquely numbered hazard report form and followed through resolution (Figure 2-10).

Hazards are defined as system level "top" or "end" events. One of the common errors introduced during Hazard Report generation is listing hazard causes/causal factors in place of the hazard itself. Figure 2-2 gives guidance and examples on how to avoid this pitfall. Figure 2-11 contains sample Hazard Report data.

Experience has shown that in describing a hazard, use will usually be made of action words (verbs) such as ... failure... firing, or... release. It will be noticed that action words such as given above relate to the release of (payload) possessed material that could cause damage/injury to outside environment (launch vehicle facilities, or personnel).

Most hazard reports will be resolved upon completion of the Phase 3 Safety Review with the exceptions, mostly involving operating procedures, tracked via a resolution log. (See MIL-STD 1574A, Para. 5.2.10)

2.4.4.2 Identifying Potential Causes - As hazards are discovered during the time period of the Phase 0 or Phase 1 Safety Reviews, identity of the potential causes must be ascertained. Causes are types, or classes of events, or conditions that can lead to the identified hazard. Typical causes are:

- Mechanical component failure
- Electrical component failure,
- Operator error,
- Induced environments

Examples of structural failure causes are:

- Propagation of pre-existing flaws
- Stress Corrosion
- Orbiter induced environment
- Hydrogen embrittlement

*Note: This discussion on hazard reports has been extracted for the most part from MCR 82-800, Rev. B, 29 Sept 82, "DOD Safety Review Team Lessons Learned Database", lesson number 001.0A-00175 prepared by Martin Marietta. (Reference 11)

Individual causes can be sub-divided if necessary or desired.

2.4.4.3 Propose/Track Controls - The proposed hazard controls and tracking process should be established and in effect by the conclusion of the Phase 1 Safety Review. Controls are specific facts as to how a design (or procedure) will control the identified hazard causes. Each identified cause should have a one-for-one corresponding control (minimum) and verification method. Statements implying that "Requirements will be met" are unacceptable. Some examples of acceptable controls would be:

- Safety Factor 1.4
- Three flow devices provided... (identify)
- Three inhibits are provided... (identify)

Some examples of unacceptable controls would be:

- Requirements of SPEC X will be implemented
- Structure will be verified per test plan X

Supporting data must be provided for each control identified. (See MIL-STD 1574A, Para. 5.2.14.1). Examples: If the control is a design feature, provide drawing or simplified sketch. If the control is a procedure, summarize procedure and safeguards. (See MIL-STD 1574A, Para. 5.2.10) If the control is a safety factor, or quotes a worst-case environment, summarize how this environment was determined by:

(1) Summarizing analyses.
(2) Referencing Launch Vehicle-induced environment.
(3) Defining boundary conditions.

If the controls are unknown, identify them by a "TBD" (to be determined). They should be identified by Phase 2.

2.4.4.4 Verifying/Finalizing Controls - Identification of controls should be accomplished by the end of the Phase 2 Safety Review. All controls planned should be identified and complete-TBD's or tentative controls could jeopardize Phase 2 completion. Where controls are inhibits, define how it will be verified that environments will not affect inhibits. If a safety factor is used, specify how the factors will be verified (i.e., test or analysis). The status of verification action should be indicated (See MIL-STD 1574A, Para. 5.2.12 and 5.2.14.1). Although most verification cannot be completed until after CDR, the eventual verification of controls should be a consideration from the earliest design phases. Many times contractors have committed to a control, only to be faced with impossible or costly verification.

In addition, specify how and when controls will be verified prior to operation of the system. The acceptable methods of verification (See NHB 1700.7A, Para. 214) and associated backup data are:

(1) Test - summarize test plans and results or attach report.
(2) Analysis - summarize or attach analyses.
(3) Inspection - summarize how/when inspection was performed.

Examples of improper verification:

(1) SPEC X incorporated.
(2) Drawing Y inspected.
(3) Test Plan Z followed.

2.4.4.5 References and Resolution - All design references and resolutions should be completed by the end of the Phase 3 Safety Review. For each control, or verification approach, specific source references must be provided. (See MIL-STD 1754A, Para. 5.2.14.1) Released and controlled references are required to resolve design/test items. Procedural items require the procedure number and the actual hazard control incorporated in the procedure, for resolution. Procedures, however, are generally not completed by the Phase 3 Safety Review.

When resolved, all reports should be signed by the Program Safety Manager, Program Manager, and the Safety Review Team (SRT) or Safety Review Panel (SRP) Chairman.

2.5 PROJECT INTERFACES

System safety interfaces with a wide range of program disciplines. Examples of possible system safety inputs and associated analytical tasks for some disciplines are listed.

System/Subsystem Design

(1) Provide safety criteria and requirements to designers.

(2) Review and provide safety input into system and component specifications.

(3) Review interface specifications and control drawings for safety.

(4) Review concepts and participate in trade studies.

(5) Support design reviews and technical interchange meetings.

(6) Review schematic diagrams and engineering drawings to assure incorporation of safety controls.

7) Perform safety hazard analyses.

Human Factors

(1) Utilize human engineering design criteria in designing hazard controls.

(2) Utilize human reliability data.

(3) Support human engineering analyses.

Maintainability

(1) Review maintainability plans and analyses for safety impacts.

Reliability

(1) Utilize failure mode analyses and reliability models to assist in the identification of failure points.

(2) Identify safety critical components for reliability analysis.

(3) Review reliability plans and analyses for safety.

System Test

(1) Provide safety criteria and requirements.

(2) Identify special safety tests if needed in addition to the normal test program (for hazard control verification).

(3) Review and approve test plans and procedures, and standard operating procedures to insure proper hazard controls are included.

(4) Review test set-ups and monitor potentially hazardous tests.

Quality Assurance/Product Assurance

(1) Review corrective action requirements with safety impact.

(2) Review customer deficiency reports with safety impact.

(3) Identify potential hazards and control requirements.

(4) Serve on certification boards.

(5) Inspection of safety critical components.

Configuration Management

(1) Review and approve engineering changes for safety.

(2) Identify potential hazards and control requirements.

(3) Serve as change authorization committee member/consultant.

Manufacturing and Facilities

(1) Review manufacturing plans, process and analyses for safety.

(2) Identify hazardous materials and operations.

(3) Identify facility safety requirements.

(4) Provide safety criteria and approvals.

(5) Support personnel safety activities.

Maintenance Engineering

(1) Review maintenance engineering analysis, tool lists, test equipment and time lines for safety impacts.

(2) Identify potential hazards and control requirements.

Technical Publications

(1) Review contractor operations and maintenance instructions for safety.

(2) Review technical orders (if applicable) for safety.

(3) Provide safety criteria and requirements.

Training

(1) Review safety training plans and lesson plans.

(2) Provide safety criteria and requirements.

(3) Approve training for potentially hazardous operations.

(4) Input into training certification requirements and certification board.

Ground Operations

(1) Participate in design of GSE for safety.

(2) Assess operating procedure sequence flow to eliminate hazardous conflicts/situations.

(3) Assess capability of support equipment and facilities to safely interface with the launch vehicle and/or payload, personnel.

(4) Review and approve standard operating procedures to insure proper hazard controls are included.

Flight Operations

(1) Review operating procedures for hazards and associated controls; either those resulting from crew activities or those having an effect on the crew.

Environmental Engineering

(1) Assess design adequacy to maintain safety in predicted environmental exposures, i.e.; for thermal, acoustic, contamination, vacuum, RF, overpressure, humidity, loads, shock, vibration, etc.

2.6 PROGRAM PHASES AND TASKS

The program phases and parallel safety activities discussed in this section are portrayed graphically in chronological order, with a brief discussion following each Figure. It is for a typical DOD STS payload from the payload builder's viewpoint. There are many more contractor safety tasks not addressed here, such as those of the safety verification contractor. A single border, surrounding a Figure item in this section, identifies continuing tasks performed during the program phase, whereas a double border identifies a milestone meeting or event. All too often emphasis is placed on meetings or events, when the bulk of the safety job is done in-between.

Non-STS payload programs should adapt this as required, and should find most of the discussion applicable, with the exception of the phase safety reviews. In lieu of the phase safety review, the safety program status is traditionally presented in conjunction with the applicable program review (SSR, SDR, PDR, etc.), or safety working group meeting. Although they are not listed in the Figures, it is essential that the requirements of the counterpart Range Safety documents be recognized for non-STS operations. These are contained ESMC 127-1 for Cape Canaveral Air Force Station and WSMC 127-1 for Vandenberg Air Force Base.

2.6.1 Conceptual (See Figure 2-12)

Event:

1. Request for Proposal (RFP): The request for proposal is issued by the procuring activity and contains the Statement of Work (SOW) which identifies the tasks the procurement activity desires the contractor to perform. The RFP also contains listings of compliance documents and a Contract Data Requirements List (CDRL).

2. Proposal Activity: During this activity the contractor prepares the proposal in response to the RFP. The proposal usually contains a draft System Safety Program Plan (SSPP) and a discussion on how each SOW task and requirement document will be met. Trade studies are usually initiated in this phase to evaluate alternative approaches to respond to the RFP. At this point the safety manager should review the proposal for the following points:

a) Organization:
Reporting level of safety manager.
Relationship between safety and other disciplines.
Can the safety manager effectively do the job in the proposed organization?

b) Requirements:
Does the program recognize and understand the requirements?

c) Methodology:
Is the safety manager submerged and ineffective in the program or is his job at the right level - and effectively directed toward the end events and products?

3. Authority to Proceed (ATP): After evaluation of all proposals, sources selection, fact finding, and negotiations the ATP is issued to begin work.

4&5. Requirements Definition and Concept Development: The safety activities here involve updating the SSPP, continuing trade studies, input to specifications, and identification of safety requirements, usually by use of safety checklists.

2.6.2 System Definition (See Figure 2-13)

Event:

6. System Definition: This phase finalizes the design requirements and establishes the system design baseline.

7. Allocation of Requirements: Results of trade studies, preliminary hazard analyses, risk factor matrix, and all other safety tasks are used to generate the safety requirements. These are then disseminated to design engineers for their incorporation. The safety checklist is the tool usually used for this task.

8. System Requirements Review: The objective of this review is to ascertain the adequacy of the contractor's efforts in defining system requirements. It is usually conducted when a significant portion of the system functional requirements have been established. Safety requirements should have been firmly established by the time of this review. The safety manager should present these results.

9. System Design: The safety activities in this phase are of utmost importance in establishing an effective system safety program. The safety engineer must ensure that all identified hazards have been incorporated in the PHA so as to influence the design and to allow for the eventual incorporation of hazard control(s). A safety program can have a major cost avoidance impact if this is done properly. Safety design features required later in the program can have a large cost impact. A properly prepared SSPP with the required management support for implementation will allow this task to be accomplished smoothly.

10. System Design Review: This review is usually conducted when the definition effort has proceeded to the point where system requirements and the design approach are more precisely defined (i.e., alternate design approaches and corresponding test requirements have been considered and the contractor has defined and selected the required equipment, logistic support, personnel, procedural data, and facilities). The intent of the review is to ensure a technical understanding between the contractor and the procuring activity. The safety manager should present the results of the safety activities.

11. Phase 0 Safety Review (STS only): The purpose of this review is to determine if the contractor has adequate planning, qualified personnel, managerial authority, and resources to complete the safety review process. (SDR 127-8, para. 3-4, Phase 0 Safety Review, soon to be released). In addition, emphasis is given to the SSPP, Preliminary Hazard Analysis and the safety requirements allocation. The resources which the contractor intends to apply to the program are also carefully assessed for DOD programs. (safety man hours, engineering man hours, etc.)

2.6.3 System Development (See Figure 2-14)

Event:

12. System Development: This phase of the program implements the design to its lowest level and establishes the operational concepts. At the end of this phase is the Critical Design Review (CDR) and the Phase 2 safety review, at which time all design hazard controls should have been identified.

13. Develop Subsystem Requirements: The safety efforts here are nearly the same as for (Event 7) except the detailed design requirements for subsystems and components are identified and development of the Accident Risk Assessment Report (ARAR) is initiated.

14. Preliminary Design Review: This review is conducted prior to the detailed design process to (a) evaluate the progress and technical adequacy of the selected design approach; (b) determine its compatibility with the performance requirements of the development specification; and (c) establish the existence and compatibility of the physical and functional interfaces between this system and other systems, facilities and Ground Support Equipment (GSE).

15. Phase 1 Safety Review (STS only): The purpose of the Phase 1 Safety Review is to assess the preliminary design to ensure all design and operational hazards have been identified. This review concentrates on the identified hazards and causes, and evaluates intended design controls. Compliance with requirements is assessed, especially NHB 1700.7A. (SDR 127-8, Para. 3-5, Phase 1 Safety Review, soon to be released).

16. Subsystem Design: This effort is nearly the same as for (9) except the design concentrates on the subsystem and component levels.

17. Critical Design Review: This review is conducted when the detail design is essentially complete and fabrication drawings are ready for release. The purpose of this review is to (a) determine that the design satisfies the design requirements established in the specifications, and (b) establish the exact interface relationships between the system and other systems, facilities and GSE.

18. Phase 2 Safety Review (STS Only): The purpose of the Phase 2 Safety Review is to evaluate the system at the critical design review level to ensure all hazards existing in the payload and its associated support equipment (ASE/GSE) have been identified and hazards effectively controlled by design and oeprational failures of the system, subsystems and related support equipment, and that appropriate means of verification of hazard control implementation and effectiveness have been defined. This review concentrates on the final hazard controls and their incorporation into the final design and intended verification techniques. Also, the anticipated operational scenario (flight and ground) is assessed to assure that proper procedural controls are planned. Compliance with requirements is assessed, especially NHB 1700.7A and SAMTO HB S-100/KHB 1700.7. It is important that all design related safety issues be resolved by this review since the next program phase is manufacture/test.

2.6.4 Manufacture/Test (See Figure 2-15)

Event:

19. Manufacture/Test: During this phase the design safety features are incorporated into the hardware and the essential safety related procedural controls are implemented. Safety monitoring of many of the tests is required to ensure both the safe conduct of tests and to collect data for hazard control verification. Many of the verifications to be performed by inspection and analysis are completed during this phase.

20. Phase 3 Safety Review (STS only): The intent of this review is for the contractor to present final hazard reports with all controls incorporated and verified for both the flight hardware and ground support equipment. It is recognized that all operating procedures may not be completed by this time, but hazard reports should reference the proper procedure where controls are to be incorporated. The remaining open items are tracked on a log to ensure safety validation prior to first use. (See MIL-STD 1574A, Para 5.2.10)

21. Integrated Safety Review (ISR) (STS only): The ISR is intended to review the cargo mix for an STS flight. Since each cargo element (payload) should have completed Phase 3 by this time, payload contractor involvement should be as an advisory role and to provide a completion status of open log items. The integrating contractors' results are the main items of evaluation.

22. Safety Certification: The last meeting of the Safety Certification Panel (SCP) is to brief the SD commander on the results of the safety review program. The outcome is a signed letter of safety certification.

23. Flight Readiness Review (FRR): The FRR is the milestone by which time the cargo should have completed safety certification.

2.6.5 System Use (See Figure 2-16)

Event:

24. System Use: This phase involves the ground processing, launch, orbital operations, and return of the payload (as applicable). The contractor should provide safety support during the pre-launch processing and be available for consultations during the actual mission.

25. Post Flight Analyses: If flight or ground hardware is to be re-used, the contractor should review test and operational results and assess the safety impacts. This effort also applies to series payloads where "identical" pieces of hardware are used; modifications may have a safety impact. Considerations should include refurbishment and safety critical limited life items.

2.7 SUMMARY OF ACCIDENT RISK ASSESSMENT IN REQUIREMENTS DEFINITION

The purpose of any risk assessment is to provide some estimate of the accident risk involved in the testing, operation or maintenance of a system, subsystem, facility and related procedures. This assessment is a tool used by management, designers and planners in making decisions related to the design and operation requirements to be imposed on the system.

There may be a tendency to regard the assessment as the culmination of the system safety analysis process; as the end product of the system safety effort. The system and subsystem hazard analysis are the basis for system and subsystem accident risk assessment reports and are usually submitted at the Critical Design Review, when the system designed is pretty firm. It is important to remember, however, that the assessment process is begun in the earliest stages of the system development process - in the PHA. The assessments done in this early phase of analysis may not be formally documented or delivered but they may be the most significant and powerful of the overall assessments produced. The reason is that early assessments based on the PHA establish the requirements for hazard controls in the system design. If the hazards associated with alternative designs or procedures are

accurately identified and the hazard control requirements are properly presented to decision makers, major hazards may be eliminated from a system before it is on the drawing boards. And this is the essence of the system safety philosophy: establish the system design requirements as early as possible in the development life cycle. Effective and realistic risk assessment to provide hazard control requirements definition early in the program is the key.

Early in the development phase the threat of failure to meet performance objectives may tend to overshadow efforts to reduce mishap risk. Because it represents a negative aspect, mishap risk reduction is often overlooked in the glare of management optimism. Where it is not overlooked entirely, mishap risk may be appraised but not deeply enough to serve as a significant input for decision making. As a result, the sudden identification of a significant mishap risk, or the occurrence of an actual incident, can provide an overpowering impact on schedule, cost, and sometimes performance.

To avoid this situation, methods to reduce mishap risk must be applied commensurate with the task being performed in each program phase. In the early development phase (system conceptual phase and system definition), the System Safety task is usually directed toward: 1) establishing risk acceptability parameters; 2) practical tradeoffs between engineering design and defined mishap risk parameters; 3) avoidance of alternatives with high mishap risk; 4) defining system test requirements to demonstrate safety characteristics; and, 5) safety planning for follow-on phases. The culmination of this effort is the mishap risk assessment which is a summary of the work done toward minimization of unresolved safety concerns and a calculated appraisal of the risk. Properly done, it allows intelligent management decisions concerning acceptability of the risk. Mishap risk management is a concept which, if properly used, can provide a practical, cost-effective method to reduce risk. Mishap risk management will not work effectively without full support of all concerned management levels. Planning for reduction of mishap risk requires coming to grips with the hard details of program execution. It involves examination and re-examination of problems that are anticipated. It requires an effective management system by which these problems might be solved - a management system applied with intelligence to assure a proper system safety balance to achieve safety objectives with the least possible impact on cost, performance and schedule.

Quantitative Assessment - In any discussion of accident risk management and assessment, the question of quantified acceptability parameters arises. While it is not impossible to obtain meaningful results from such a program, care should be exercised so that the program balance is not disturbed. In any high risk system, there is a strong temptation to rely totally on statistical probability since it looks on the surface like a convenient way to measure safety. Before embarking in this direction, be sure that the limitations and principles of this approach are well understood and that past engineering experience is not ignored. Acceptability parameters must be well defined, predictable, well demonstrated, and useful. Useful in the sense that they can easily be converted into design criteria. Many factors fundamental to system safety cannot be quantified. Design deficiencies are not easily examined. Also, the danger exists that System Safety analysts and managers will become so enamored with the statistics that simpler and more meaningful engineering processes could be ignored. Quantification of certain specific failure modes that depend upon one or two system components may be effective to bolster the

decision for acceptance or correction. Be careful! Arbitrarily assigning a quantitative measure for a system creates a strong potential for the model to mask a very serious risk. For example, on the Peacekeeper project, the only quantified analyses required are Fault Trees. They provide numerical probabilities for undesired nuclear weapons related events specified in AFR 122-10, Nuclear Weapon Systems Safety Design and Evaluation Criteria.

In the design of certain high-risk systems such as nuclear weapon systems, there may be a strong tendency to rely solely on statistical analysis. Regarding program management, this appears reasonable since it provides a convenient medium to express safety in terms that unknowledgeable managers can relate to. One trap for the unwary is the failure to establish reasonable limits on the acceptability of a probability of occurrence. On one such program, risks with an apparent probability of occurrence of 10^{-42}, could lead managers into a false sense of security. Let us consider this in terms that are easily related: for instance, money. If it may be assumed that a single dollar bill is three thousandths of an inch thick, the probability of selecting that bill from a stack of bills which is three inches high (or 1000 dollars) is 1×10^{-3} (or 1 chance in 1000). One million dollars is a stack 250 feet tall. The chance of selecting that single dollar bill from the stack is now 1×10^{-6} or one chance in a million. When we go to 1×10^{-9}, or one chance in a billion, our stack is now over 47 miles high. One chance in a trillion is 47,000 miles high! When we talk in terms of 1×10^{-42} our stack probably would not fit in the galaxy! The point is that we have to establish realistic, reachable safety goals so that management may make intelligent decisions. In this particular instance, the safety analyses dwelled upon the probability of the impossible and allowed a single human error, with a probability of occurrence in the range of 1×10^{-3}, to cause a near disaster; mainly, because it was not a quantifiable element. It is doubtful if the decision-makers were fully aware of the accident risks they were accepting, but were placated by a large, impressive-looking number.

In order to help mitigate pitfalls such as this, it is recommended that the probability analysis technique of fault tree be combined with the qualitative techniques of integrated risk assessments.

The general principles of accident risk management are:

(1) All human activity involving a technical device or process entails some element of risk.

(2) Do not panic at every hazard.

(3) Keep problems in proper perspective.

(4) Weigh the risks and make judgments according to your own knowledge, experience and program need.

(5) Encourage other program disciplines to adopt the same philosophy.

(6) All system operations represent a gamble to some degree.

(7) System Safety analysis and risk assessment does not free us from reliance on good engineering judgment.

(8) It is more important to establish clear objectives and parameters for risk assessment than to find a cookbook approach and procedure.

(9) There is no "best solution" to a safety problem. There are a variety of directions to go in. Each of these directions may produce some degree of risk reduction.

(10) To point out to a designer how he can achieve a safety goal is much more effective than to tell him his approach will not work.

(11) Safety is a condition which can seldom be totally achieved in a practical manner. Therefore, there are no "safety problems" in system planning or design. There are only engineering or management problems which, if left unresolved, may cause mishaps.

Safety Concerns and Risk Acceptance - Many times safety critical aspects or risk factors are identified during the conduct of a System Safety analysis task that cannot be satisfactorily resolved or closed out by the contractor. In these cases, a complete risk assessment is made of the condition.

The problem is elevated to the procuring activity for action as a "Safety Concern." Based on the contractor's risk assessment, a decision is made to take some sort of action to resolve the issue. If the decision is to do nothing or to leave the condition as is, Department of Defense and Air Force regulations (DODI-5000.36, AFR 800-16) require that the program manager document his acceptance of the mishap risks identified. Although acceptance of risk may appear on the surface to be easily resolved, it can become quite complicated. Mishap risks can be accepted by the program manager only when the effects of the mishap are contained entirely within program controlled resources. If the effects of a mishap can be generated across interfaces and damage resources under control of another agency, mishap risks can only be accepted with concurrence of the highest management authority within that operation.

A concerted effort by the System Integrator, and all contractors involved is required to ensure that the integrated system meets system level safety requirements for the test range and for the operational system. If a condition exists that violates a safety rule common to all of the interfacing agencies, then an agreement from each of these agencies that the mishap risks are adequately controlled is required. This usually takes the form of a waiver or deviation request. Approval of the waiver request is then a joint agreement that the risk presented by noncompliance is acceptable. Few of these agencies will accept a waiver to the same requirement for a series of flights, so the request must be resubmitted each time the agencies resources are used. After first use, the program office must be prepared to correct the problem if the request is refused.

It is the task of the resource user to independently verify and present evidence to the resource controlling agency that specified requirements have been met. This presentation usually is required to identify methods used to effectively control mishaps. In the case of the example shuttle payload, design specifications, engineering drawings, control procedures, documented inspection, and test results are required to verify risk control. The resource control agency needs to be assured that user equipment does not present an uncontrolled hazard which will cause damage to their equipment or injure any personnel. When so many agencies are represented this can be a formidable task.

2.8 REFERENCES

(1) NHB 1700.1 (V7), "System Safety"

(2) Department of Defense Instruction (DOD-I)-5000.36, "System Safety Engineering and Management"

(3) Department of Defense Directive (DOD-D)-3200.11, "Use, Management and Operation of Department of Defense Major Ranges and Test Facilities."

(4) Air Force Regulation (AFR) 800-16, "USAF System Safety Programs"

(5) Military Standard (MIL-STD)-882B, "System Safety Program Requirements"

(6) Military Standard (MIL-STD)-1574A, "System Safety Program for Space and Missile Systems"

(7) SAMSO STD #79-1, "Integrated System Safety Program for the MX Weapon System"

(8) Western Space and Missile Center Regulation (WSMCR) 127-1

(9) Eastern Space and Missile Center Regulation (ESMCR) 127-1

(10) Roland and Moriarty, System Safety Engineering and Management, Wiley, New York, 1983, p.p. 64-68

(11) Martin Marietta MCR 82-800, Rev. B, 29 September 1982, "DOD Safety Review Team Lessons Learned Data Base," Lesson No. 001.0A-00175

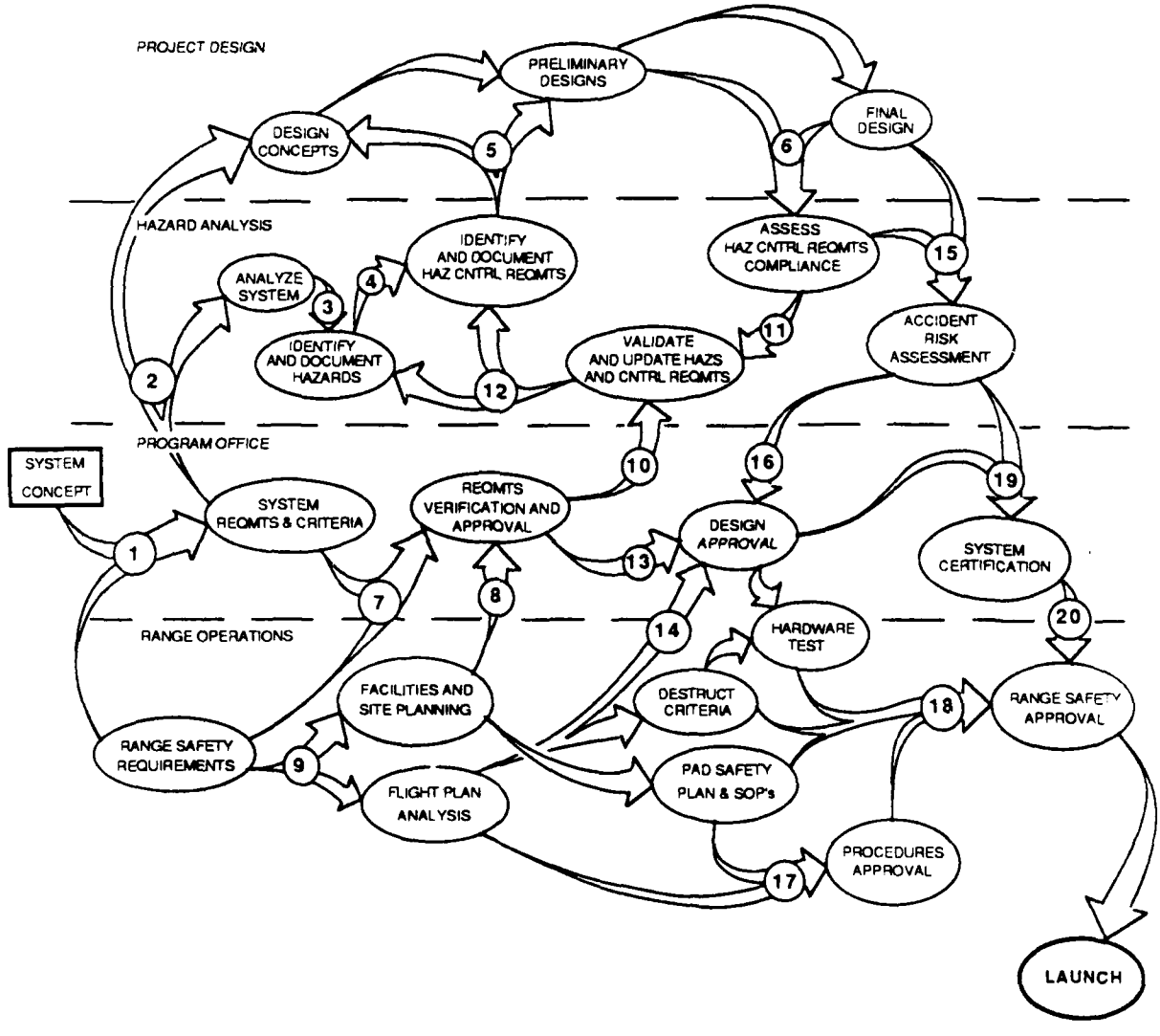
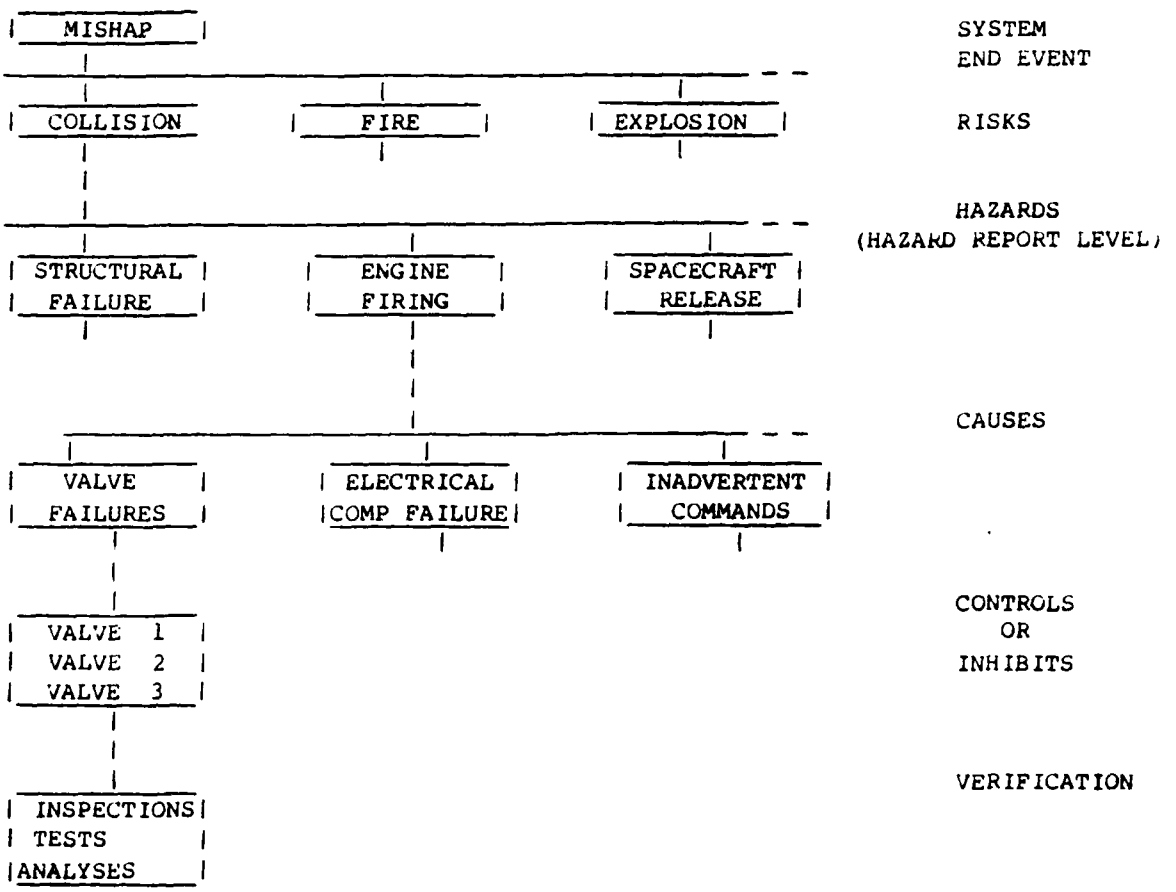


Figure 2-1 The Hazards Analysis Process



NOTE: This figure is for illustration of the analytical logic which should be applied in preparing safety analyses. Do not attempt to draw it for the entire program.

Figure 2-2 The Hazards Analysis Flow

Hazard Identification Checklist

ITEM	Hazard Group	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.

Figure 2-3 Hazard Identification Checklist (Page 1 of 4)

Hazard Identification Checklist (Continued)

ITEM	Hazard Group	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 controls. 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.

Figure 2-3 Hazard Identification Checklist (Page 2 of 4)

Hazard Identification Checklist (Continued)

ITEM	Hazard Group	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.

Figure 2-3 Hazard Identification Checklist (Page 3 of 4)

Hazard Identification Checklist (Continued)

ITEM	Hazard Group	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. Distrotion 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.

Figure 2-3 Hazard Identification Checklist (Page 4 of 4)

POTENTIAL HAZARD MATRIX

Date:
Page:

System: Activity/Phase / Subsystem/Component	Design	Fabrication	Handling And Transportation	Subsystem Tests	Assembly/ Erection	Integrated System Tests	Flight Readiness Tests	Flight	Deployment	Retrieval	Reentry	Landing	Refurbishment	Maintenance

Figure 2-4 Example Potential Hazard Matrix Form

HAZARD ANALYSIS

HAZARD LEVEL (4)		NO. (1)	
STATUS (5)		PAGE (2)	
PROGRAM PHASE (6)		DATE (4)	
SYSTEM: (7)	SUBSYSTEM:		
OPERATION/PHASE: (9)			
HAZARD TITLE: (10)			
REFERENCES: (11)			
HAZARD DESCRIPTION: (12)			
POTENTIAL EFFECTS: (13)			
ASSUMPTIONS/RATIONALE/CAUSES: (14)			
HAZARD CONTROL REQUIREMENTS: (15)		STATUS (19)	REFERENCE (16)
VERIFICATION: (17)		(19)	(18)
DISPOSITION: (20)			
ORIGINATOR/LOCATION: (21)	CLOSURE SIGNATURES: (22)		
	SAFETY MANAGER	PROGRAM MANAGER	

Figure 2-5 Example Hazard Analysis Sheet Format

SYSTEM SAFETY CHECKLIST

PROG-ELEMENT (1) System Safety - Master Text

SOURCE (2) ESMCM 127-1, Vol 1, 01 Sept 1972

TITLE (3) RANGE SAFETY MANUAL

COMPLETED BY (4)

DOCUMENT DATE 05Jan81 (5)

LAST REVISION DATE (6)

PAGE 1 (7)

DOC # Rev	ITEM No	CRITERION	SYSTEM	COMPLIANCE (11)	NON COMPL (12)	NOT APPL (13)	RESOLUTION (14)	REFERENCE (15)
ddd.rr-	nnnnn	(9)	(10)					
(8)								
352.01-	00001	All missiles/space vehicles flown from or on the Eastern Test Range shall be equipped with a flight termination system. Flight termination shall consist of thrust termination and destruct. (1.2.2.1)	AQ					
352 01-	00002	The flight termination system shall be capable of terminating thrust on all stages until final impact point is established or orbital injection occurs. (1.2.2.1)	AQ					
352 01-	00003	Obviously erratic flight shall require flight termination. (1.2.2.3)	AQ					
352.01-	00004	Flight termination line violation shall require flight termination. (1.2 2.3)	AQ					
352.01-	00005	Unknown performance shall require flight termination. (1.2.2.3)	AQ					
352 01-	00006	All hazardous missile/space vehicle systems and associated ground support equipment shall be designed, tested, operated and approved in accordance with Chapters 3, 4 and 5 of AFETRM 127-1. (See later items in this checklist for details.) (1.2.4)	AG D					
352 01-	00007	At least two adequate and independent sources of instrumentation are required for each phase of powered flight. (1 2 5.1)	AHUS					
352 01-	00008	At least one tracking aid compatible with Range instrumentation shall be carried on all launch vehicles to improve tracking capability and data quality. (1.2.5.2)	AHUS					

20DEC82

Figure 2-6 Example System Safety Checklist (Master File)

SYSTEM SAFETY CHECKLIST

DOC. & Rev — ITEM No

PROG-ELEMENT Skynet 4 (1)

SOURCE MIL-STD-1512 STS TAILORING (2)

TITLE ELECTROEXPLOSIVE SUBSYSTEM (3) ELECTRICALLY INITIATED, DESIGN REQUIREMENTS AND TEST METHODS TAILORED FOR SPACE TRANSPORTATION SYSTEM (STS) PAYLOADS

COMPLIANCE | NON-COMPL | NOT APPL

COMPLETED BY: D.J. Ray (4)

DOCUMENT DATE: 15APR83 (5)

LAST REVISION DATE: 05NOV84 (6) PAGE 13 (7)

ddd.rr-nnnnn (8)	CRITERION (9)	SYSTEM (10)	COMPLIANCE (11)	NON-COMPL (12)	NOT APPL (13)	RESOLUTION (14)	REFERENCE (15)
103.02-00127	Shields. The firing circuit shall be completely shielded, or shielded from the EED back to a point in the firing circuit at which filters or absorptive devices eliminate RF entry into the shielded portion of the system. (Para. 5.5a)	BHU1	X			Shielding provided from RF filters or PRU (as applicable) to EEDs. Full compliance pending review of approved, released and configuration-controlled engineering documentation.	RPT/UKS/45629/BAe, ARAR, Issue 5, Appendix A, HR-1A, 1B & 5
103.02-00128	Shielding shall provide a minimum of 85 percent of optical coverage ratio. (Para. 5.5b)	BHU1	X			90% shielding provided by chosen wire. Full compliance pending review of approved, released, and configuration-controlled engineering documentation.	RPT/UKS/45629/BAe, ARAR, Issue 5, Appendix A, HR-1A, HR-1B, Controls 3(c)
103.02-00129	There shall be no gaps or discontinuities in the shielding, including the termination at the back faces of the connectors. (Para. 5.5c)	BHU1	X			Shields bonded to "circumference of the connectors at each end of the pyro harness". Also, "the shield is electrically bonded around the circumference of the NSI, and around the RF absorber". Full compliance pending review of approved, released, and configuration-controlled engineering documentation.	RPT/UKS/45629/BAe, ARAR, Issue 5 HR-1, Control 3(c)
103.02-00130	Shields terminated at a connector shall be electrically joined with no gaps around the full 360 degree circumference of the shield. (Para. 5.5d)	BHU1	X			See item -00129 above	
103.02-00131	Electrical continuity of electroexplosive subsystem circuitry shields shall be maintained. (Para. 5.5e)	BHU1	X			See item -00129 above	
103.02-00132	If the electroexplosive initiator is enclosed in a metal container which provides attenuation equal to or greater than the shield, the shield may be terminated at the container	BHU1	X			Only enclosed EEDs are in 2134A Safe & Arm device which provides requisite shielding. Full compliance pending successful qualification of 2134A.	RPT/UKS/45629/BAe, ARAR, Issue 5, Appendix A, HR-5, Verification

9JAN85

Figure 2-7 Example System Safety Checklist (Project)

TYPE	SYSTEM	SUBSYSTEM	COMPONENT
A All aspects of design and operations.	G Applicable to all systems/subsystems.	I Environmental	1. Humidity
B Design, Hardware	H. Airborne equipment/ hardware		2. Temperature (high/low)
C Design, Software, Firmware	I. Ground equipment, ground support equipment, ground		3. Pressure (high/low)
		----------	----------
		* Human factors	
		----------	----------
	J. Facilities	JA Elevator JB Cranes JC Vehicles	
		----------	----------
		U. Electrical/Electronic	1. Components-cables, connectors, wires, inhibits
			2. Circuitry, drawings, grounding, insulation
			3. Generators, power
			4. Computers
			5. Instrumentation, monitoring, command
			6. Lightning strike
			7. Electrostatic discharge
			8 Battery
		----------	----------
		V. Mechanical	1 Components valves, fasteners, rivets, screws, inhibits
			2. Structure
			3 Vibration, shock, acceleration, collision
		----------	----------
		W Pyrotechnics, Ordnance	1. Initiators, detonators (A-the
			2 Solid Rocket Motors/propulsion subsystems

Figure 2-8 Example System Safety Master Checklist Coding System (Page 1 of 4)

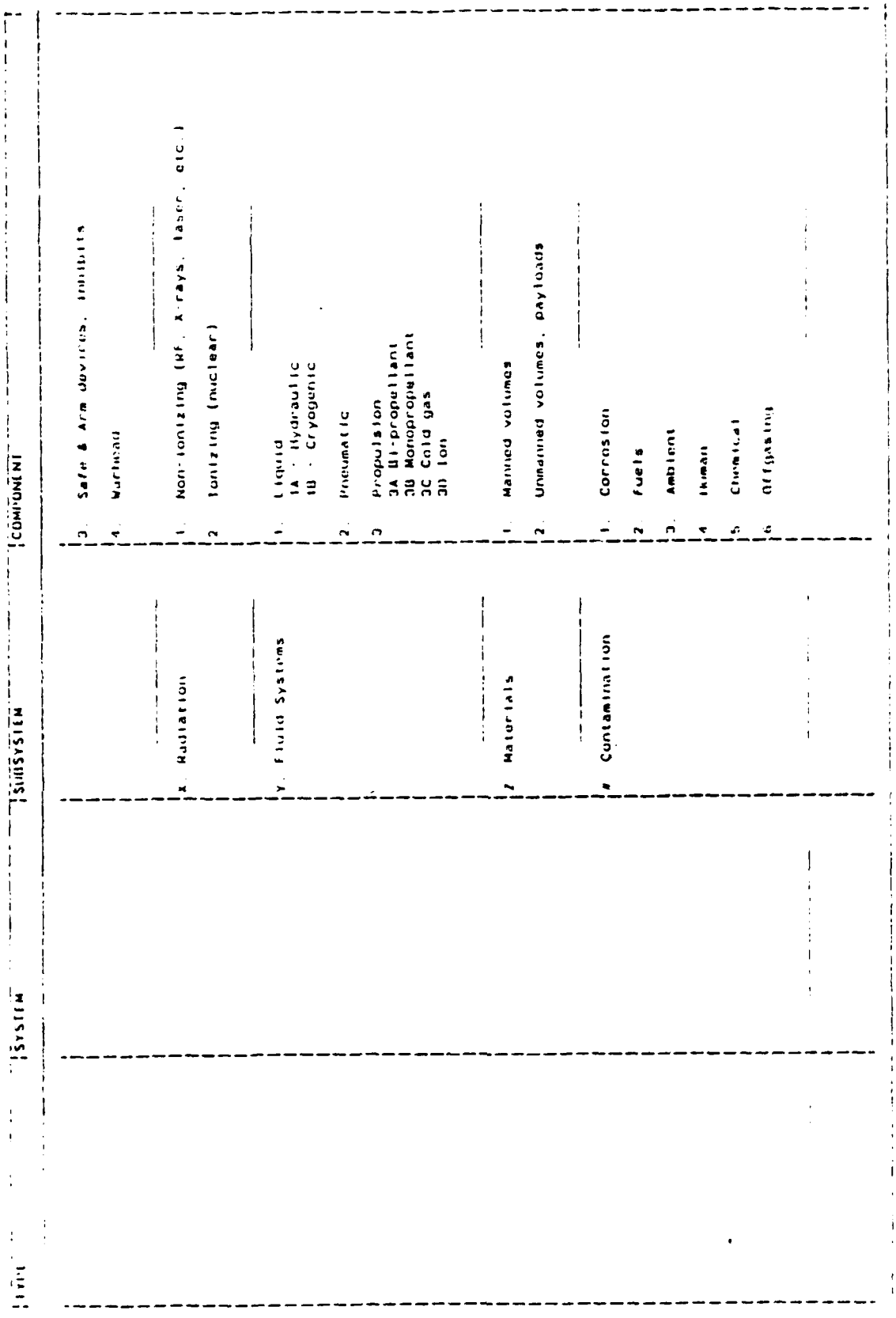


Figure 2-8 Example System Safety Master Checklist Coding System
(Page 2 of 4)

Item		SYSTEM	SUBSYSTEM	COMPONENT
B	Operations	K Fabrication, assembly, construction		
		L Handling, transportation, storage		
E	Training	M Subsystem tests, qual. tests, acceptance tests, test-general		
		N Integrated system tests		
		O Maintain readiness		
		P Launch		
		Q Flight, landing, flight termination, flight systems		
		R Maintenance, inspection (including safety inspections)		
		S Emergency, Contingencies, Post Safety, hazard operations subsystem, rescue, evacuation, EVA		
		T Procedure (subsystem integrated)		
F	Management Administration	1 Applicable to all System Safety Programs		
		2 Reference		
		3 Analyses, compliance data, other documentation, plans, studies, engineering changes, reviews, requirements		

Figure 2-8 Example System Safety Master Checklist Coding System
(Page 3 of 4)

Figure 2-8 Example System Safety Master Checklist Coding System
(Page 4 of 4)

HAZARD CATALOG

PART I - HAZARDS LIST

SYSTEM: (1) PAGE (2)

HAZARD NUMBER	HAZARD	ELIMINATED	RESIDUAL	CONTROLLED	ACCEPTED	OPEN
(3)	(4)	(5)	(6)	(7)	(8)	(9)

HAZARD CATALOG

PART II - RESIDUAL HAZARDS

SYSTEM: (4) ITEM NO.: (1)

SUBSYSTEM: (5) HAZARD LEVEL: (2)

COMPONENT: (6) DATE: (3)

HAZARD DESCRIPTION: (7)

RECOMMENDATION: (8)

DISPOSITION: (9)

Figure 2-9 Example Hazard Catalog Format

| NO. /REV: |

PAYLOAD	HAZARD LEVEL
SUBSYSTEM	DATE
OPERATION/PHASE	CLOSURE LEAD

HAZARD/UNDESIRED EVENT:

CAUSAL FACTOR/ASSUMPTIONS:

APPLICABLE REQUIREMENT:

HAZARD CONTROLS	STATUS	REFERENCE

VERIFICATION METHODS	STATUS	REFERENCE

REMARKS:

CLOSURE CONCURRENCE:

PROJECT SAFETY ENGINEER		DATE:
PROJECT MANAGER		DATE:
SRT CHAIRMAN		DATE:

Figure 2-10 Hazard Report Form (DOD STS)

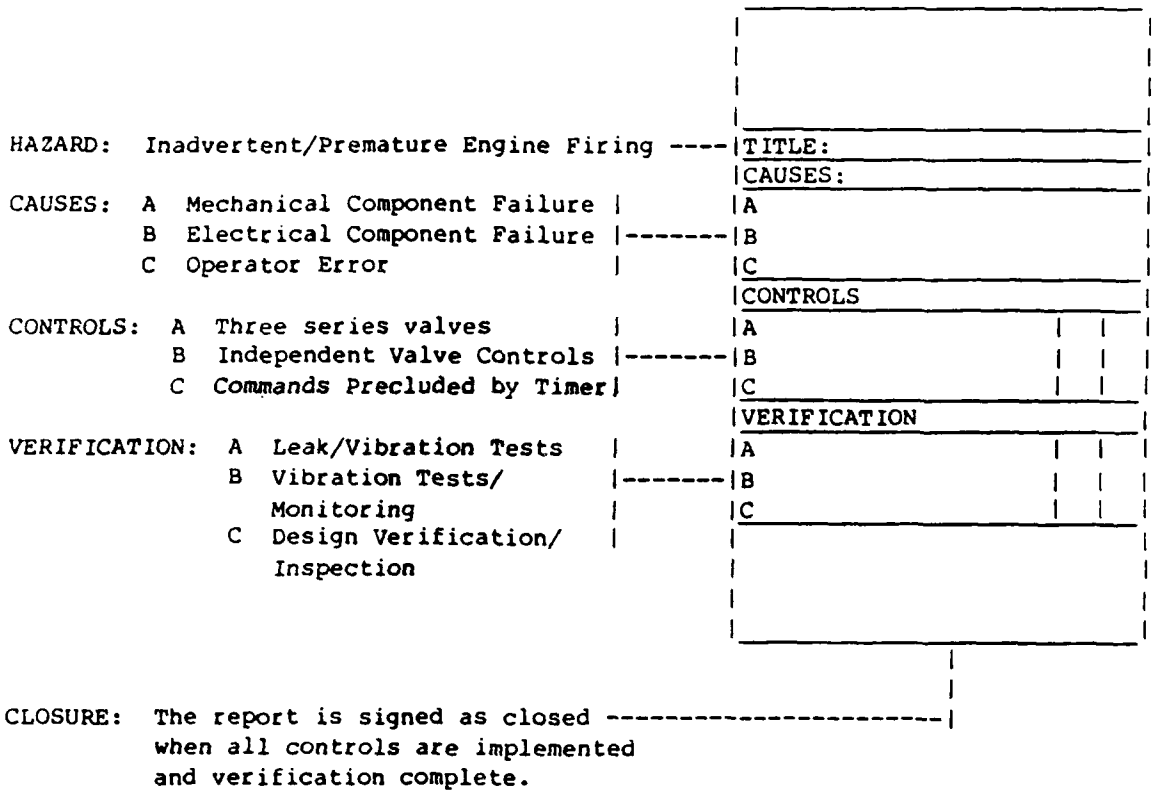


Figure 2-11 Sample Hazard Report Data

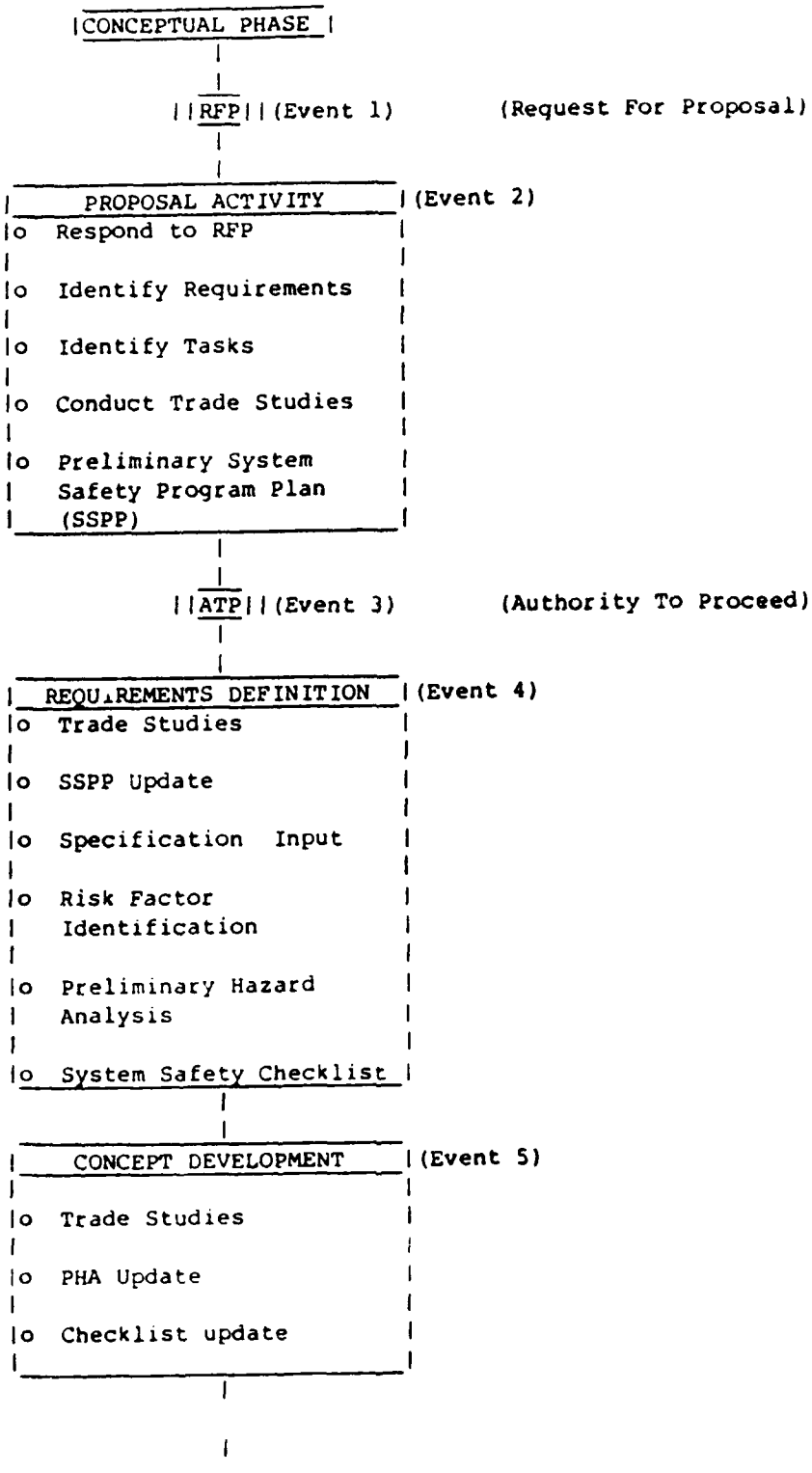


Figure 2-12 Concept Phase

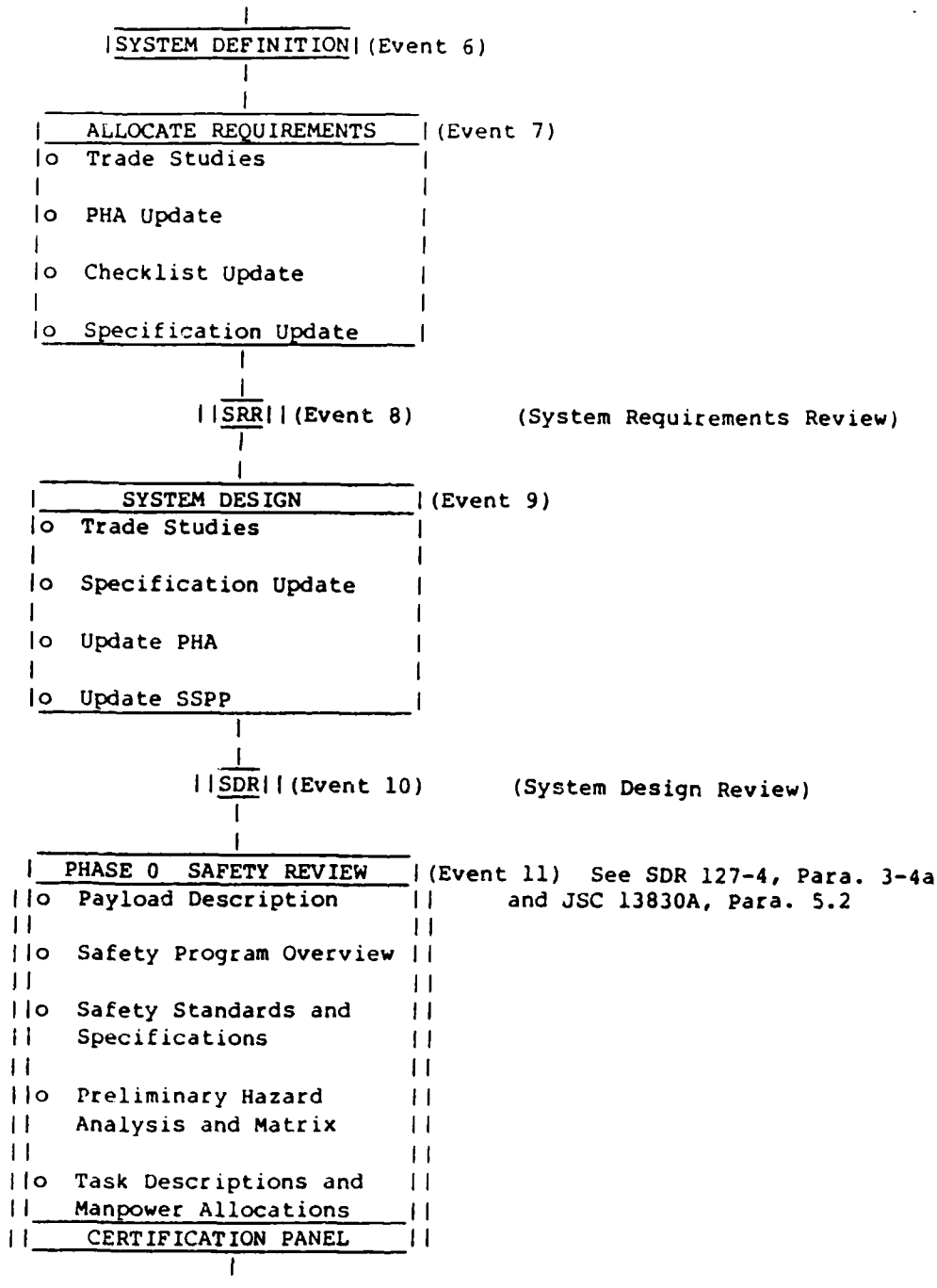


Figure 2-13 System Definition Phase

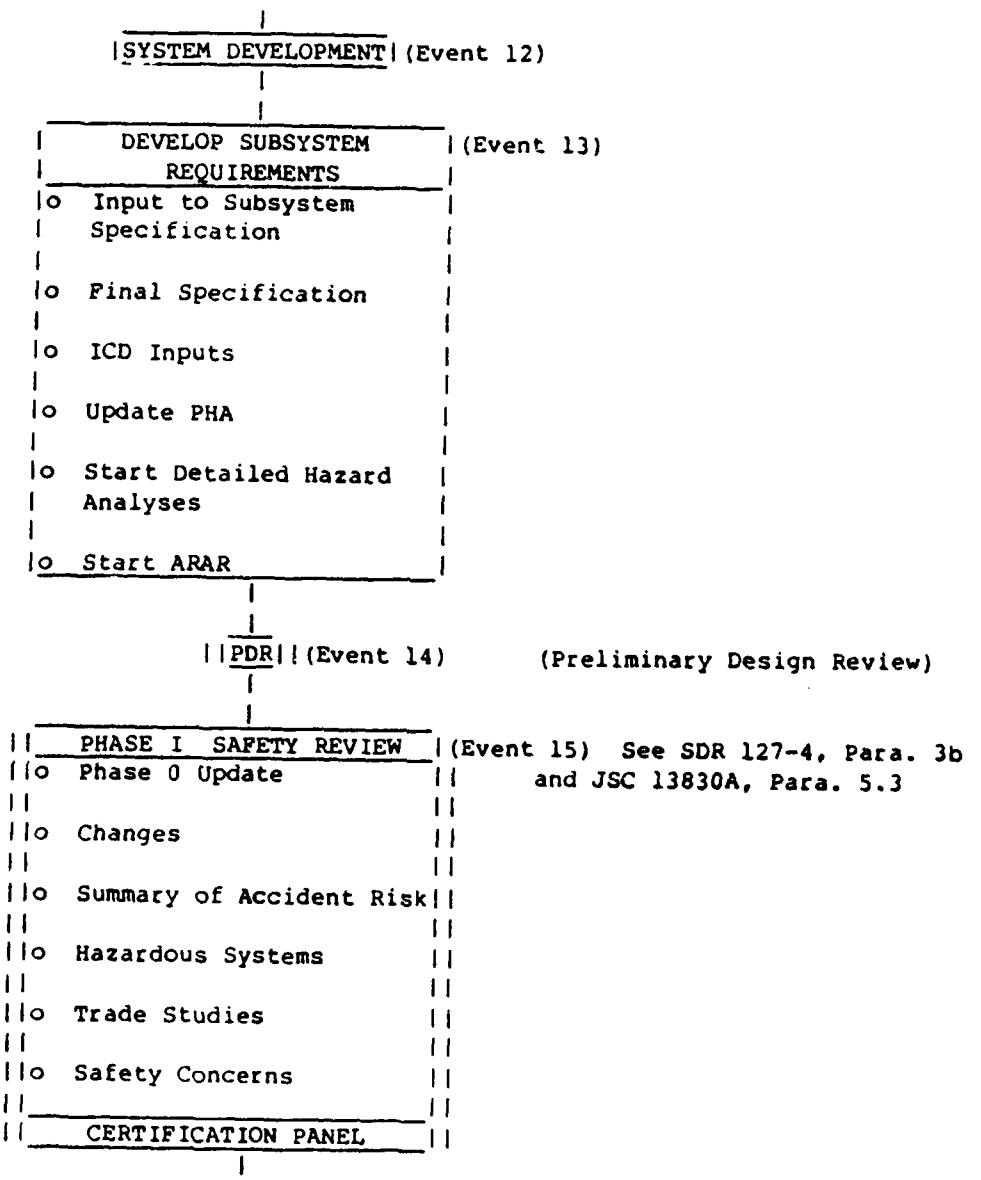


Figure 2-14 System Development Phase (Page 1 of 2)

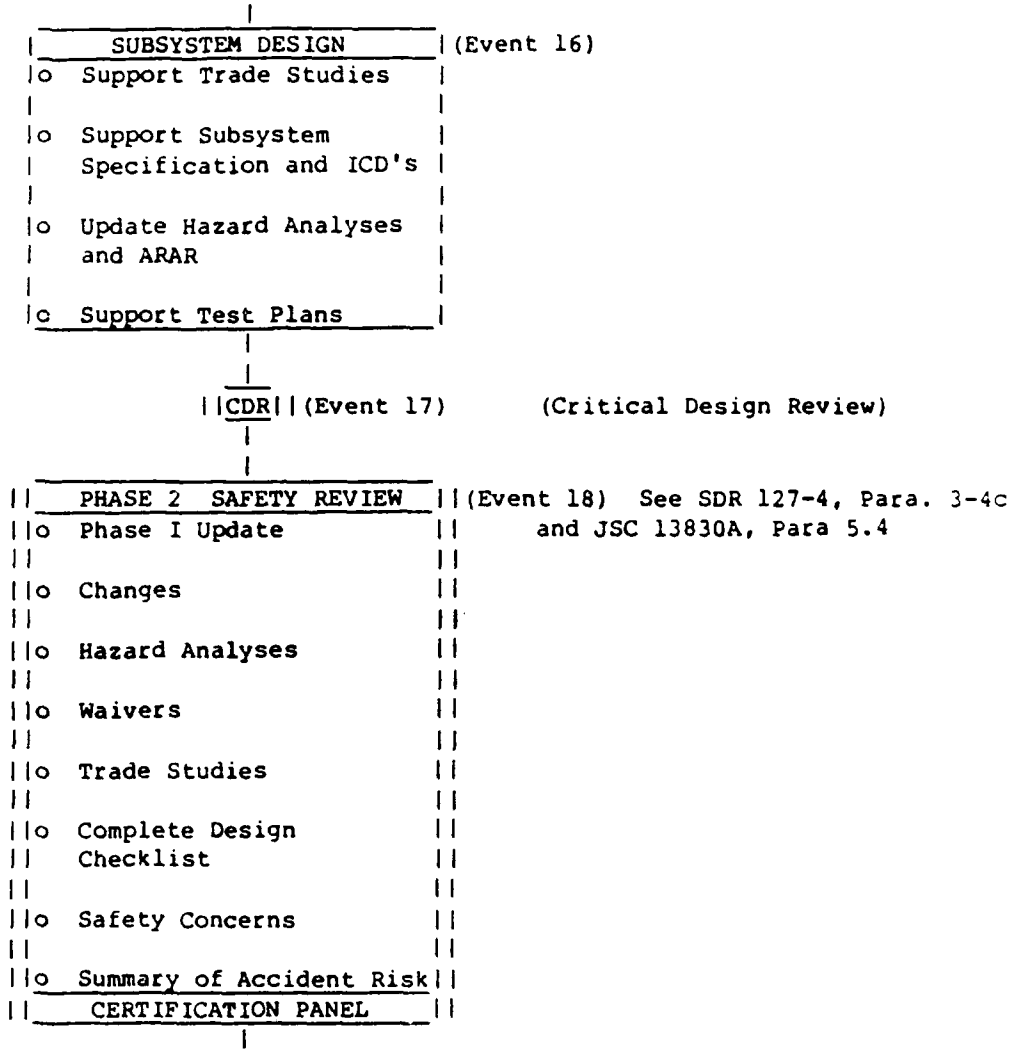


Figure 2-14 System Development Phase (Page 2 of 2)

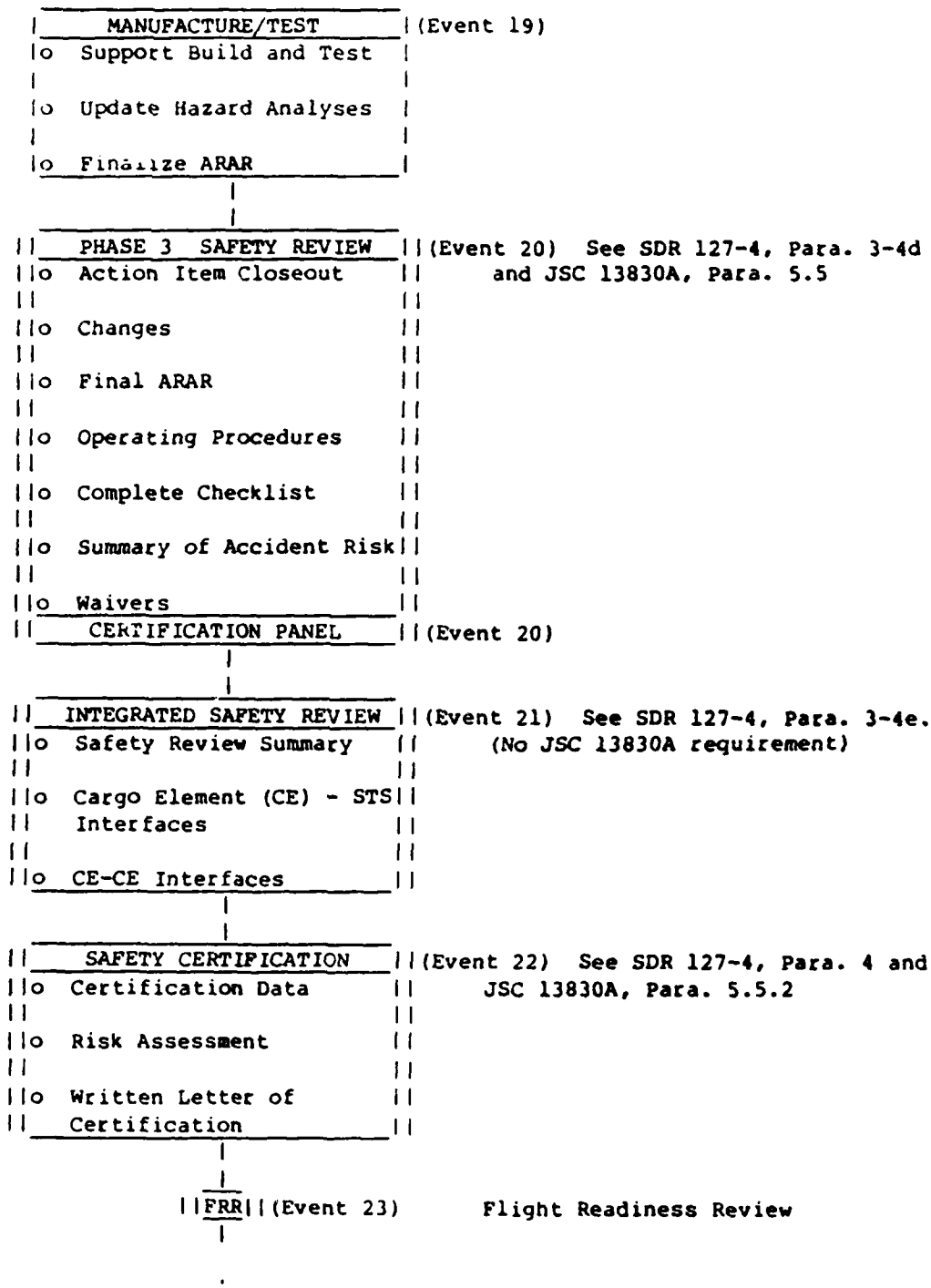


Figure 2-15 Manufacture/Test Phase

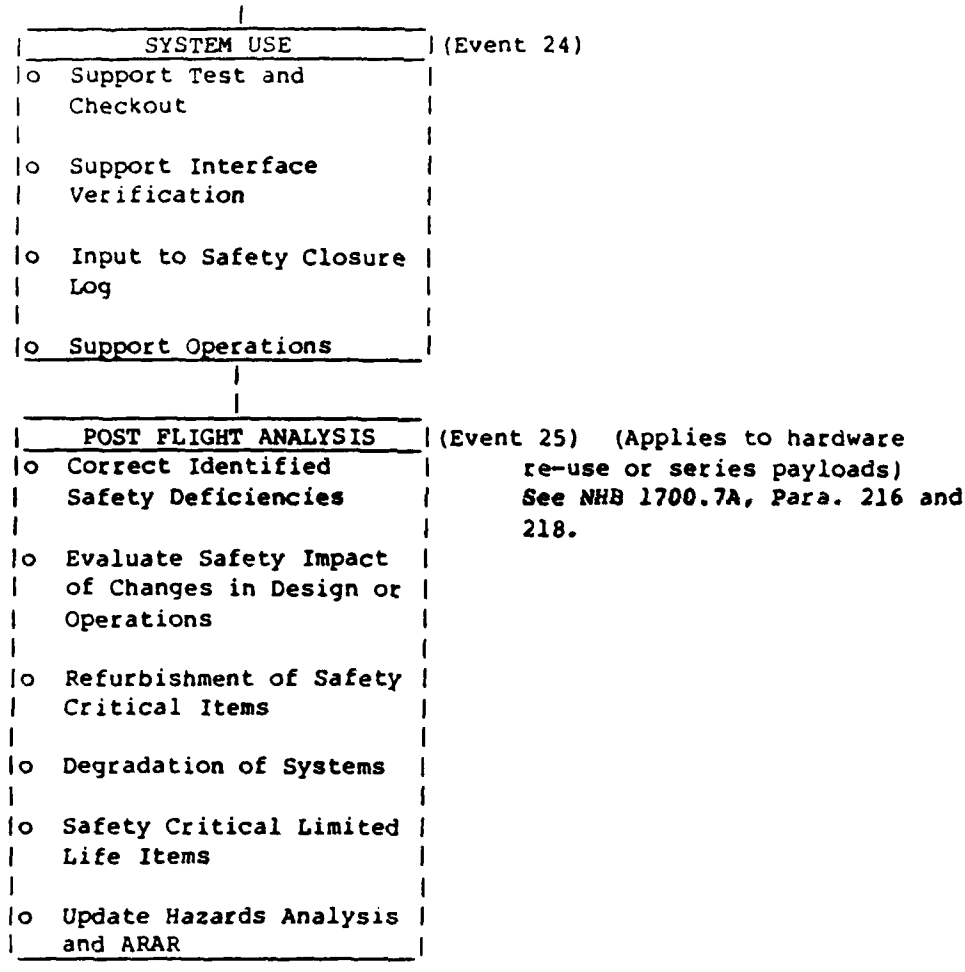


Figure 2-16 System Use Phase

Chapter 3
Accident Scenarios

CHAPTER 3
ACCIDENT SCENARIOS

TABLE OF CONTENTS

Section	Title	Page
3.0	Introduction	3-1
3.1	Accidents and Post Accident Environments - General	3-1
3.1.1	Liquid Propellants	3-2
3.1.2	Solid Propellants	3-3
3.2	Flight Termination Systems	3-4
3.3	Accident Definitions	3-8
3.4	Accident Dynamics	3-11
3.5	Accident Scenarios and Their Development	3-12
3.6	Accident Scenarios - Analytical	3-14

LIST OF FIGURES

Figure No.	Title	Page
3-1	Cause and Effect Relationships In Accident Phenomenon	3-30
3-2	Accident Scenario Relationships.	3-31

CHAPTER 3
ACCIDENT SCENARIOS

3.0 INTRODUCTION

The purpose of the Hazards Analysis Process is to manage accident risk to acceptable levels, wherein accidents can be viewed as any unplanned event which results in major injury, death, or system and property loss beyond defined limits. Accident Risk Assessment can be both formal or informal. In its formal application, accident risk assessment is directed at predicting the risk of experiencing a certain type, or types, of accident(s). In its informal application, accident risk assessment can be thought of as the continuing process of assessment and verification of minimum and adequate controls for hazardous conditions existing in a system. Accident scenarios and the effort to develop them can also be formal or informal. The function of accident scenarios as discussed in this chapter of the SPHAM is to provide the event data necessary for formal accident risk assessment of space vehicle propulsion systems during prelaunch and flight operations. However, all efforts to develop accident scenarios regardless of their formality can benefit from the methods and data of this chapter.

The effort to develop accident scenarios can, should, and often do lead to corrective action or subsequent measures to reduce risk. These risk mitigation efforts are not the subject of this chapter and are treated throughout the SPHAM.

3.1 ACCIDENTS AND POST ACCIDENT ENVIRONMENTS - GENERAL

In both the prelaunch and flight phases of space vehicles, the accidents which have the greatest consequence are those which potentially involve mixing and/or detonation of propellants. The specific scenario will have a large influence on the explosive yield, and the resultant blast overpressure, fragmentation, and thermal effects and thus on the severity of the post accident environments and the subsequent threat to life, health and property. The properties and effects of these environments are discussed in detail in Chapter 5. A general discussion of these factors is useful here.

Liquid propellants and solid propellants are handled separately because their geometric chemical configurations are different. In the case of solid propellants, the fuel and oxidizer are already mixed homogeneously and therefore the accident scenario does not have to account for mixing. Liquid propellants, on the other hand, are configured in separate tanks of fuel or oxidizer and therefore the accident scenario must account for the type and amount of propellants and their probability of mixing.

3.1.1 Liquid Propellants

Several things are important with regard to liquid propellants and their potential explosive yield. This includes the initial vehicle geometry, types of fuel and oxidizer tanks and their configuration, length to diameter ratio of the tanks, whether they have a common bulkhead, whether there are multiple tanks for both fuel and oxidizer, relative tank location, total quantity of each propellant, and the types of propellant, either cryogenic or hypergolic. For each liquid propellant missile system there are a diverse number of ways in which the propellants can be mixed. These were originally defined and used during the project PYRO in the early 1960's and include the following:

(1) Unconfined. Propellants are spilled into the atmosphere during flight.

(2) Confined by Ground Surface (CBGS). Propellants are spilled and spread over a large surface area with minimal confinement.

(3) Confined by Missile (CBM). Propellants are spilled and are confined by some kind of structure (missile, silo, etc.) or are mixed internally within the tankage (e.g., failure of common bulkhead).

(4) High Velocity Impact (HVI). Propellants are released and mixed due to a high velocity impact with a ground surface.

- Hard Surface — Propellants tend to spread over a large surface area with minimal to intermediate confinement.
- Soft Surfaces — Surface craters upon impact; propellant collects in crater to provide a higher degree of confinement and mixing.

An example of an event in a scenario that could lead to a liquid propellant spill and mixing accident during prelaunch operations is tank overpressurization (or underpressurization) during propellant loading. A failure of the propellant tank will cause spill of one or both propellants. If hypergolic propellants are involved, a fire will ensue if both propellants spill and mix. In the case of cryogenic propellants, the propellants may spill and mix forming an explosive mixture that may not be initiated unless an ignition source is present. The most credible scenarios that can lead to propellant spill and mixing accidents during prelaunch operation involve propellant loading and propellant tank pressurization after loading is complete just prior to liftoff or in the case of hypergolics, 2-3 days before liftoff. Specific failure modes include failures in the propellant servicing system, such as service line rupture, scrubber failure, connector failure, non-scheduled venting, etc. It should be pointed out that in mishaps at both National Ranges the spills have been confined in most cases to the planned hazard area.

A failure during launch operations can result in any one of the mixing modes discussed above. Confinement by the ground surface or the missile (CBGS or CBM) are most likely to occur during the first few seconds of flight. Typical failure modes in the scenario would be loss of thrust immediately after liftoff, engine boat-tail explosion, guidance system failure, or engine actuator failure, or destruct action resulting from loss of flight control.

Depending on the launch vehicle and mission, high velocity impact is possible from the first few seconds of flight until approximately T+30 seconds. The precise time frame during which high velocity impact is a credible accident event is a function of the vehicle performance characteristics and Range Safety missile rules for errant vehicle flight. Higher performance vehicles with high thrust to weight ratios may impact during errant flight before the Range Safety Officer can send destruct commands. A low performance vehicle allows the Range Safety Officer greater time to disperse the propellants prior to ground impact. The credibility of this scenario must be addressed as a function of the specific vehicle performance, Range Safety mission rules and destruct system capability.

If destruct action can be taken in flight, propellant mixing is unconfined and the destruct action will disperse the propellant, limiting the amount of mixing because an ignition source is present to burn the propellants before the mix. The history at both Ranges is that the liquid propellant explosive yields following inflight destruct action are extremely low or non-existent.

3.1.2 Solid Propellants

Since solid propellants contain a homogeneous mix, fuel and oxidizer mixing is not an issue. The key variables which determine the explosive potential and its credibility for solid propellants include the following:

(1) The chemical constituent and the reactivity of the propellant, i.e., is it a mass-detonating or a mass-fire solid propellant formulation?

(2) The propellant mass and general configuration including length to diameter ratio, web size, thickness, core configuration, loading density and case confinement including case material and thickness.

(3) Propellant grain physical characteristics such as grain toughness, modular elasticity, propellant granular bed characteristics, critical diameter.

(4) Response to shock (SDT).

(5) Response to impact, reduce shock (XDT).

(6) Response to DDT.

Solid propellant can react in one of several ways as a function of the scenario. Typical scenarios include inadvertent ignition that can result in propulsive flight or pressure rupture of the case; shock impact from a fragment resulting in ignition, detonation or pressure rupture; intact high velocity impact resulting in a low order explosion or complete detonation; inflight destruct action resulting in a pressure rupture or detonation. Each of these responses will depend on the characteristics of a particular propellant and its configuration.

In general, the most credible failure mode in a solid propellant accident scenario that can lead to these events during prelaunch operation is inadvertent ignition from an external ignition source which would ignite the motor case to become propulsive with resulting impact and pressure rupture. It is unlikely during prelaunch operations that any true detonation or high order explosion would occur no matter what the propellant configurations are since the stimulus available would not be sufficient to initiate this type of reaction.

During the early period of flight from T-0 to at least T+50 seconds any large solid propellant rocket motor stage could fail by case rupture or burn-through, destruct action, guidance failure, loss of nozzle or loss of guidance actuation. In the event of an inflight pressure rupture due to destruct action of a monolithic motor such as the Minuteman, Navy Fleet Ballistic missile, or Castor configured motor, the results would be to spew large quantities of burning propellant fire brands throughout the area. It is unlikely that they would have a sufficient mass or sufficient size to explode on impact. The other credible failure mode for this class of motor would be the scenario where the destruct action could not be taken in time to prevent an intact impact. If the impact velocity is above 300'/second there is at least a 50% chance that the result would be a high order detonation or at least a low order explosion depending on the type of propellant, mass, confinement, hazard classification and potential for propellant granulation. It has been shown through sub-scale tests and full scale launch aborts that not only will mass detonating Class 1.1 solid propellant explode but also Class 1.3 composite propellants can detonate or explode if their grain is sufficiently damaged and the impact is at high enough velocity. The other classes of solid propellant motors are the segmented large space boosters such as used on Titan and Shuttle launch vehicles. The same inflight failure modes apply to these motor configurations but the resultant chunks of solid propellants may be big enough to explode on ground impact. In addition, the size and energy of the case fragments present a significant hazard. They can range up to 10,000 lbs of weight with surface areas of several square feet and travel at velocities of 300'-400' second.

3.2 FLIGHT TERMINATION SYSTEMS

This section provides a brief discussion of the "Destruct" systems normally employed for any missile or space system approved for launch from either the Eastern or Western Test Range (ETR or WTR). There is a dangerous tendency on the part of system developers and range users to rely on the proper functioning of these systems to ensure ultimate protection of life, health and property. In effect, there is a tendency to assume that the "Destruct" event is the end event in any credible accident scenario which may result from a vehicle failure. In reality, Flight Termination Systems may not function or may only function partially for a variety of reasons. Any effort

to develop accident scenarios for a specific system and flight plan should include analysis of the credibility of vehicle events which preclude proper functioning of inflight destruct and the consequences which result.

Any vehicle which operates from either ETR or WTR should be expected to carry the necessary airborne elements of a Flight Termination System, which will function to terminate the flight of the vehicle by command from the Range Safety Officer (RSO). For those vehicles where it is reasonably possible for stages to separate inadvertently and flight termination cannot then be commanded, it should be expected that the Flight Termination System (FTS) will include elements to accomplish flight termination, or "Destruct" automatically upon separation.

Flight termination systems now in use accomplish one or both of the following functions:

(1) Thrust Termination - Thrust termination in Solid Rocket Motors is currently accomplished by splitting or separating the SRM case, releasing chamber pressure and destroying nozzle thrust. Thrust termination in liquid propellant systems is generally accomplished by isolating the liquid rocket engine from the tankage by shutting a valve in the feedline.

(2) Fuel Dispersion - Fuel dispersion is accomplished in liquid propellant systems to disperse those propellants into the atmosphere. Fuel dispersion is activated to reduce the explosive yield of liquid propellant produced by confined mixing, either in the atmosphere or upon ground impact.

The two flight termination functions can be commanded independently. Automatic flight termination initiates both functions simultaneously. Confusion does sometimes exist regarding the conditions sufficient to initiate an automatic flight termination.

Automatic flight termination is generally initiated by breaking a wire, or wires, and destroying continuity. These "break" wires are normally attached to structure forming the attachment between stages or segments. The automatic flight termination function will initiate only upon breaking of those wires. This would typically include inadvertent separation of a stage, or a vehicle failure which would damage the structure to which the wires are attached. What is important to understand is that only a portion of the failures in a vehicle which would ultimately require termination of flight will initiate an automatic flight termination. It may be logical to expect that a certain type of vehicle failure may initiate automatic flight termination, but it would be illogical and dangerous to assume that it always will. The case failure of a strap-on SRM can be expected to produce automatic flight termination either as a result of structural damage and wire breakage from the case rupture itself or structural breakup from the vehicle loads and thrust forces after SRM case failure. It may be dangerous to assume this will always be the case, depending on the phase of flight and the nature of hazards being carried.

For the purpose of developing accident scenarios, it is useful to categorize the reasons for inability to terminate flight in the following manner, in order of likelihood:

(1) Time - The flight termination command signal results from human detection, analysis, decision and command initiation in response to available flight data. The total elapsed time required for the sequence of flight termination events, starting with the detection of a vehicle anomaly and ending with the completion of flight termination will vary with many factors, including

(a) The specific nature of the vehicle failure,
(b) The detection method which initially and most clearly reveals the failure,
(c) The mission phase at the time of failure,
(d) Environmental conditions affecting the detection method.

Human detection relies on one or more of the following, each of which is best suited to specific vehicle failures and phases of flight:

(a) Visual - Included in this category are launch observers and skyscreen operators. The skyscreen operator is the principal means of verifying the flight path of the vehicle during and shortly after lift off. It should be remembered that the cloud of reaction products which envelops the launch vehicle at the time of ignition and lift-off obscures much of the launch.

(b) Video - There are a number of video images available to the RSO at his location during launch from the time of ignition until well into the flight of the vehicle.

(c) Tracking - The RSO has available position, velocity and impact prediction data from a variety of types and locations of radars and data processors. The six tracking modes which may be used in some combination on any flight include autotrack, on-axis track, skin-track, beacon track, edge track and s-band angle track.

(d) Telemetry - Telemetry data establishes vehicle performance in real time. Telemetry data transmitted from the vehicle is available to the RSO by display and by communication with telemetry console monitors.

The time required to accomplish a commanded in-flight destruct action is probabilistic. There are no guidelines or criteria available. Expert opinion for the time required to accomplish flight termination on an expendable launch vehicle, starting with initial detection, varies in the range of 4 sec. to 10 sec. Accident scenarios should consider possible accidents which could occur within the time required for flight termination. Examples are:

(a) Can the vehicle impact ground, either by fallback or under propulsion, before thrust termination and or fuel dispersion can occur?

(b) Can the vehicle failure propagate and destroy or otherwise preclude functioning of the on-board flight termination system before the command can be received and implemented?

(2) Failure Effect on Flight Termination - It is possible for a failure within a vehicle to result in the inability of the flight termination system to function. The possibility of this event in a given vehicle reflects the inherent vulnerability of the airborne flight termination system elements to credible vehicle failure modes and their effects. There are many factors which affect the vulnerability of flight termination elements to vehicle events, and raise or lower the likelihood of survival of the system for the time required to accomplish a commanded flight termination. Examples include:

(a) Co-location - Many elements of airborne flight termination systems are redundant. If redundant elements are located in the same vicinity, the likelihood of damage to both elements as a result of a vehicle failure increases.

(b) Hazard Source Proximity - Location of functional flight termination elements in the vicinity of a hazard source which can damage those elements, if released, increases vulnerability.

(c) Environmental Protection - The degree of protection or isolation from environments which can be created as a result of vehicle failures will strongly influence vulnerability. Specific environments include fragmentation, heat, high shock, G-loads, rapid corrosion, acoustic vibration. It should be pointed out that the environments created as a result of a failure do not relate to the environmental limits or extremes expected during operation, and successful qualification to those limits does not relate in any way to vulnerability to vehicle failures.

(d) Wiring/Cable Run - The factors discussed above pertain to the vulnerability of components and wiring. Other factors such as length routing, distance between support clips, etc., affect the vulnerability of airborne wiring to vehicle failures.

The purpose of (2) is not to establish vulnerability and survivability criteria for flight termination elements. The purpose is to establish that these elements may be vulnerable to damage from vehicle failure events. Accident scenarios developed for risk assessment purposes should include accidents resulting from vehicle events which result in the inability of the flight termination system to function.

There are other factors which should be given consideration as part of an effort to identify credible accidents which result from loss of flight termination capability. These may include:

(3) Command signal attenuation produced by vehicle position, trajectory, attitude and maneuver which may result from a vehicle failure.

(4) Tracking errors or confusion produced by the separation and relative trajectory of stages or major segments of the vehicle.

3.3 ACCIDENT DEFINITIONS

The best assurance of complete accident scenarios and credible formal risk assessment is good accident definitions. Any effort to develop accident scenarios for the purpose of formal risk assessment should start with a clear statement of what they are for, i.e., the risk for which assessment is required in as clear terms as possible. It is this statement which defines the accidents which are of interest, or logically results in a definition of the accidents which are of interest. Accident definitions then can be derived from the risk assessment goal, and initiate the effort to develop accident scenarios.

The following illustrate risk statements and resultant accident definition (for example).

Risk Statement

What is the chance (risk) of an inadvertent radioactive release?

Accident Definitions

What are the ways (scenarios) that a radioactive release can occur in the atmosphere (accident) during flight?

and/or

What are the ways that a radioactive release can occur during prelaunch operations or as a result of ground impact during flight?

The above statements may be of interest in the case of a payload containing a Radioisotope Thermoelectric Generator (RTG) and launched aboard an expendable launch vehicle, for example.

It is most likely that formal risk assessments and the corresponding accident scenarios will be developed at a program or mission level. In this case, it is typical for a large number of organizational entities to participate in the effort, each having expertise and responsibility for different elements of the hardware, software or operations. In this case, the risk assessment effort can be managed most efficiently by deriving accident definitions for each organization from the mission or program level risk statement. Using the above example, accident definitions provided the launch vehicle contractor may be:

(1) What are the ways and their probabilities that a launch vehicle failure can result in a ground impact of an RTG-equipped payload with one or more intact vehicle stages?

and

(2) What are the ways and their probabilities that a launch vehicle failure can occur and result in confined mixing of the fuel and oxidizer in a liquid propellant stage, including the upper stage?

and

(3) What are the ways and their probabilities that a launch vehicle failure can occur and produce segments and fragmentation that can impact the payload airborne (exclusive of 2).

Accident definitions direct the analysis to scenarios that produce the defined accident(s). Accident definitions can be used to encourage (or eliminate) consideration of factors which can reasonably be anticipated at the program or mission level. In the launch vehicle example above, the accident definitions provided the launch vehicle contractor can be used to encourage consideration of vehicle events which preclude functioning of the on-board flight termination system (FTS) as discussed in Section 3.2. Accident definition (1) may be rewritten as the following example:

(1A) What are the ways and their probabilities that a launch vehicle failure can occur and sufficiently damage the on-board FTS such that the RTG-equipped payload impacts ground with one or more intact vehicle stages.

(1B) What are the ways and their probabilities that a launch vehicle failure can occur and result in a ground impact of an RTG-equipped payload with one or more intact vehicle stages before the FTS command signal can be received.

(1C) What are the other ways and their probabilities that a launch vehicle failure can occur and result in a ground impact of an RTG-equipped payload with one or more intact vehicle stages?

In the above illustrations, certain knowledge or assumptions may have been inherent in the accident definitions. For example, it may be known, or assumed that the environment produced by an in-flight destruct and/or a land impact of a separated payload or a separated payload and vehicle stages with dispersed propellants may not threaten the integrity of the RTG and produce a radioactive release. These types of accidents then become eliminated from the accident definition. There may be concern, however, over the integrity of the RTG-equipped payload after ground impact with velocities greater than an established maximum. This could produce the accident definition:

(1D) What are the ways and their probabilities that a launch vehicle failure can occur and result in the ground impact of a separated payload with a velocity in excess of the maximum?

it may be argued that accident definitions that are too rigid or premature may result in some types of accidents being ignored and an incomplete risk assessment. It is the responsibility of the risk assessment management to ensure that.

(1) All organizational elements understand thoroughly the accident definitions provided them.

(2) All organizational elements understand the risk assessment goal.

(3) Allorganizational elements understand the inductive logic, including assumptions, which yielded the accident definitions from the risk assessment goal.

If this is done, the organization elements participating in the development of accident scenarios can assists in redefining the accidents or adding to the accident definitions as the analsis proceeds, and as failure effects become understood.

Accident scenarios that are developed without prior and adequate accident definitions come at a high price:

(1) Considerable time can be spent identifying, analyzing and documenting failure modes and their effects which do not contribute to the real risk for which measurement is desired.

(2) There is no assurance that the accident scenarios are thorough and complete and the real risk is understood. This is because the analysis lacks clear objectives, and because it becomes tempting to use the deductive results of functional FMEA as the starting point.

3.4 ACCIDENT DYNAMICS

An accident scenario is an analytical model of a phenomenon which ends or results in some form of loss. The next section treats conventions and approaches for the model. In this section we will briefly discuss the "dynamics" of the phenomenon.

The basic law governing all accidents is the law of Cause and Effect. The cause and effect relationship of the events and conditions which define the dynamics of an accident are complex. Any attempt to represent them requires simplification. Figure 3-1 is an effort to graphically illustrate the dynamics of an accident in the form of "snapshots" of the cause and effect sequence which constitutes the total phenomenon. The elements of Figure 3-1 are described as follows:

(1) Loss - Loss is the ultimate and final outcome as the result of the accident. It is measured in terms of life, health, property damage and dollars. There are some realities of loss which are not always apparent to the developers of accident scenarios or to the managers of risk assessment.

(a) Loss is not avoided by reducing accident risk. Reducing accident risk reduces expected loss. Precluding the accident precludes the loss.

(b) Losses which become reality after an accident occurs can be very obscure or hidden to the risk assessment effort. These hidden costs can be billions of dollars.

(2) Accident - The accident is the end event in the accident scenario. It is probably generally true that the accident as defined represents the final event within the system. The post-accident environment created by the accident and the environment of the system at the time of the accident yield or determine the loss.

(3) Triggering Event - A triggering event can best be thought of as an event wherein loss of control of a hazard is realized, i.e., where the state of an uncontrolled hazard exists in the system, or the event which results directly in the loss of control of an existing hazard or creates a new uncontrolled hazard. The triggering event, the mode, phase or sequence of operation, the environment of the system, and the human response to the triggering event will then determine the specific accident form.

(4) Cause - A triggering event cause can be any discrete event preceding the triggering event which can be isolated and described. It will generally be associated with:

(a) The loss of a human, hardware or software function which propagates physically or functionally to result in the loss of control of a hazard.

(b) A human, hardware or software function performed outside of limits.

(c) An unplanned human action which results in (a) or (b).

(d) An unplanned event in the environment of the system.

(5) First Cause - First cause will rarely be defined or isolated in accident scenario development. Once an accident has occurred the ensuing accident investigation may approach first cause in such ways as poor training, employee stress, wrong materials, poor revision control or a host of factors. First cause is significant to accident scenario development only from the standpoint of awareness.

3.5 ACCIDENT SCENARIOS AND THEIR DEVELOPMENT

For the purpose of modeling the phenomenon discussed in the previous section, the analytical relationship between cause, triggering event and accident is best illlustrated by Figure 3-2. What Figure 3-2 means is that a single type of vehicle event may result from many different possible causes and it may have many different possible effects. An example is the triggering event associated with rupture of an SRM case. This event can result from causes within the solid propellant, propellant sealing, case material, case seals and so on. The effect of the SRM case rupture will vary as a function of elapsed time from SRM ignition to failure, activation of ISDS, fragmentation produced, etc., (Reference Section 3.5, item 1B). For the purpose of developing accident scenarios, then, the key event is the triggering event. Identification of triggering events initiates the development of specific accident scenarios.

The overall structure or approach to the development of accident scenarios for formal risk assessment can be summarized as follows:

(1) Verify the risk assessment goal.

(2) Develop accident definitions. These accident definitions are defined by or derived from the risk assessment goal. They represent the types of accidents which can produce the effect for which risk measurement is desired. They should be mutually exclusive. It may be necessary to develop accident definitions for each phase of operation.

(3) Identify triggering events for each defined accident. Since triggering events are identified with, or directly result in, loss of control of a hazard, it can be very useful to start this step with a complete tabulation of hazard sources. The release or loss of control of the source can then be postulated as an initial identification of triggering events. Those events which cannot produce the accidents defined in (2) are discarded.

The credibility of the triggering event may be in question at this point. If so, a preliminary effort to identify possible causes to establish credibility should be made.

(4) Develop assessments of the possible accidents that can result from each triggering event. (It may be desirable at this point to modify the initial accident definitions to reflect the analysis of the possible accidents. The assessments of the possible accidents are more precise and detailed statements of state(s) of the system than are provided by the accident definitions. At this point the analysis takes the structure illustrated by Figure 3-2.

(5) Identify causes for each triggering event. It should be noted that the effort to develop casual data for accident scenarios has only two purposes.

(a) They may be necessary to establish the credibility of a triggering event.

(b) The exact nature of the accident may be a function of the specific cause, and the causes are needed for accident assessment.

If the credibility of the triggering event is not in question, and if causes are not needed for accident assessment, we need not be concerned with them initially.

(6) Review available cause and effect data for additional events and data. Principal sources will be the available FMEAs and Fault-Tree analysis. The results from these data bases should not be substituted for the foregoing steps 1-5. The reasons are:

(a) They have a tendency to deal with only functional failures, and they tend to ignore critical issues such as unplanned human actions, improper human actions or responses to events, secondary damage effects, system environments out of limits, etc.

(b) Their top-level events are not consistent with those of (2) or (3), or the cause and effect relationships are not complete to that level.

3.6 ACCIDENT SCENARIOS - ANALYTICAL

The data of this section are presented to illustrate the development of accident scenarios and to provide data which may be useful for accident risk assessment for specific vehicles and/or missions. The data are limited in that they do not derive from a specific vehicle or mission. They were developed within the frame of reference of an expendable launch vehicle having the following characteristics:

(1) 2 stage core vehicle each using liquid bi-propellant - ignition of the Stage 1 liquid rocket engines occurs near the end of the SRM burn.

(2) 2 solid propellant rocket motors (SRM) with fixed nozzles and fluid injection for thrust vector control. SRMs are strapped to core vehicle. - Ignition occurs at T_o.

(3) Payload consists of a spacecraft carrying hazardous material attached to a liquid bi-propellant upper stage and enclosed by a payload fairing (PLF) shroud.

(4) The 2 SRMs carry attached ordnance to split the SRM case to accomplish thrust termination. The core vehicle and upper stage carry ordnance to accomplish isolation of the rocket engines for thrust termination and ordnance to accomplish fuel and oxidizer dispersion from the liquid propellant tanks.

(5) The flight termination system functions automatically at inadvertent separation of a stage or by command from a ground transmitter.

(6) Jettison of the payload fairing is not accomplished prior to fuel dispersion.

The accident scenarios presented apply to flight operations for the mission phase starting wih SRM ignition to approximately T_o + 30 sec. Accident definitions were derived for this phase assuming that the inadvertent release of hazardous material contained within the spacecraft resulting from a vehicle failure was the risk assessment goal. Those accident definitions are shown in below.

(1) Ground impact of vehicle under propulsion payload first.

(2) Ground impact (fall-back) of payload with intact upper stage with or without payload fairing.

(3) Atmospheric detonation of core vehicle liquid propellants confined by missile and upper stage propellants confined by payload fairing and SRM rupture fragmentation.

(4) Atmospheric detonation of mixed upper stage propellant confined by payload fairing.

For the purpose of this data, it was assumed that normal and proper functioning of the FTS, except for the confinement of upper-stage propellants by the PLF, would not threaten a release of the hazardous material, nor would a ground impact of the spacecraft in the absence of non-dispersed propellants. The accident definitions therefore do not include these events.

Triggering events were defined which could possibly lead to each of the defined accidents. The data was then formatted in the manner of Figure 3-2.

Included in the formatted accident scenario data for event 1A is an indication of the appropriate proabilities associated with each event. The development of probabilities is not the objective of accident scenario development; that is the function of risk assessment. Probabilities are best ignored during the development of scenarios. However, accident scenarios are the basis for risk assessment, and the method of presentation can ease the risk assessment task.

The probabilities associated with the accidents are designated "Conditional Probabilities." These are the probability that the specified accident will occur, given that the triggering event occurs. Ultimately, the probability of a specific accident resulting from a designated triggering event is the product of the probability of occurrence of the triggering event and the conditional probability of the accident.

In practice, the probability of occurrence of the triggering event can be determined or estimated:

(1) at the level of the triggering event itself, perhaps using historical data. An example is an SRM case failure.

(2) in combinatorial fashion using the probabilities of occurrence of the causes multiplied by effect probability where the triggering event is not a certain effect of a cause.

Vehicle Event

(1A) One SRM fails to ignite at ignition

Probability of Occurrence =

Maximum Possible Accident

(1A1) Vehicle partially lifts off and tips over. Upper stage and core vehicle propellant tanks rupture with confined-by-missile and confined-by-ground mixing and detonation. The time required to disperse propellants with range safety action is inadequate.

Conditional Probability of Occurrence =

Other Possible Accidents

(1A2) Vehicle partially lifts off and strikes tower. Tower collision damages structure or SRM attachment initiating the Inadvertent Separation Destruct System (ISDS). Core vehicle propellants are dispersed into the atmosphere. Upper stage propellants are dispersed into payload fairing and detonate.

Conditional Probability of Occurrence =

(1A3) Vehicle partially lifts off. Thrust vector control on functional SRM maintains vehicle attitude sufficiently to allow range safety action. In-flight destruct disperses core vehicle propellants. Upper stage propellants are dispersed and detonate inside payload fairing.

Conditional Probability of Occurrence =

Possible Causes

(1Aa) Ignitor Hang-fire

Probability of Failure =

(1Ab) Ignitor Misfire

Probability of Failure =

Vehicle Event

(1B) SRM case fails in one SRM resulting in loss of thrust.

Maximum Possible Accident

(1B1) SRM failure does not activate ISDS. Vehicle vectors over and impact ground surface, payload first, under propulsion from one SRM. The time required to disperse liquid propellants by range safety action is inadequate.

Other Possible Accidents

(1B2) SRM failure produces case and propellant fragments which rupture core vehicle and/or upper stage propellant tanks producing confined by missile mixing of propellants and atmospheric detonation.

(1B3) SRM failure initiates ISDS event. Core vehicle propellants are dispersed into atmosphere. Upper stage propellants are dispersed and detonate inside payload fairing.

(1B4) SRM failure releases propulsive upper segment. Segment impacts payload fairing and payload, rupturing propellant tanks producing confined propellant mixing and atmospheric detonation.

(1B5) SRM failure produces case and propellant fragments without ISDS. Fragments damage payload and/or core vehicle Command FTS antenna, receivers or cabling. Vehicle veers off course and impacts ground with non-dispersed propellants, payload first.

Possible Causes

(1Ba) Propellant chunks break off exposing SRM case to hot gas.

(1Bb) Propellant slumps or shrinks, opening seal between segments and exposing SRM case to hot gas.

(1Bc) Propellant chunk partially/temporarily restricts flow area or nozzle throat with chamber pressure spike and overpressure of case.

Vehicle Event

(1C) One SRM nozzle and throat separates resulting in loss of SRM thrust.

Maximum Possible Accident

(1C1) Same as (1B1).

Other Possible Accidents

(1C2) Vehicle veers off course. Flight Termination System is activated. Payload propellants are dispersed into payload fairing and detonate.

(TBD)

Vehicle Event

(1D) Loss of thrust vector control - one SRM. (Assume sufficient vehicle control to preclude ground impact)

Maximum Possible Accident

(1D1) Vehicle pitches/yaws/rolls and strikes tower. Tower collision damages structure or SRM attachment initiating an ISDS event. Core vehicle propellant are dispersed into the atmosphere. Upper stage propellants are dispersed into the payload fairing and detonate.

Other Possible Accidents

(1D2) Vehicle clears tower and deviates from flight path. Flight termination system is activated. Payload propellants are dispersed into payload fairing and detonate.

Possible Causes

(TBD)

Vehicle Event

(1E) Loss of thrust vector control - both SRMs.

Maximum Possible Accident

(1E1) Vehicle vectors hard over and impacts ground surface payload first under propulsion. Time required to disperse liquid propellants with range safety action is inadequate.

Other Possible Accidents

(1E2) Vehicle pitches/yaw/rolls and strikes tower. Tower collision damages structure or SRM attachment initiating an ISDS event. Core vehicle propellants are dispersed into the atmosphere. Upper stage propellants are dispersed into payload fairing and detonate.

(1E3) Vehicle clears tower and deviates from flight path. Flight Termination System is activated. Payload propellants are dispersed into the payload fairing and detonate.

Possible Causes

(TBD)

Vehicle Event

(1F) Premature/inadvertent Stage 1 liquid rocket engine firing. (Assume thrust vector control maintained)

Maximum Possible Accident

(1F1) Increased vehicle thrust causes structural overload and core vehicle and/or payload propellant tanks rupture. Propellants mix confined by missile and payload fairing and detonate.

Other Possible Accidents

(1F2) Increased vehicle thrust causes structural damage and initiates ISDS. Core vehicle propellants are dispersed into atmosphere. Upper stage propellants are dispersed into payload fairing and detonate.

(1F3) Flight termination system is actuated. Payload propellants are dispersed into the payload fairing and detonate.

Possible Causes

(TBD)

Vehicle Event

(1G) Premature/inadvertent Stage 1 liquid rocket engine firing. (Assume loss of vehicle flight control)

Maximum Possible Accident

(1G1) Vehicle vectors hard over and impacts ground surface payload first under propulsion. Time available to disperse liquid propellants with range safety action is inadequate.

Other Possible Accidents

(1G2) Vehicle pitches/yaw/rolls and strikes tower. Tower collision damages structure or SRM attachments initiating an ISDS events. Core vehicle propellants are dispersed into the atmosphere. Upper stage propellants are dispersed into the payload fairing and detonate.

(1G3) Flight termination system is activated. Payload propellants are dispersed into the payload fairing and detonate.

Possible Causes

(TBD)

Vehicle Event

(1H) Premature/inadvertent Stage 2 liquid rocket engine firing.

Maximum Possible Accident

(1H1) Heat and vibration from stage 2 exhaust rupture Stage 1 propellant tanks and detonate confined propellants. Explosion propagates to Stage 2 and upper stage, mixing and detonating confined propellants.

Other Possible Accidents

(1H2) Stage 2 engine firing damage structure and initiates ISDS. Core vehicle propellants are dispersed into the atmosphere. Upper stage propellants are dispersed into the payload fairing with confined mixing and detonation.

Possible Causes

(TBD)

Vehicle Event

(1I) Premature/inadvertent attitude control system firing.

Maximum Possible Accident

(1I1) Vehicle strikes tower. Tower collision damages structure or SRM attachment initiating an ISDS event. Core vehicle propellants are dispersed into the atmosphere. Upper stage propellants are dispersed into the payload fairing and detonate.

(TBD)

Other Possible Accidents

(TBD)

Possible Causes

(TBD)

Vehicle Event

(1J) Inadvertent activation of ISDS.

Maximum Possible Accident

(1J1) ISDS Event disperses core vehicle propellants into atmosphere. Upper stage propellants are dispersed into payload fairing and detonate.

Other Possible Accidents

(TBD)

Possible Causes

(TBD)

Vehicle Event

(1K) Premature separation of one SRM.

Maximum Possible Accident

(1K1) Separation of SRM initiates ISDS. Core vehicle propellants are dispersed into the atmosphere. Upper stage propellants are dispersed into the payload fairing and detonate.

Other Possible Accidents

(TBD)

Possible Causes

(1Ka) Structural failure of SRM attachment.

(1Kb) Inadvertent activation of SRM separation.

Vehicle Triggering Event

(1L) Umbilical connector does not release at lift-off.

Maximum Possible Accident

(1L1) Umbilical connector pulls out airborne cabling and connections necessary for inflight functioning of guidance and ordnance activation for flight termination. Vehicle veers off course and impacts ground payload first. Produces detonation of liquid and solid propellants.

Other Possible Accidents

(TBD)

Possible Causes

(TBD)

Triggering Event

(1M) ACS or stage propellant leakage into avionics compartment producing localized fire or minor explosion.

Maximum Possible Accident

(1M1) Guidance components and FTS receivers are damaged. ISDS is not activated. Vehicle veers off-course and impacts ground payload first. Produces detonation of liquid and solid propellants.

Other Possible Accidents

(TBD)

Possible Causes

(TBD)

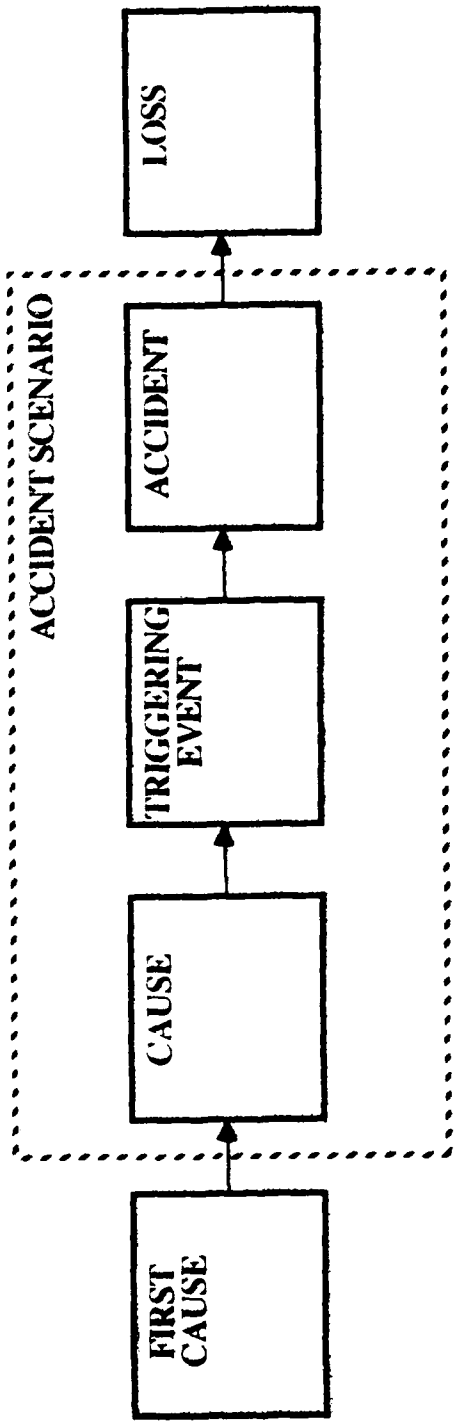


Figure 3-1 Cause and Effect Relationships In Accident Phenomenon

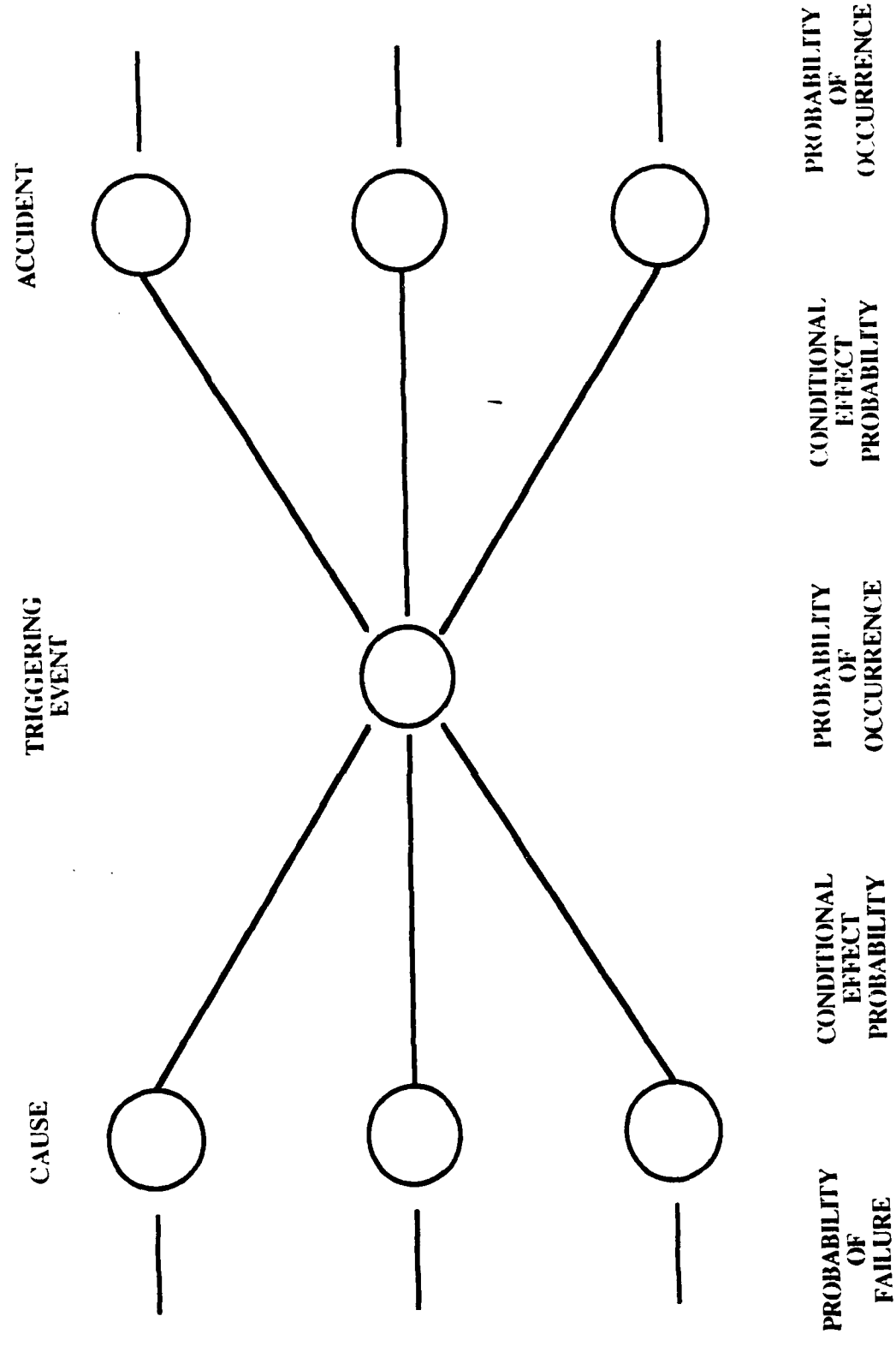


Figure 3-2 Accident Scenario Relationships

Chapter 4
System Failure Probabilities

CHAPTER 4
SYSTEM FAILURE PROBABILITIES

TABLE OF CONTENTS

Section	Title	Page
4.0	Introduction	4-1
4.1	Event Probabilities in Risk Assessment	4-1
4.2	System Failure Probability Methods	4-2
4.2.1	Scenario Event Probability Models	4-3
4.2.1.1	Scenario Event Probability Modeling Process	4-4
4.2.1.2	Solid Rocket Motors - A Case Study	4-6
4.2.1.3	Data Analysis	4-9
4.2.2	Scenario Probability Modeling	4-13
4.2.2.1	Fault-Tree Scenarios	4-14
4.3	Data	4-15
4.3.1	VRM Probability Results	4-15
4.3.1.1	Program 624A	4-15
4.3.1.2	STS Filure Probabilites	4-19
4.3.2	Component Reliability Data	4-24
4.3.3	Notes on Tables 4-10 and 4-11	4-32
4.3.3.1	Notes on Pumps	4-32
4.3.3.2	Notes on Valves	4-33
4.3.3.3	Notes on Pipe Testing	4-34
4.3.3.4	Notes on Motors	4-34
4.3.3.5	Notes on Relays	4-34
4.3.3.6	Notes on Switches	4-35
4.3.3.7	Notes on Batteries	4-35
4.3.3.8	Notes on Solid State Devices	4-35
4.3.3.9	Notes on Instrumentation	4-35
4.3.3.10	Notes on Wires and Terminal Boards	4-36
4.3.4	Human Reliability Data	4-36
4.3.4.1	Level of Presumed Psychological Stress	4-40
4.3.4.2	Quality of Human Engineering of Controls and Displays	4-40
4.3.4.3	Quality of Training and Practice	4-41
4.3.4.4	Presence and Quality of Written Instructions	4-41
4.3.4.5	Coupling of Human Actions	4-42
4.3.4.6	Type of Display Feedback	4-44
4.3.4.7	Personnel Redundancy	4-44
4.3.5	Common Events - Human Death Rates	4-45
4.4	References	4-47

LIST OF FIGURES

Figure No.	Title	Page
4-1	Weibull Plot for Augmentation Pump Bearing	4-48
4-2	Augmentor Pump 650 and Up	4-49
4-3	Risk Analysis	4-50
4-4	Projected Pump Failures	4-50
4-5	Weibull Plot for Augmentor Pump	4-51

LIST OF TABLES

Table No.	Title	Page
4-1	SRM Historical Data	4-7
4-2	(SRM) Failure Mode Distribution	4-8
4-3	SRM Comparisons	4-8
4-4	(624A) Failure Categories	4-17
4-5	Failure Category Summary for Liquid Propellant	4-18
4-6	Failure Category Summary for Solid Propellant	4-18
4-7	Failure Category Summary for All Propellant	4-18
4-8	Catastrophic Failure Probabilities - MECO through Payload Separation	4-21
4-9	Catastrophic Failure Probabilities - Liftoff through MECO	4-22
4-9A	Estimated "Loss of Control and Tumble" Failure Rates	4-23
4-10	Summary of Assessments for Mechanical Hardware	4-25
4-11	Summary of Assessments for Electrical Hardware	4-28
4-12	General Error Rate Estimates	4-38
4-13	Overall U.S. Death Rates (1980)	4-46
4-14	U.S. Accidental Death Rates (1980)	4-46

CHAPTER 4
SYSTEM FAILURE PROBABILITIES

4.0 INTRODUCTION

This chapter presents data and methodology extracted from available references that is useful for developing quantitative estimates of system failure probability. The term "system failure probability" in this chapter means the probability of a system event of interest, or the end event, in the scenario of events which leads to that system event. In this chapter, and in analysis using the methods and data from this chapter, system failure probability could variously represent, for example, the probability of:

(1) An accident, such as collision between a reusable orbiter and a deployed payload, or the high velocity impact of an inflight expendable launch vehicle.

(2) A defined top-level system response to the propogated effect of a lower level failure, or Vehicle Response Mode (VRM). The VRM need not be the actual event in the scenario which yielded or resulted in loss of control of a hazard. An accident event may also follow the VRM. A VRM example would be loss of flight control of a vehicle.

(3) An end event wherein control of a hazard in the system is no longer ensured. Release of the hazard may be uncertain after the occurrence of the event.

In the discussion of this chapter, the VRM is most often used as the scenario end event. The VRM is the most commonly defined scenario end event in the literature.

A scenario is a unique combination or sequence of states, conditions and events which lead to the end event in the scenario. It should be remembered that there may be (and often are) more than one scenario which can lead to a defined end event of interest. The probability statement must distinguish. For example, Accident Scenario Probability denotes the probability of an accident that results from a specific scenario. Accident probability denotes the combined probability of the accident from any one scenario.

The purpose of this chapter is to present data and methods for the development of probability models of scenarios for which risk assessments are required. In principle, this chapter aids in developing probability models for scenarios which may be developed using the methods of Chapter 3 (Failure Scenarios); these probability models in turn being used for the risk assessment of Chapter 7 (Risk Assessment).

4.1 EVENT PROBABILITIES IN RISK ASSESSMENT

Event probabilities that result from a scenario model and the probability models of the events in the scenario are required to quantitatively evaluate the risk of maintaining a hazard and its existing controls in a system design or operational concept. They will be used:

(1) in comparison with quantitative risk acceptability criteria to aid decisions to accept or reject a hazard in a system or its level of control,

(2) in aggregate with other event probabilities in a mission, or a number of missions to assess program vulnerability,

(3) in combination with estimates of accident consequence to measure the expected loss from an accident, or

(4) to focus risk mitigation efforts onto risk-sensitive factors or events in the scenario.

There is sometimes reluctance to quantify probabilities of catastrophic events because credible results can be difficult to achieve. Quantitative estimate that are not realistic and are misleading can hinder the risk assessment decisions. However, these decisions are necessary decisions, and will be made in the absence of quantitative estimates or perhaps by arbitrary assignment of probabilities to these events (Ref. Chapter 7).

Some limitations normally associated with event probability methods or the analyses which result are in fact not limitations on the probabilities, they are deficiencies in scenario modeling. An example is the frequent exclusion of human error, often regarded as a limitation of quantitative methods. If in fact a human function improperly performed, or lost, can result in loss of control of an energy or toxic source and lead to an accident, its exclusion as an event is a deficiency of the event model, or scenario, of the accident. Its exclusion is not a deficiency of the probability model for the scenario or for the events in the scenario. Its exclusion from the scenario also implies incomplete identification and assessment of hazard control function which is basic to hazards analysis.

In this chapter on System Failure, or Event, probabilities the definition or modeling of the scenario of events which can lead to an accident is considered a part of the hazards analysis process, i.e., the process which yields and fully describes those hazards/controls/events which are of concern in the system design or operational concept.

4.2 SYSTEM FAILURE PROBABILITY METHODS

The process of developing system failure (scenario) probability models and estimates has two major elements:

(1) Scenario event probability modeling - for each event in a scenario, it will be necessary to model or estimate its probability of occurrence. A scenario event may include:

(a) loss of a hardware, software, or human function,
(b) a hardware, software, or human malfunction; i.e, function outside of specification,
(c) an inadvertent human function or response,
(d) an unplanned environmental event or environment outside of limits.

A scenario event probability model can be a constant in the scenario, i.e., a fixed probability independent of mission variables. The Solid Rocket Motors (SRM) estimates of Section 4.2.1.1 are examples. They can also be continuous or discontinuous functions of mission random variables. Failure probability as a function of the number of re-use cycles on non-expendable hardware is an example. Scenario event probability modeling is discussed in section 4.2.1

(2) Scenario Probability Modeling - scenario probability modeling is the process of developing or modeling the probability of the event of interest or top event in the scenario. It is the combinatorial "and"/"or" process of modeling the probability of the top event from the probability models of the events in the scenario. In its analytically straight-forward form it is a fault-free model. Where the event probability models are functions of mission random variables, the model can become analytically complex and techniques such as monte-carlo modeling may be necessary. Scenario probability modeling is discussed in section 4.2.2.

4.2.1 Scenario Event Probability Models

It is necessary to develop or model the probability of occurrence for each event in the scenario. Common types of models of independent scenario event probability include:

(1) The constant - This model is commonly thought of as the failure rate. For a given scenario, it yields a fixed, constant probability of occurrence for the scenario event. It is independent of any mission variable.

(2) The Distributed Constant - This model reflects uncertainty in the failure rate. It may be represented by failure rate associated with frequency, e.g., at the .05 and .95 percentiles. A failure rate of .001 at the 5 percentile level can be interpreted as having a 5% chance of the true failure rate being less than .001. Similarly, a failure rate of .01 at the 95 percentile level can be interpreted as having a 95% chance that the true failure rate is less than .01. Together, the failure rate may be interpreted as having a 90% chance that the true failure rate lies between .01 and .001. This assumes, of course, that all assumptions and judgments made in developing the estimate are valid. The distributed constant may also be modeled continuously using, for example, the Normal, Log-Normal or Weibull distribution properties. These are established statistical models and are not discussed here. Modeling the scenario event probability using the distributed constant or failure rate will always be an improvement over the fixed failure rate wherever serious uncertainty exists. This is because uncertainty in a single or multiple events of a scenario defines the uncertainty in the subsequent scenario probability and risk assessment.

(3) The Continuous/Discontinuous Function - The probability of occurrence of a scenario event may be modeled as a function of a mission random variable which in some way relates to the instantaneous and accumulated stress of the hardware or human element.

Examples are:

(a) Ambient temperature
(b) Flight Trajectory
(c) Payload weight
(d) Operating time (including test)
(e) Operating cycles (including test)

A continuous function model ofthe probability of a hardware failure scenario event using operating cycles as a random variable may be represented by the familiar Weibull expression (for example)

$$P = (1-e)^{((C/Cr)^{BETA})}$$

where P = Probability of occurrence of scenario event
C = Number of cycles to be accumulated at the end of the mission
Cr = The number of cycles by which 63.2% of the events would have occurred
Beta = The severity of wearout with the accumulation of cycles

There are some important considerations involved with the development and application of scenario event probability models which are functions of mission random variables.

(1) Where non-Poisson processes (increasing or decreasing probability in equal units of exposure such as cycles, i.e., Beta not equal to one) exist or where they are suspected, and where the event probability relationship to the mission variable can be established, they are the most credible models.

(2) Their development requires failure and success event data along with associated mission data.

(3) Their use potentially complexes the modeling of the scenario probability.

4.2.1.1 Scenario Event Probability Modeling Process - The process of developing the scenario event probability model has two major elements. The first, most important, and often the most difficult is the process of collecting and analyzing the experience gained with hardware, software or personnel which is most representative of these variables in the scenario event, i.e., experience analysis. At the extremes, experience data can be viewed as:

(1) highly disassociative - experience data is derived from generic data sources where the operational and environmental of stresses are unknown, the failure and success events are not included or are not traceable, and compilation methods are not identified, and failure modes are not included.

(2) highly associative - experience data is for the specific hardware under analysis, all failure and success events are known and traceable to mission data, and the modes and mechanisms of failure are known.

The more associative the experience data is with the events in the scenario model, the stronger and more useful will be the input to risk assessment. This is a corollary to the idea that the greater the use and understanding of experience, the better will be the understanding of risk. The use of disassociative data for developing scenario event probability models should be strongly discouraged where they will be used in hazards analysis risk assessment. Every effort should be made to identify, collect and analyze data which is equivalent to the scenario event.

The second element is the process of projecting or predicting a probability model for the scenario event, based on the results of experience analysis, i.e., Probability Modeling. Major factors in this process include, but are not necessarily limited to:

(1) the assumption of inclusion or exclusion of certain failure modes, (usually dominant failure modes),

(2) the assumption of learning which has the effect of reducing the failure probability of the scenario event. Design and manufacturing learning both apply.

(3) the extrapolation, correction, or adjustment of the model based on variations between the hardware, software, and personnel in the experience base and the scenario event under consideration. These variations result from differences (hardware) in operating stresses, environmental stresses, duty cycle, stress time, manufacturer, manufacturing screening, acceptance test procedures, maintenance practice, and a host of others.

(4) the culling or weighting of the data to favor the experience data which is judged to be most applicable to the scenario event.

The process of developing the scenario event probability model from experience involves considerable judgment. Some guidelines can be applied, however,

(1) exclude failure modes only when it can be shown that the associated functions and hardware/human elements have been omitted by design or operational concept from the scenario event,

(2) learning should be applied by failure mode or mechanism where possible. In general, do not project improvements to the scenario event probability model based on learning for predominant failure modes unless specific action directed at the failure mode can be demonstrated by design or operational procedure.

(3) where learning cannot be shown in the presence of historical data from several generations of design and/or operational concepts, no learning should be applied even where specific action can be demonstrated.

(4) where learning is to be applied to a hardware or human element in a scenario event and not to the failure modes discretely, learning should be based on improvements which are known to produce reductions in failure rate and failure probability. Examples are the incorporation of temperature cycling and random vibration (environmental stress screening) during acceptance testing. Other examples may be the incorporation of a more conservative derating criteria for electronic components or the implementation of a parts rescreening program.

The literature of the annotated bibliography is noticeably lacking in data and methods for uniformly developing scenario event probability models in the fashion described. Much of that which is available is directed at or derived from reliability studies, data, handbooks, and text references.

A very good single reference to these methods is O'Connor's Practical Reliability Engineering.[1] An extremely complimentary source is AFWAL-TR-83-2079[2], "Weibull Analysis Handbook." These two references will provide the user of this manual considerable and in-depth methods for analyzing experience data and developing or projecting probability models for scenario events. To illustrate the process (at least one of its variations) and the critical nature of judgment in the process, a summary of available analysis and data for large solid rocket motors is presented in the form of a case study.

4.2.1.2 Solid Rocket Motors - A Case Study - A series of reliability studies of the NSTS was conducted. The first study[3,4,5] was conducted by the J. H. Wiggins Co. and was sponsored by NASA. It was initially directed toward range safety considerations, but was redirected to develop reliability data to be used for nuclear safety analysis of the Galileo and Ulysses missions. The Wiggins study was then reviewed by Sierra Energy and Risk Assessment[6] (SERA), Inc. SERA was sponsored by Teledyne Energy Systems (TES) under contract to the Air Force Weapons Laboratory (AFWL).

Because of substantial differences in failure rate estimates between the Wiggins and SERA studies, the AFWL contracted a second review by Sandia National Laboratories. The Sandia review[7] found weaknesses in each of the prior studies. Following the Challenger STS-51L loss, TES and SERA reviewed and evaluated the Sandia report, although this review was not directly related to the presidential commission investigation of the Challenger incident. However, a study of solid rocket motor reliability was conducted by the

Eastern Space and Missile Center (ESMC) to provide the STS 51L presidential commission information on the history of large SRM flight failure modes and failure probabilities.(8)

In the Wiggins study, the SRM burn-through/rupture represents the only scenario event in the accident scenario "loss of control and tumble." This scenario is referred to as Vehicle Response Mode (VRM) number 2 in the Wiggins reports and in the presentation of VRM data in section 4.4.1.2. SERA questions the completeness of the scenario; however, as discussed earlier, this is a deficiency of scenario modeling and is not an issue in probability modeling.

The Wiggins data contained 32 confirmed failures and 23 suspected failures in a large-SRM launch data base of 1902 launches. Using confirmed failures only, Wiggins models the historical large SRM average failure probability as 0.0175. However, the Wiggins study recommends using a projected failure probability of 0.001 - 0.0001 for the STS SRM to adjust for expected reliability growth. Wiggins did not establish a basis for the expected growth.

The SERA study concluded a mean failure probability of 0.014 per motor per launch on the basis of (1) a somewhat different statistical approach to the analysis of the data, and (2) most significantly, their conclusion that the STS SRM failure probability will not benefit from learning. SERA concluded that there was no (calendar) time-related correlation of SRM reliability and therefore the assumption of learning was unwarranted.

Sandia concluded that both studies had methodologized weaknesses. Their most significant criticism of the SERA study was that the analysis of the historical data and the projection of STS SRM failure probability did not account for anticipated reliability growth. Sandia, however, did not recommend an appropriate failure probability model for the STS SRM or suggest a basis for growth prediction.

The ESMC briefing to the STS 51-L presidential commission on Solid Rocket Motor Reliability was developed for the commission investigation of the Challenger incident. The historical failure events included in the briefing are shown in Table 4-1 and the distribution of predominant failure modes are shown in Table 4-2.

Table 4-1 SRM Historical Failure Data

Time Period	Motor Population	Failures	Failure Rate	Population Description
1959-1979	1933	33	.0174(1/57)	FBM*, Castor, Titan
1959-1983	2810	121	.0431(1/25)	MM**, FBM, Castor, Titan
1970-1983	713	23	.032(1/31)	First Stage only
1959-1985	(All inclusive)		.020(1/50)	First Stage only

* Fleet Ballistic Missile
** Minute Man

Table 4-2 Failure Mode Distribution

Failure Mode	Proportion (%)
Nozzle Failure	20.4
CASE Burn-thru/rupture	25.6
Forward Closure Failure	16.5
Total	62.5%

The history of SRM failure modes included in the ESMC briefing were:

1. Nozzle Failure
2. Nozzle Burn-thru
3. Aft Closure Rupture
4. Aft Closure Burn-thru
5. Case Burn-thru
6. Case Rupture
7. Forward Closure Rupture
8. Forward closure Burn-thru
9. TT Port Failure
10. Ignitor Boss Leak/Burn-thru
11. No Ignition
12. Ignitor Ejected
13. Range Defect after QC7 Qual - No Flight

Table 4-3 provides comparative data for the STS and other SRMs that was extracted from the ESMC briefing.

Table 4-3 SRM Comparisons

Parameter	STS	Other SRMs
Segmentation	Segmented	Only Titan III segmented
Case Material	Steel	Steel and Glass
Propellant	PBAN composite	Poseidon same Titan, MM similar Polaris A-3, A-2 similar but less energetic
Liners	Liners with stress relief	Liners with varying types of stress relief
L/D	6	2 - 10
Diameter	156"	All less than 120"
Soft Goods ('O' ring)	2/joint	Most single (ignitor BOSS)
Factor of Safety	1.65	1.33 - 2.0

Inspection of the ESMC data indicates that the original Wiggins assessment and the subsequent SERA assessment of historical SRM probability of SRM failure/motor/launch are not conservative. The ESMC data also provide no basis for the assumptions of learning that would benefit the projected STS SRM failure probability.

In Dr. Richard Feyhman's review and critique of NASA's estimates of probability of an STS failure with loss of vehicle and human life, he concludes, for example:

(1) Reasonable estimates of mature solid fuel rocket failure probability using historical flight data do not support the optimistic estimates made for the STS.

(2) Ample evidence arose during STS development and operations to indicate that the probability of an STS in-flight failure was considerably higher than official estimates as a result of known problems or deficiencies.

Dr. Feyhman concludes that estimates of the probability of loss of an STS are more reasonably 1 or 2 out of 100, rather than 1 out of 100,000, a conclusion which could have been reached if the available data from STS flight hardware had been used in failure probability estimates.

4.2.1.3 Data Analysis - It is the analysis of experience data which yields the information necessary for scenario and scenario event probability modeling and ultimately risk assessment. Data analysis is a broad topic with a multitude of subtopics, each with a large array of methods, models, techniques, limitations, etc. To complex the issue, each data analysis project will be found to be unique. It will have its own facets, and it will uniquely apply different sets of methods and models. There is no one method, therefore, which can satisfy the data analysis requirements for scenario event probability modeling projects.

The techniques of Weibull analysis will be presented very generally in this section. The discussion and data are derived from the AFWAL-TR-83-2079,[2] "Weibull Analysis Handbook." This reference was produced by Pratt & Whitney Aircraft and sponsored by the Air Force Wright Aeronautical Laboratories. It is the best single reference to applied Weibull analysis available. Its most significant limitation for SPHAM is its orientation toward the commercial and military gas turbine. This does not reduce its utility for methods data however.

The Weibull distribution and the techniques of Weibull analysis described in the handbook are perhaps the most useful to data analysis in the Space Propulsion environment.

(1) The Exponential function can be viewed as a special case of the Weibull. The Exponential function and the failure rate models which result have historically provided the basis for much, if not most, of the data analysis for risk assessment for NASA and for the Air Force. The familiar Exponential function

```
F = 1-e**(-Lamda*-t)

  = 1-e**(-t/MTBF)
```

can be seen immediately as a special case of the two parameter Weibull, i.e.,

```
F = 1-e**(-(t/c1)**BETA)
```

where

Lamda = Failure Rate (failures/unit time)
MTBF = mean time between failure
BETA = Shape severity parameter = 1.0
F = Probability of failure
C1 = Characteristic life parameter
t = random stress time variable

(2) Use of the Exponential function for data analysis and modeling implies the assumption of a Poisson process wherein the probability of failure is equal in equal intervals of time. This disallows degradation or wearout. The Weibull distribution does not suffer from this limitation.

(3) The Weibull distribution appears to handle a wide range of problems. It often approximates well the properties of many other statistical distributions including the Exponential, the Raleigh, the Normal and the log-Normal.

(4) Practitioners experienced with Weibull analysis view the shape, or severity, parameter, BETA as representative of the physics of failure and conclude that hardware with familiar and predominant modes of failure possess a BETA characteristic which is relatively stable. This is an extremely useful property in the analysis of small data sets or data sets with extremely small numbers of failures. (A normal situation for data in the space environment.)

(5) The Weibull distribution is mathematically simple. Because it is simple, it lends itself to straight-forward analytical solutions to highly-censored data sets (small number of failures, large number of success) to complement graphical solutions. Together, the two approaches provide valuable information, including population homogenuity.

The following example of Weibull analysis was extracted from Chapter 6, "Case Histories With Weibull Applications," of the referenced handbook. It is included intact, with minor editing to accomplish its incorporation (e.g., figure numbers, formula symbols).

EXAMPLE 1 - TURBOPUMP BEARING FAILURES

When this study began, three failures of the augmentor turbopump of an aircraft fighter engine had occurred in the field. This was an urgent problem because the failure enabled fuel to escape and ignite. Because of this hazard, top priority was assigned to the analysis of data that might help resolve this problem.

INITIAL ANALYSIS - SMALL SAMPLE

The first analysis was the evaluation of the three failures through Weibull analysis. Note that this was an extremely small sample from the 978 turbopumps that were operating in the fleet. The data were ranked by turbopump operating time, treating the successful pumps as censored units. The resulting Weibull plot is shown in Figure 4-1 at the end of this chapter.

Even with this small sample some valuable observations could be made. First, the very steep slope. BETA = 10, indicates that the failure mode is one of rapid wearout preceded by a relatively safe period. Inspection of Figure 4-1 shows that the probability of a turbopump failure prior to 200 hours is negligible, but after 250 hours the probability increases rapidly.

A second inference can be made from the initial Weibull analysis. The very steep slope (BETA = 10) along with the existence of many unfailed pumps with run times greater than the failed pumps suggests that the failed pumps are part of a unique batch. The method used to determine whether or not a given failure mode is a batch problem is to evaluate the Weibull equation with the parameters calculated (Figure 4-1) for each successful and failed turbopump. For each pump, the probability of failure is determined from the Weibull equation and these probabilities are then summed. If the failure mode applies to the entire fleet, the sum of the cumulative probabilities should approximate the number of failures observed, in this case 3. For example:

$$SUM(F) = SUM(1-e^{**}(-(ti/C1)^{**}BETA)))$$

where:

- SUM(F) = sum of probabilities of each unit
- t_i = time on each unit (both failed and unfailed)
- c1 = 520.963 = characteristic life (hours)
- BETA = 10.094 = slope of Weibull
- e = exponential (base of natural logarithms).

However, with these data the answer was 117 failures, indicating that the failure mode applied to less than the entire fleet of turbopumps. Recommendations were made to Project Engineering that the turbopump vendor and the bearing vendor should review their processes to determine if anything had changed, either in the process, the material, or the assembly. Initially, no change was found that supported the batch hypothesis.

TWO MONTHS LATER - BATCH IDENTIFIED

At this point in the analysis there were seven confirmed and two unconfirmed failures. It was observed that the serial numbers of the failed pumps were all quite high, ranging from No. 671 to No. 872 in the sample of approximately 1000 pumps. The closeness of serial numbers supported the hypothesis that this was a batch problem. If it is assumed that the batch started at the first failed part, Serial No. 671, and extended to the latest pumps produced, the Weibull equation generated fewer than nine failures. By iterating, it was found that by starting at Serial No. 650 nine failures were generated, corresponding to the seven observed and two unconfirmed failures. (See Figure 4-2) This indicated there were about 353 pumps in the batch.

RISK PREDICTION

With a serious problem involving approximately 350 pumps, the next step was to forecast the number of failures which could be expected in the near future. The risk analysis was performed using the methods described in Chapter 3 (of the reference handbook), and was limited to 353 suspect pumps.

The total operating time on engines is kept in a data system that is updated monthly. It is also known that each pump accumulates an average of 25 hours operating time per month. The risk analysis is illustrated in Figure 4-3. With the 353 pump times for the Weibull curve in Figure 4-2, a cumulative total of 9.17 failures can be calculated for the "now" time using the method explained in Chapter 3. Increasing each pump's time by 25 hours and again accumulating the probabilities of failure, the value of 12.26 was obtained. The delta between 9.17 and 12.26 indicated that approximately three more failures were expected in the next month. This analysis covered 24 months of operation and the results are presented in Figure 4-4.

As the forecast indicates, almost all of the suspect lot was expected to fail within a little more than two years. This was obviously a serious problem if the analysis was correct.

Based on this analysis, it was recommended to Project Engineering that turbopumps No. 650 and up with more than 175 hours of time be replaced in the fleet. Fortunately, there were sufficient spare turbopumps to allow this to be accomplished without grounding aircraft. In addition, this would not have been possible without the knowledge of the relatively low risk between 0 time and 200 hours. This action was effective as there were no more field failures.

Laboratory analysis of the failed pumps indicated that the failure mode was caused by swelling of the plastic ball bearing cage to the extent that the balls would skid, causing the bearing to fail. Coordinating with the turbopump manufacturer, the bearing manufacturer, and the plastic manufacturer, a statistical factorial experiment was designed to determine the cause of the swelling of the plastic cages for corrective action.

FOUR MONTHS LATER - FINAL WEIBULL PLOT

Inspection of the turbopumps replaced in service (Number 650 and up with 175 hours or more) revealed 15 more bearings considered to be imminent failures. The addition of these failures to those originally seen in the field produced the final Weibull plot with 24 failures in a sample of 387 turbopumps (Figure 4-5). Note that the original three-failure curve is a good approximation of the final plot, the only difference being that the earlier curve had a steeper slope (10 rather than 4.6) as indicated on Figure 6.1. Although this slope difference sounds large, in fact, the inference from either curve would be substantially the same, that is, a rapid wearout problem. The second Weibull based on seven failures was also a good approximation of the final Weibull (Figure 4-5).

By this time the results of the statistically designed factorial experiment were available. It was found that a process change had been made in the manufacture of the plastic cage to reduce costs. The change resulted in cages of lower density. When these lower density cages were subjected to the combination of heat, fuel and alcohol , the alcohol diffused through the plastic causing it to swell and crack. All such cages were removed from service. (Alcohol is a de-icing agent added to jet fuel.)

The above example illustrates more of the result and impact of Weibull analysis than it does the technique. The reference handbook provides detail sufficient to enable an inexperienced analyst to perform data analysis using Weibull, including:

(1) Algorithms for constructing probability plotting paper and plots

(2) A BASIC computer program for calculating plotting ranks

(3) Tables of median ranks for plotting

(4) Forecasting using simulation

(5) Development of confidence bounds

(6) Analytical methods

(7) Illustrative case histories.

4.2.2 Scenario Probability Modeling

In the literature of the annotated bibliography, the processes of scenario development and scenario probability modeling were inextricably tied via techniques such as fault-tree analysis. The generalized discussion of scenario probability modeling which follows in Section 4.2.2.1 therefore retains that character. The user of this manual should be aware that the two processes are separate. The most illustrative example in the literature was the WASH 1400 Reactor Safety Study[9]. The WASH 1400 models and results are not included here since they are not directly applicable to space propulsion hazards analysis. The discussion of 4.2.2.1 is generalized from the vehicle data which were available and uses terminology consistent with that data.

4.2.2.1 Fault-Tree Scenarios - Scenario probability models are often developed using Fault-Tree Analysis. The steps below outline the approach:

(1) Define the mission, mission segments and the Post-Accident environments of interest. A specific post-accident environment of interest may be launch vehicle propellant explosion at or near the launch pad.

(2) Identify the Vehicle states or modes which can lead directly to the hazard of interest. These states or modes should be considered to be the system effect or response to lower level failures or errors. A specific VRM may be tip-over at the launch pad. The identification of specific VRMs should be done by deduction. For systems which are complex, the initial identification should be supplemented and substantiated by an informal analysis of the system effect of non-passive safety-critical system or subsystem failure modes. The VRM should be viewed as the propogated effect of credible lower level failures or errors. It is the top level event in a tree of cause and effect, i.e., a fault tree.

(3) Identify the hardware, software, human, and environmental causes of the VRMs. This should be done by development of a fault-tree for each VRM. All potential causes of each event in the fault-tree must be identified. These include:

(a) Functional hardware failure modes
(b) Out-of-Tolerence hardware failure modes (e.g., performance, timing)
(c) Operational errors
(d) Maintenance errors
(e) Natural hazards
(f) Out-of-Limit environments

This is the critical step in developing system failure probability estimates, since it yields the basic event data to which probabilities are assigned and it yields the engineering data that defines the necessary and sufficient sequence of events that can cause an accident and result in a loss.

An excellent reference for the development of fault-trees is the "Fault Tree Handbook", NUREG 0492, November 1978.[10]

Failure Modes and Effects Analysis (FMEA) data is sometimes used to identify failure modes which can cause VRMs of interest in lieu of performing fault tree analyses. This will generally not yield satisfactory results, since:

(a) FMEAs are typically developed for reliability purposes and often consider only effects of single-point failures leading to mission failure.

(b) FMEAs typically deal only with the single-event functional failure of hardware. Those modes not considered include human error, common cause failures, etc. This is the most serious deficiency.

(4) Develop probability models and calculate probabilities for each event in the fault tree. (Reference Section 4.2.1.) This requires:

(a) A definition of the use or duty profile for each hardware element of the fault tree (e.g., hours and/or demand cycles accumulated for the mission segment of interest).

(b) Estimates of the failure rates for each hardware element of the fault tree for each unit of stress time and estimates of error rate for each human error event in the fault tree.

An initial failure and error rate data base has been provided in Tables 4-10, 4-11, and 4-12 of this section.

(5) Calculate the VRM probability or the system failure probability. This is done by combining the event probabilities of (4) where the joint probabilities of "or" events are additive and these of "and" events are multiplicative. The mathematics of the fault tree are covered in detail in many excellent references including the "Fault-Tree Handbook", referenced above.

4.3 DATA

This section provides data which was available within the references reviewed. Section 4.3.1 provides selected VRM probability results from risk assessment studies which may be useful as reference data. Section 4.3.2 provides component reliability data and Section 4.3.3 provides clarifying notes. Section 4.3.4 provides data on human error rates, and Section 4.3.5 provides data on common events to serve for comparison.

4.3.1 VRM Probability Results

4.3.1.1 Program 624A - Annotated Bibliography reference 340[11] utilized historical VRM data to estimate VRM probabilities. The objective of the analysis was to quantify the risk of damage to a missile sited on a pad adjacent to the launch site of a malfunctioning 624A missile. In this study 511 AMR (Atlantic Missile Range) launchings of large solid and liquid propellant missiles were used as the study data base. Five VRMs were postulated:

(1) Pad explosions with or without liftoff
(2) Explosions near pad
(3) Ascent failure prior to programming
(4) Post Programming failures - no flight line deviations
(5) Post Programming failure - large flight line deviations.

Ninety-two first stage failures in the data base were examined and allocated to the 5 categories and the VRM probability was calculated as a simple proportion of 511 events. Table 4-4 describes the 5 VRMs and presents the results of the VRM calculations in the study. Tables 4-5, 4-6 and 4-7 show the results broken down by propellant type and the totals.

Table 4-4 Failure Categories

Category Number	Assigned Probability	Remarks
1	.027	Pad explosions. Liftoff may or may not occur. Hazards due solely to flying debris from explosion. Pieces have a circular, normal impact distribution with standard deviation of 2250 ft. Hazard from overpressure negligible since pads will be sited at the .4 psi level.
2	.016	Explosions near pad. Impacts have circular, normal distribution with a standard deviation of 200 feet. Hazards due to flying debris only. Dispersion of pieces about impact point follows a circular, normal distribution with a standard deviation of 2550 feet. Hazard from overpressure negligible since pads will be sited at the .4 psi level.
3	.018	Missiles in this category fail during the vertical part of flight prior to programming. Circular normal distribution about pad assumed for impacting pieces with a standard deviation of 3000 feet for dense metal pieces, a standard diviation of 4000 feet for propellant chunks, and a standard deviation of 5000 feet for motor case and tank fragments. Liquid fuels dispersed in the air by safety officer unless destruct system fails.
4	.086	Failures occur after programming with resulting impacts along the intended flight line. Lateral density function normally distributed about flight line with different standard deviations determined for dense metal piece, typical propellant chunks, and motor case or tank section fragment. Values of calculated from the combined effects of winds, a hard-over turn, explosion velocities, and normal missile dispersions. Probability of impact in any range interval determined by calculating the probability of failure in the corresponding time interval. Liquid fuels dispersed in the air by safety officer unless destruct system fails.
5	.033	Failures of such a nature to permit large deviations from the intended flight direction. However, the larger the angular deviation from the intended flight direction, the less likely the assumed probability of occurrence. Probability of failure in any range interval, as with category 4, determined by calculating the probability of failure in the corresponding time interval. Liquid fuels dispersed in the air by safety officer unless destruct system fails.
Total	.180	

Table 4-5 Failure Category Summary for Liquid Propellant Vehicles

Missile Program	First Stage Failures	Category Number 1	2	3	4	5
A	22	4	0	3	11	4
B	9	0	2	1	6	0
C	8	1	0	0	4	3
D	0	0	0	0	0	0
E	19	4	0	2	10	3
F	7	1	1	1	4	0
TOTAL	65	10	3	7	35	10
PROBABILITY	.195	.030	.009	.021	.105	.030

TABLE 4-6 Failure Category Summary for Solid Propellant Vehicles

Missile Program	First Stage Failures	Category Number 1	2	3	4	5
G	1	0	0	0	1	0
H	2	0	1	0	1	0
I	3	0	0	0	2	1
J	8	1	0	1	2	4
K	1	1	0	0	0	0
L	8	2	2	0	3	1
M	4	0	2	1	0	1
TOTAL	27	4	5	2	9	7
PROBABILITY	.153	.023	.028	.011	.051	.040

TABLE 4-7 Failure Category Summary For All Vehicles

Missile Program	First Stage Failures	Category Number 1	2	3	4	5
ALL	92	14	8	9	44	17
PROBABILITY	.180	.027	.016	.018	.086	.033

4.3.1.2 STS Failure Probabilities - The purpose of this section is to present the catastrophic failure probabilities for each identified STS vehicle response modes for the following phases of interplanetary missions, such as the Galileo mission.

(1) Liftoff through MECO.

(2) MECO to OMS first burn ignition: This phase has an approximate duration of 120 seconds.

(3) OMS first burn ignition to OMS second burn completion: This phase has an approximate duration of 25 minutes.

(4) OMS second burn completion to Orbiter separation: The duration of this phase is mission-dependent.

Only failures leading to loss of vehicle and, hence, the payload are included.

This section is based largely on the studies performed by the J.H. Wiggins Company,[1,2] and summarized in Reference (12). Since the STS 51-L incident and the investigation which followed, the results of the Wiggins study have become viewed as optimistic. The data of this section is presented to illustrate VRM development and probability modeling. The quantitative results should not be used in analysis.

The results of this section were developed as input to an analysis of the risk associated with carrying a nuclear payload on the STS, and as input to range safety analyses. The data of this section were developed before any actual Shuttle flight data existed, and since numerous Shuttle flights will be required to generate enough data to be statistically significant, the failure probabilities presented herein are based on failure data of components and systems having characteristics as similar to those of the Shuttle as possible.

The approach used to develop the data in this section was:

(1) Assess which failure modes require inclusion in the MECO to payload separation phases of STS flight. List such failure modes with the item or items of Shuttle hardware involved. Only category 1 failure modes (loss of life or vehicle) are included.

(2) Group failure modes according to their effect on the Shuttle vehicle in each of the four phases, from lift-off to payload separation.

(3) Assign failure rates to each hardware component contributing to catastrophic failure in each of the four phases for each vehicle response mode, from MECO to payload separation.

(4) Compute failure probabilities for each vehicle response mode (resulting from a category 1 failure), from lift-off to payload separation.

The failure definition, i.e., that which results in loss of payload, constrained which STS failures were included in the analysis. Since the payload has been deployed successfully, for this study a reentry failure of the STS is of no consequence. Loss of payload is directly relatable to failure of components and/or systems of the STS. Failure of certain critical components and systems could lead directly to catastrophic failure of the vehicle. Therefore, component failures are grouped according to expected vehicle response modes. These catastrophic vehicle response modes are listed in Tables 4-8 and 4-9.

The Reactor Safety Study, WASH-1400 (Ref. 9), database was used as a starting point for the development of failure rates. The WASH-1400 study collected data from numerous sources, including NASA data. Many of the components used on the STS are pumps, pipes, valves, pressure vessels, etc., whose failure rates are expected to fall within the ranges of similar components presented in the WASH-1400 document. Tables 4-8 and 4-9 presents the results of this analysis giving STS failure response probabilities from lift-off to MECO.

Tables 4-8 and 4-9 contain the conditional failure probabilities per second from MECO to payload separation; i.e., the failure probabilities in the time period (t) to (t+1) seconds given that a failure has not occurred prior to (t). The probability values are presented as a mean upper and lower bounds, consistent with the use of the log-normal distribution, to describe the uncertainty in component failure rates.

There is one significant difference between Tables 4-8 and 4-9. The former includes weighting factors intended to reflect the conditional probability that, given failure of an item of hardware, a criticality 1 condition will occur. These conditional probabilities, established by NASA for more realistic overall results, are specified in the tables of reference 2 using the mnemonics defined as follows:

(1) ACT: Actual loss. The probability of a criticality 1 condition is 100%,

(2) PROB: Probable loss. The probability of a criticallity 1 condition is between 5 and 100%, except for SRB components where a value between 10 and 100% was used.

(3) POSS: Possible loss. The probability of a criticallity 1 condition is between 0 and 5%, except for SRB components where a value between 0 and 10% was used.

(4) NONE: The probability of a criticallity 1 condition is essentially 0.

The appropriate conditional probability was used as a multiplier on each hardware failure rate to obtain the "critical" failure rate actually used to generate the results given in Table 4-9. More specifically, the median value of the conditional probability is used (e.g., for 10 to 100%, a 55% value is used). Conditional probabilities are not included in Table 4-8 due to the fact that, when the table was generated, the appropriate conditional probabilities had not been defined yet.

Table 4-8 Catastrophic Failure Probabilities - Meco Through Payload Separation

Vehicle Failure Mode	No. Components Failure Modes	No. of Components	Failure Rates* 90% Confidence Bound		
			Mean	Lower	Upper
1.External Tank Punctured					
o MECO to Start RCS Separation Burn	50	255	1.8E-7	7.6E-8	4.2E-7
o During RCS Separation Burn	73	461	1.3E-6	5.5E-7	2.1E-6
2.Loss of Maneuverability & Orbiter Tumbles to Earth					
o MECO to Start RCS Separation Burn	15	93	6.0E-8	1.6E-8	1.1E-7
o During RCS Separation Burn**	4	11	-	-	-
o End RCS Separation Burn to OMS-1 Complete	46	360	2.2E-7	9.0E-8	4.6E-7
3.Loss of Maneuverability On Orbit (Orbital Decay)					
o OMS-1 Complete to Payload Separation	46	360	2.2E-7	9.0E-8	4.6E-7
4.Fire & Explosion of Main Engine Compartment					
o End RCS Separation Burn to Orbit Insertion (OMS-1 Complete)	23	185	1.1E-7	4.4E-8	3.0E-7

*Probability of failure per second
**Values are insignificant

Table 4-9 Catastrophic Failure Probabilities - Liftoff Through Meco

Vehicle Failure Mode	No. Components Failure Modes	No. of Components	Failure Rates* 90% Confidence Bound Mean	Lower	Upper
1.Tipover on pad	7	14	3.3E-5	1.6E-5	6.0E-5
2.Loss of control and tumble	See Table 4-9A				
3.Inadvertent separation at an SRB/ET aft attachment					
o Liftoff to 100 seconds	5	34	4.5E-9	3.1E-9	6.5E-9
o 100 seconds to staging	6	36	5.3E-9	3.6E-9	7.4E-9
4.Inadvertent separation at an SRB/ET forward attachment	3	8	1.5E-9	7.2E-10	2.4E-9
5.Corckscrew motion (resulting from an SRB TVC failure	38	442	4.2E-7	2.3E-7	7.4E-7
6.External tank punctured					
o Liftoff to staging	99	538	2.0E-7	8.4E-8	4.6E-7
o Staging to MECO	93	445	1.8E-7	7.5E-8	4.1E-7
7.ET intertank and/or aft LOX tank failure***	15	98	7.7E-8	2.6E-8	1.6E-7
8.SRB recontact at separation	18	168	1.1E-5	7.1E-6	1.7E-5
9.Loss of ME propulsion					
o Liftoff to staging	18	60	6.6E-9	1.2E-9	2.3E-8
o Staging to MECO	23	71	2.4E-8	3.9E-9	1.3E-7

*Probability of failure per second (except for response modes 1 and 8)
**Probability of failure per event
***This mode is much more likely to occur during stage 1 flight, when the loads and heating are high

Table 4-9A Estimated "Loss of Control and Tumble" Failure Rates*

Time Space (sec)	Failure rate (1/sec) Case 1 (Total probability = 2×10^{3})	Case 2 (Total probability = 2×10^{4})
0-10	7.2E-5	7.2E-6
10-70	1.9E-5	1.8E-6
70-125	2.6E-6	2.6E-7

*Due to SRB case/nozzle failure.

4.3.2 Component Reliability Data

Table 4-10 and 4-11 tabulate the component reliability data available in Appendix III, Table III 4-1 and III 4-2, of the Wash 1400 report (Ref. 9). The data presented in these tables represents the final assessed data base utilized in that study. This data base was the only reliability data base available with the literature reviewed. The data of Tables 4-10 and 4-11 is appropriate for SPHAM since it has incorporated data from NASA and it has been used for studies of STS-related failure probabilities. Although elements of these tables may not be appropriate for SPHAM, it is included unedited for completeness. Section 4.3.3 should be referred to before the data is utilized.

The tables contain the assessed ranges for the data, the median value of the range and the error factor. The range represents a 90% probability, or ("confidence level"), associated with the failure rate. The median is a reference value for the range; there is a 50-50 chance that the data value is either higher or lower than the median value. The error factor is the upper limit of the range divided by the median value. Since the median is the geometric midpoint, the error factor is also the median divided by the lower limit. The values given in the tables are rounded to the nearest half exponent value (i.e., 1 or 3 appearing as the significant figure). Units for the data are probability per demand, "d", or per hours, "hr".

Table 4-10 Summary of Assessments For Mechanical Hardware

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Pumps (includes driver):	Failure to start on Demand, Q_d (See Note a)	$3x10^{-4}$ - $3x10^{-3}$/d	$1x10^{-3}$/d	3
	Failure to run, given start (normal environments)	$3x10^{-6}$ - $3x10^{-4}$/hr	$3x10^{-5}$/hr	10
	Failure to run, given start, (extreme, post accident environments inside containment)	$1x10^{-4}$ - $1x10^{-2}$/hr	$1x10^{-3}$/hr	10
	Failure to run, given start, (post accident, after environmental recovery)	$3x10^{-5}$ - $3x10^{-3}$/hr	$3x10^{-4}$/hr	10
Valves Motor Operated:	Failure to operate, Q_d (includes driver) (See Note b)	$3x10^{-4}$ - $3x10^{-3}$/d	$1x10^{-3}$/d	3
	Failure to remain open, Q_d (plug)	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	(See Note c)	$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Rupture,	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10

Table 4-10 (Continued)

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Solenoid Operated:	Failure to operate, Q_d (See Note d)	$3x10^{-4}$ - $3x10^{-3}$/d	$1x10^{-3}$/d	3
	Failure to remain open, Q_d(plug)	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Rupture	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Air-Fluid Operated:	Failure to operate, Q_d (See Note a)	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Failure to remain open, Q_d(plug)	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
		$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Rupture,	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Check Valves:	Failure to open, Q_d	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Internal leak, (severe)	$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Rupture,	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Vacuum Valve:	Failure to operate, Q_d	$1x10^{-5}$ - $1x10^{-4}$/d	$3x10^{-5}$/d	3
Manual Valve:	Failure to remain open, Q_d(plug)	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Rupture	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Relief Valves:	Failure to open, Q_d	$3x10^{-6}$ - $3x10^{-5}$/d	$1x10^{-5}$/d	3
	Premature open	$3x10^{-6}$ - $3x10^{-5}$/hr	$1x10^{-5}$/hr	3

Table 4-10 (Concluded)

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Test Valves, Flow Meters, Orifices:	Failure to remain open, Q_d(plug)	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Rupture	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Pipes Pipe 3" dia per section:	Rupture/Plug	$3x10^{-11}$ - $3x10^{-8}$/hr	$1x10^{-9}$/hr	30
Pipe 3" dia per section	Rupture/Plug,	$3x10^{-12}$ - $3x10^{-9}$/hr	$1x10^{-10}$/hr	30
Clutch, mechanical:	Failure operate, Q_d (See Note d)	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
Scram Rods (Single):	Failure to insert	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3

Notes:

a. Demand probabilities are based on the presence of proper input control signals. For turbine driven pumps the effect of failures of valves, sensors and other auxiliary hardware may result in significantly higher overall failure rates for turbine driven pump systems.

b. Demand probabilities are based on presence of proper input control signals.

c. Plug probabilities are given in demand probability, and per hour rates, since phenomena are generally time dependent, but plugged condition may only be detected upon a demand of the system.

d. Demand probabilities are based on presence of proper input control signals.

Table 4-11 Summary of Assessments for Electrical Equipment

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Clutch, Electrical:	Failure to operate, Q_d (See Note a)	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Premature disengagement	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
Motors, Electric:	Failure to start, Q_d (See Note a)	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
	Failure to run, given start, (normal environment)	$3x10^{-6}$ - $3x10^{-5}$/hr	$1x10^{-5}$/hr	3
	Failure to run, given start, (extreme environment)	$1x10^{-4}$ - $1x10^{-2}$/hr	$1x10^{-3}$/hr	10
Relays:	Failure to energize, Q_d (See Note a)	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
	Failure of NO contacts to close, given energized	$1x10^{-7}$ - $1x10^{-6}$/hr	$3x10^{-7}$/hr	3
	Failure of NC contacts by opening, given not energized	$3x10^{-8}$ - $3x10^{-7}$/hr	$1x10^{-7}$/hr	3
	Short across NO/NC contact	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
	Coil open	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
	Coil Short to power	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10

Table 4-11 (Continued)

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Circuit Breakers:	Failure to transfer, Q_d (See Note a)	$3x10^{-4}$ - $3x10^{-3}$/d	$1x10^{-3}$/d	3
	Premature transfer	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
Switches				
Limit:	Failure to operate, Q_d	$1x10^{-4}$ - $1x10^{-3}$/d	$3x10^{-4}$/d	3
Torque:	Failure to operate, Q_d	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$d/d	3
Pressure:	Failure to operate, Q_d	$3x10^{-5}$ - $3x10^{-4}$/d	$1x10^{-4}$/d	3
Manual:	Failure to transfer, Q_d	$3x10^{-6}$ - $3x10^{-5}$/d	$1x10^{-5}$/d	3
Switch Contacts:	Failure of NO contacts to close given switch operation	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
	Failure of NC by opening, given no switch operation	$3x10^{-9}$ - $3x10^{-7}$/hr	$3x10^{-8}$/hr	10
	Short across NO/NC contact	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Battery Power Systems (wet cell):	Failure to provide proper output	$1x10^{-6}$ - $1x10^{-5}$/hr	$3x10^{-6}$/hr	3

Table 4-11 (Continued)

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Transformers:	Open Circuit primary or secondary	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
	Short primary to secondary	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3
Solid State Devices, Hi power Applications (diodes, transistors, etc.):	Fails to function	$3x10^{-7}$ - $3x10^{-5}$/hr	$3x10^{-6}$/hr	10
	Fails shorted	$1x10^{-7}$ - $3x10^{-5}$/hr	$1x10^{-6}$/hr	10
Solid State Devices, Low Power Application:	Fails to function	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
	Fails shorted	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
Instrumentation-General (Includes transmitter, amplifier and output device);	Failure to operate	$1x10^{-7}$ - $1x10^{-5}$/hr	$1x10^{-6}$/hr	10
	Shift in calibration	$3x10^{-6}$ - $3x10^{-4}$/hr	$3x10^{-5}$/hr	10
Fuses:	Failure to open Q_d	$3x10^{-6}$ - $3x10^{-5}$/d	$1x10^{-5}$/d	3
	Premature open	$3x10^{-7}$ - $3x10^{-6}$/hr	$1x10^{-6}$/hr	3

Table 4-11 (Concluded)

Components	Failure Mode	Failure Rate Assessed Range	Computational Median	Error Factor
Wires (Typical circuits, serveral joints):	Open circuit,	$1x10^{-6}$ - $1x10^{-5}$	$3x10^{-6}$/hr	3
	Short to ground	$3x10^{-8}$ - $3x10^{-6}$/hr	$3x10^{-7}$/hr	10
	Short to power	$1x10^{-9}$ - $1x10^{-7}$/hr	$1x10^{-8}$/hr	10
Terminal Boards:	Open connection	$1x10^{-8}$ - $1x10^{-6}$/hr	$1x10^{-7}$/hr	10
	Short to adjacent circuit	$1x10^{-9}$ - $1x10^{-7}$	$1x10^{-8}$/hr	10

Note:

a. Demand probabilities are based on presence of proper input control signals.

4.3.3 Notes on Tables 4-10, 4-11

A discussion of the data elements within Tables 4-10 and 4-11 were included in the Wash 1400 report, and are included here with only minor editing. These "notes" contain amplifying information on use of the data in the tables. These notes should be reviewed before the data of Tables 4-10 or 4-11 are utilized.

4.3.3.1 Notes on Pumps

(1) Test and Maintenance - Generally, those test and maintenance situations where an override feature can automatically return the pump (or other devices) to operational status, given demand will have no test and maintenance contribution to unavailability. Distributions on test and maintenance act durations are used to account for variations in the times required to complete the act from plant to plant or situation to situation. Testing times include the time required to make the minor repairs incidental to the tests.

Testing the pumps within nuclear power plant safety systems requires isolation of the pump under test in the majority of cases. This results in a contribution to unavailability due to pump downtime. In general, the probabilistic contribution is derived from the test act duration time which ranges (90%) from 15 minutes to 4 hours, under a log-normal distribution. From this range, the mean test duration time (downtime) is thus 1.4 hours (t_D = 1.4 hours for test).

Maintenance on the pumps ranges in duration from 30 minutes to several days. From this range the mean maintenance act duration t_D is 37 hours. Maximum outage during powered operation may be limited to 24 hours on pumps other than those located inside containment. Use of the 24 hour limit as an upper bound gives a mean maintenance act duration, (t_D), of 7 hours. Pumps located inside the containment vessel are permitted by specification to be down singly for a maximum of 72 hours during plant operation. The associated mean duration time for these particular pumps is t_D = 19 hours.

In general, the test period for nuclear power plant safety system pumps is fixed by specification at monthly intervals. The test frequency is therefore approximately constant at 1 act per month. The nominal test contribution to unavailability, Q_T, is the ratio of mean test act duration time (t_D), to test interval.

$$Q_T = \frac{t_D}{\text{hrs/month}}$$

Non-routine maintenance ranges from monthly to yearly with a mean pump maintenance interval of 4.5 months/act or a mean frequency of maintenance of 0.22 acts/month. The maintenance contribution to unavailability Q_M is a function of the

maintenance frequency (f), mean maintenance act duration (t_D), and maintenance interval. The equation for Q_M is:

$$Qm = \frac{f _ t_D}{720}$$

when t_D is now the average maintenance downtime. Substituting values into the above equations will give numerical values for Q_M.

(2) Environments - The safety pumps located outside containment are not likely to be subjected to abnormal environmental conditions in the event of the assumed loss of coolant accident with the exception of a temporary change in temperature and radiation level of the pumped fluid. Since these pumps are designed for such conditions, the assessments for outside pumps are based on performance data from similar pumps operating under design conditions.

The pumps located inside containment may be subjected to a much more severe environment during the period from the accident to the time that the safety system can reduce the temperature, pressure, humidity, and radiation levels to near normal. This extreme environmental condition has a chance of subsiding within 24 hours.

The levels of the immediate post-accident environment cannot be determined exactly, but conditions generally representative of the accident were used in a series of pump qualification tests for the inside pumps. Those tests were non-exhaustive. The results of those tests and experience data from pump performance in test reactors operating at extremely high temperatures were considered in making the assessments for pumps inside containment. Recovery to near normal environmental conditions is likely to increase the probability of continued pump operation. Experience and testing have revealed, however, some degradation in lubricants, bearings, and motor insulation after exposure, possibly degrading pump performance given survival for the initial 24-hour period. To account for the potential degradation, a failure probability between normal and abnormal conditions is assigned with sufficient associated uncertainties to account for the possibility of deviations.

4.3.3.2 Notes on Valves

(1) Failure Modes - Failure of a valve to operate includes changing state from closed to open or open to closed. Failure to remain open (plug) refers to reduction of flow to an unusable level due to foreign material or gate failure, etc. Not included in the data is the contribution for an inadvertent or false signal driving valves closed. Instances of valve gates separating from drive stems and lodging in a closed position (while the valve monitors continued to indicate open) have been reported in nuclear operating experience.

(2) Test and Maintenance - Motor operated valve test act duration times range from 15 minutes to 2 hours (90% range) with a mean test time t_D of 0.86 hours (log-normal). No downtime test contribution is obtained if the valve has a test override feature which automatically returns the valve to an operational status given demand. The position monitors used on automatic valves detect the position of valve drive; they do not determine flow or position of valve gate. Hence monitoring does not influence fault duration time for failure to remain open (plug) failure modes.

Valve outages for maintenance range from 30 minutes to several days with a mean maintenance duration t_D of 24 hours. Maintenance acts on certain valves may be limited to 24 hours during powered operations by specification. Under these conditions the mean act duration time t_D is 7 hours. The mean maintenance act frequency f is 0.22 acts per month. Thus,

$$Q_T = \frac{t_D}{720} \quad , \quad Q_m = f\,\frac{t_D}{720}$$

where t_D in the first equation is the test downtime and in the second equation maintenance downtime. Substituting will yield the applicable numerical values for Q_T and Q_M.

(3) Environments - In general, valves within safety systems operate on demand within a few minutes after the accident. Hence degradation due to post-accident environments is deemed not significant within the associated uncertainties.

4.3.3.3 Notes on Pipe - Testing - Certain safety piping is tested monthly during the tests on pumps within the safety system. Certain portions of the piping however are incapable of being periodically tested except during the initial tests prior to final licensing of a nuclear power plant.

Therefore the failure rate assessments were applied to both standby pipes (safety) and active pipes (process) with large uncertainties to account for the possibility of either extreme. The safety assessments are given in units of per section per hour with a section defined as an average length between major discontinuties such as valves, pumps, etc. (approximately 10 to 100 feet). Each section can include several welds, elbows and flanges.

4.3.3.4 Notes on Motors - In many instances, pumps and valves within the safety system are driven by electric motors. Available experience data did not permit separation of motor failure from pump failure. Therefore, separate motor failure rates for pump and valve drive motors should not be included. The assessments above apply to those electric motors that function independently of pumps and valves.

4.3.3.5 Notes on Relays - Failure Modes - The available data did not completely isolate separate causes of failure; hence the table failure modes are not necessarily independent. For example, failure rates for failure to energize includes failure of the normally open contacts to close. Hence relay and contact failure rates in general should not be combined together to determine overall relay failure rates. Individual contributions, however, can

be employed where there are individual, separate effects on the system. Examples are failure of contact of a multiple contact relay, or shorts to power (which could effect power circuit) if these modes have a unique, individual effect on the system.

4.3.3.6 Notes on Switches - Failure Modes - The data did not uniquely separate the causes of failure; hence the above failure modes are not necessarily independent. Failure to operate includes failure of contacts. In general, the contact contribution should not be added to the switch contribution to determine overall switch failure rate. As with relays, when separate, individual effects occur, individual contact contributions can be computed (such as for multiple contact switches).

4.3.3.7 Notes on Batteries - Failure Modes - The emergency dc power system involves 58-60 series connected lead cadmium or lead calcium battery cells to form a 125 volt supply. Two 125 volt systems are series connected to obtain 250 volts. These batteries are constantly charged by chargers and the open circuit output voltage monitored at regular intervals. The significant failure mode in this arrangement involves failure to provide adequate output voltage under emergency load conditions. Failures by shorts to ground or internal shorts within cells are likely to be detected quickly with negligible resulting fault duration time.

4.3.3.8 Notes on Solid State Devices

(1) Environments - High power application is defined as application in circuits involving currents of 1 ampere or above and/or voltages - 28 volts and above.

(2) Failure Modes - The available data do not permit separation of the causes of failure in all cases; hence the above failure modes are not independent. Failure rates for shorts should not be added to rates for failure to function unless special consideration of short failures is necessary due to unique effects on the system.

The relatively large error factors on solid state device assessments reflect the potential variation from application to application. For particular situations, a detailed analysis could yield narrower bounds.

4.3.3.9 Notes on Instrumentation - Failure Modes - The data for shift in calibration incorporate a variation of drift magnitude. These data may be pessimistic if used for instrumentation with wide operational tolerance bands. In these cases individual assessment should be performed.

The relatively large error factors associated with instrumentation assessments reflect the wide variation in configuration from application to application. For any particular instrumentation system, a detailed analysis may be done to obtain narrower bounds.

4.3.3.10 Notes on Wires and Terminal Boards - Failure Modes - The failure rates for wires are based on a typical control circuit wire section with soldered and lug connections to components and terminal boards. The circuit consists of approximately 30 connections with approximately 20 of these connections comprised of lug terminals on terminal boards.

The data did not permit a unique separation of failure modes in all cases; hence the failure modes listed for wires and terminals are not necessarily independent. Probabilities for defective terminations should not in general be added to wire probabilities to obtain overall circuit probabilities. Separate terminal board data are provided for those cases in which unique system effects exist.

4.3.4 Human Reliability Data

Table 4-12 presents general human error rate estimates derived from the Wash 1400 report which incorporates independent judgments of two human-reliability analyses. These judgments were made after reviewing information on nuclear power plant personnel skill levels, previous jobs held by these personnel, operating procedures, and the design of the controls, displays, and other equipment read or manipulated by the operating personnel. The information was obtained in interviews with operating personnel, supervisor, and engineering personnel at nuclear power plants, by observation of control room, test, maintenance, and calibration tasks at several plants, and by a study of written materials and photographs.

As noted in the table, modification of these underlying (basic) probabilities was made as necessary when incorporated into the fault trees. The modifications considered the exact nature of the human engineering, e.g., the close similarity of labeling of different switches, with the attendant higher probability of grasping and manipulating the wrong switch.

In general, human error rates for tasks were estimated to the nearest order of magnitude, with two analysts making independent estimates based on a detailed description of the task requirements (including written instructions and photographs of controls, displays, valves and other items to be read or manipulated by operating personnel). In all cases, the independent estimates agreed to the nearest order of magnitude. The associated assessed error factors (probability ranges) covered the possible variations and uncertainties associated with the final estimates.

Some of the estimates were based directly on data collected on tasks identical or highly similar to nuclear reactor tasks. For example, UKAEA experience is that large manual valves that have no readout of their position except the valve itself are left in the incorrect position after non-routine operations approximately once in 100 times (10^{-2} occurrence). Such information was applied in the Wash 1400 study without modification. (This is the case when no special precautions are taken, such as use of padlocks with administratively controlled keys.)

In other cases an analytical approach was necessary to apply existing data on human error rates. In these cases, a nuclear power plant task was broken down into individual steps involving perceptual, conceptual/emotional, and motor aspects of behavior. In more common terms, this means taking a particular step in a task and considering the following three aspects:

(1) The inputs to the operator, as provided by such things as displays on control panels, labels, configuration of manual valves (including presence or absence of padlocks), written instructions, and other signals.

(2) The thinking and decision making done by the operator is influenced by the interaction of his emotional state (e.g., fear and worry immediately after a large LOCA).

(3) The responses the operator makes by means of switches, large valves, oral orders, writing down information etc.

The above analytical approach was used to break down the tasks into smaller bits of behavior that could more readily be combined with existing data or with the experience of the analysts.

Finally, the estimates of error rates for the individual behavioral units were combined into estimates of error rates for larger units of behavior, corresponding to nuclear power plant tasks or groups of tasks. In this recombination operation, the estimated error rates for smaller behavioral units were at times modified in consideration of their interdependencies to avoid the derivation of unrealistically low estimates of task error rates. In the Wash 1400 study, the task error rate estimates so derived were combined with consensus-estimated error rates to enhance the stability of the estimates.

The estimated task error rates were modified, where appropriate, by the effects of available personnel redundancy, that is, the checking of a man's performance by another man. In some cases, the total estimated failure rate of a task, including recovery from an original error made possible by using personnel redundancy, was equal to or less than 10^{-6}. However, experience with human reliability analysis and the observation of "the impossible" have led most specialists in this field to view with skepticism any task error rate less than 10^{-5} for any but the very simplest human acts. Consequently, in the present analysis, estimates of human error rates smaller than 10^{-5} were not used.

The estimates of task error rates were incorporated in fault trees by the fault tree analysts, and human failure events were treated in the same manner as other failure events.

Several factors were considered in deriving estimated human error rates for nuclear power plants. Following are the more important of these factors, each of which is discussed under the topic headings which follow: (1) Level of presumed psychological stress; (2) Quality of human engineering of controls and displays; (3) Quality of training and practice; (4) Presence and quality of written instructions and method of use; (5) Coupling of human actions; (6) Type of display feedback; and (7) Personnel redundancy.

Table 4-12 General Error Rate Estimates[a,b]

Estimated Rates	Activity
10^{-4}	Selection of a key-operated switch rather than a non-key switch (this value does not include the error of decision where the operator misinterprets situation and believes key switch is correct choice).
10^{-3}	Selection of a switch (or pair of switches) dissimilar in shape or location to the desired switch (or pair of switches), assuming no decision error. For example, operator actuates large handled switch rather than small switch.
3×10^{-3}	General human error of commission, e.g., misreading label and therefore selecting wrong switch.
10^{-2}	General human error of omission where there is no display in the control room of the status of the item omitted, e.g., failure to return manually operated test valve to proper configuration after maintenance.
3×10^{-3}	Error of omission, where the items being omitted are embedded in a procedure rather than at the end as above.
3×10^{-2}	Simple arithmetic errors with self-checking but without repeating the calculation by re-doing it on another piece of paper.
1/x	Given that an operator is reaching for an incorrect switch (or pair of switches), he selects a particular similar appearing switch (or pair of switches), where x = the number of incorrect switches (or pair of switches) adjacent to the desired switch (or pair of switches). The 1/x applies up to 5 or 6 items. After that point the error rate would be lower because the operator would take more time to search. With up to 5 or 6 items he doesn't expect to be wrong and therefore is more likely to do less deliberate searching.
10^{-1}	Given that an operator is reaching for a wrong motor operated valve MOV switch (or pair of switches), he fails to note from the indicator lamps that the MOV(s) is (are) already in the desired state and merely changes the status of the MOV(S) without recognizing he had selected the wrong switch(es).
1.0	Same as above, except that the state(s) of the incorrect switch(es) is (are) not the desired state.
1.0	If an operator fails to operate correctly one of two closely coupled valves or switches in a procedural step, he also fails to correctly operate the other valve.

Table 4-12 General Error Rate Estimates (concluded)

Estimated Rates	Activity
10^{-1}	Monitor or inspector fails to recognize initial error by operator. Note: With continuing feedback of the error on the annunciator panel, this high error rate would not apply.
10^{-1}	Personnel on different work shift fail to check condition of hardware unless required by check list or written directive.
5×10^{-1}	Monitor fails to detect undesired position of valves, etc., during general walk-around inspections, assuming no check list is used.
.2 - .3	General error rate given very high stress levels where dangerous activities are occurring rapidly.
$2^{(n-1)}x$	Given severe time stress, as in trying to compensate for an error made in an emergency situation, the initial error rate, x, for an activity doubles for each attempt, n, after a previous incorrect attempt, until the limiting condition of an error rate of 1.0 is reached or until time runs out. This limiting condition corresponds to an individual's becoming completely disorganized or ineffective.
1.0	Operator fails to act correctly in the first 60 seconds after the onset of an extremely high stress condition, e.g., a large LOCA, (Loss of Cooling Accident).
9×10^{-1}	Operator fails to act correctly after the first 5 minutes after the onset of an extremely high stress condition.
10^{-1}	Operator fails to act correctly after the first 30 minutes in an extreme stress condition.
10^{-2}	Operator fails to act correctly after the first several hours in a high stress condition.
x	After 7 days after a large LOCA, there is a complete recovery to the normal error rate, x, for any task.

(a) Modification of these underlying (basic) probabilities were made on the basis of individual factors pertaining to the tasks evaluated.

(b) Unless otherwise indicated, estimates of error rates assume no undue time pressures or stresses related to accidents.

4.3.4.1 Level of Presumed Psychological Stress - The highest error rates were assigned to the time period immediately after a large LOCA, with recovery to normal levels of human reliability occurring as a function of time. Implicit with this assumption that error rates decrease with time is the underlying assumption that things do get better. That is, the nuclear power plant is brought under control with appropriate automatic and manual responses to the emergency.

Normal error rate values were assigned to routine control room operations and to maintenance and calibration tasks, as it is assumed that the normal stress level has a facilitative effect. In the interviewing and observation of control room operators, maintenance personnel, and calibration technicians, it appeared that the jobs were sufficiently challenging to maintain facilitative levels of motivation. No one seemed bored or "just putting in time". (This is a clinical judgment based on the independent observations of two psychologists trained in clinical evaluations.)

4.3.4.2 Quality of Human Engineering of Controls and Displays - The basic error rates in Table 4-12 were modified by assigned higher rates to situations where the arrangement and labeling of controls to be manipulated were potentially confusing. For example, motor operated valves MOV-1860A and MOV-1860B are to be opened at the RWST low level set point (14.5% full). Immediately adjacent to these switches are MOV-1863A and MOV-1863B. The two sets of switch numbers are similar, and they have similar functional labels:

LO HEAD S.I. PP A SUMP SUCT VV

and

LO HEAD S.I. PP A DISC ISO VV

Furthermore, at the low level set point, both sets of valves would normally be closed and the green indicator lamps above them would be illuminated.

Fairly high rates were assigned to the probability of manipulating the wrong switch in cases where similar appearing controls and displays were close together without separation by functional flow lines on the panels or some other means to show normal process flow, a design characteristic of operating panels on some research reactors. In general, the design of controls and displays and their arrangements on operator panels in the nuclear plants studied deviated from human engineering standards specified for the design of man-machine systems and accepted as standard practice for military systems. Whether such standards were necessary and would result in a net benefit was outside the goal of the Reactor Safety Study.

It was appropriate to assign fairly low error rates to tasks where the quality of human engineering is such that the cues given for task initiation and correct task completion are difficult to ignore. For example, lower error rates were assigned to cases where the task initiation cue is an annunciator alarm than where the cue is merely the deviation of a meter on a panel in the control room. Also, for some large manual valves, the use of a special padlock and chain with administratively controlled keys and associated paper work reduces the probability of forgetting to return to valve to the normal condition after maintenance. In the latter case the primary cause of leaving such a valve in the wrong condition after maintenance would be failure

to use the required procedures. An estimated 10^{-4} error rate per opportunity was assigned to such failure.

In certain cases, a high recovery factor was assigned to the error of manipulating an incorrect MOV or pair of MOVs. An example of a recovery factor is an follows. Assume an operator is supposed to open a pair of MOVs to increase the flow rate as displayed on a meter. The normal procedure would be for the operator to make the switch manipulation and then observe the flow meter for the proper rate of flow. If the proper rate of flow fails to materialize, the operator would have a high probability of realizing something was wrong and would likely take corrective action.

In general, it was found that most errors in maintenance and calibration tasks either had immediate and compelling feedback of their correctness or incorrectness or that subsequent recovery factors made it highly improbable that errors would remain undetected for long.

4.3.4.3 Quality of Training and Practice - On the basis of interview, observation, a visit to a training center, and review of training materials, the level of training of nuclear power plant personnel was judged to be outstanding. For example, interview with control room operators revealed a clear understanding of normal reactor operation. They can readily describe the events occurring in normal on-line operation and have a clear conceptual picture of the processes involved. Therefore, for routine maintenance, calibration, and control room operations, a high degree of trained-in excellence has been assumed with associated high estimates of human reliability.

Although original training includes responses to emergencies, there is no provision for frequent on-site practice in responding to simulated emergencies (such as a large LOCA) at the sites visited. In the absence of appropriate simulation equipment, such on-site practice could be simulated by frequent "talk-through" of responses to emergencies. This type of informal test was made in the course of the Reactor Safety study. It was found that the operators interviewed could explain in general terms what they should do in postulated emergency situations, but they did not always appear to be sure of the locations of switches and readings on displays relevant to manual backup actions required in the event of failure of automatic safeguards systems. This does not imply that, based on such a limited "test" of operator ability in emergencies (i.e., a discussion of a hypothetical situation), operators would not be able to carry out emergency tasks. Nevertheless, the lack of ability to "talk through" appropriate procedures without hesitation or indecision potentially indicates lack of a clear plan of action should such emergency situations occur. Based on the above findings, relatively high error rates were consequently assigned to operator actions required soon after the onset of a major emergency such as a large LOCA.

4.3.4.4 Presence and Quality of Written Instructions - Generally, a lower error rate was assigned to procedures for which written instructions are available. It was necessary to make an estimate of the likelihood that written instructions would be used by the operator, maintenance technician, or calibration technician, rather than trusting his memory of the procedures. For example, in one of the cases analyzed, even with appropriate use of calibration procedures, it was observed that a technician anticipated what

approximate instrument reading should appear for each step in the procedure. He had performed this lengthy calibration procedure so often that he knew what to expect. This knowledge coupled with a very low frequency of finding an out-of-tolerance indication sets up a very strong expectancy that each reading will be in tolerance. Under these circumstances there is some likelihood (estimated as 10^{-2}) that the technician will "see" an out-of-tolerance indication as being in tolerance. (In this particular instance, however, there were so many recovery factors that even with the assumption of a 10^{-2} error rate, the probability of an uncaught and uncorrected calibration error was negligible.)

In estimating error rates, the quality of the written instructions was evaluated. Of concern were such factors as the ease with which an operator could find a written emergency procedure, the extent to which the format would aid the operator, the likely ease of understanding non-routine instructions, and so on. The style of written instructions contributed materially to the estimated error rates. The written instructions do not conform to established principles of good writing; they are more typical of military maintenance procedures of approximately 20 years ago. Other deficiencies which contributed to relatively high error rate estimates were poor printing quality, no distinctive binder or location for emergency procedures, lack of tabs and inappropriate indexing which made it difficult to find specific procedures, and poor format for each procedure.

The observed method of use also contributed to relatively high estimated error rates. Men were observed performing several tasks and then checking them off on the check list. The correct and more reliable procedure would be to perform a listed task, check it off, and then move on to the next item in the check list. Lower error rates were assigned to cases where information from a meter or a dial had to be recorded on the check list rather than merely checking off that an item had been completed. Such a procedure markedly reduces the probability of forgetting to perform a step in the check list.

4.3.4.5 Coupling of Human Actions - Another important factor is related to the type of grouping of switches or manual valves plus the effects of written instructions. This factor is the amount of coupling of human actions, that is, the relative lack of independence of such actions. Four levels of coupling were used in the analysis: no coupling (i.e., complete independence), loose coupling, tight coupling, (complete dependence). The degree of coupling is assigned on an individual failure basis but some general guidelines were used as illustrated below.

An example of no coupling between tasks would be where the probability of error in one task is independent of the probability of error in another task. Tasks which are dissimilar or which are greatly separated in space and time tend to be independent. However, such tasks might be affected by the same conditions (e.g., the stress after a large LOCA) and the estimates of their error rates were influenced by this consideration.

Loose coupling can be illustrated by two test valves in the PWR containment spray injection system located in a building next to the RWST. Both these large manually operated valves are chained and padlocked in the normally closed position. Periodically they must be unlocked and opened for

test purposes. The procedures call for one valve to be opened and that part of the system tested, and then for the valve to be closed, chained, and padlocked before proceeding to open the other valve to test the other part of the system. It was judged there was a small probability that, for convenience, an operator would regard both valves as a unit and not follow the prescribed procedures. That is, he would open both valves prior to any testing and after all testing reclose both valves. Therefore, the probability of forgetting to reclose one valve would not be independent of the probability of forgetting to reclose the other valve. Since most operators would be likely to follow the prescribed procedure, loose coupling best expressed the relationship errors of forgetting for the two valves.

For the valves in question, the important error was forgetting to reclose both valves. the probability of this error was calculated as follows: Generally, loose coupling was taken to be the log-normal median value between the upper and lower bounds. The upper bound on coupling is defined by the assumption of complete coupling between the two acts (i.e. reclosing of the two valves). The lower bound is obtained from the assumption of complete independence between the two acts. Given an estimate of 10^{-2} for the error of forgetting to reclose a single valve, the upper bound becomes 10^{-2} and the lower bound $10^{-2} \times 10^{-2} = 10^{-4}$. The log normal median is the square root of the product of the lower and upper bounds, or,

$$(10^{-2} \times 10^{-4})^{1/2} = (10^{-6})^{1/2} = 1 \times 10^{-3}$$

Thus, the probability of forgetting to reclose each valve is estimated as 10^{-2} and the probability of forgetting to reclose both valves (the only error of importance in the analysis) is estimated as 1×10^{-3}.

Tight coupling can be illustrated by the requirement to calibrate three bistable amplifiers in the reactor protection system (SCRAM). One calibration technician performed the calibration in the instrument room while communicating with an operator in the control room. A 10^{-2} probability was assessed for the error of the technician's miscalibrating the first bistable amplifier, as by using an incorrect set level. The incorrect set level, for example, could be due to a simple misreading error. Given that the calibration technician has miscalibrated the first amplifier, there is a substantial probability of carrying over the incorrect set level to the second bistable amplifier. It was estimated that the conditional probability of miscalibrating the second amplifier, given miscalibration of the first, would be 10^{-1}, or a joint probability of 10^{-3} of miscalibrating both amplifiers. It was estimated that the conditional probability of miscalibrating the third amplifier, given miscalibration of the first and second amplifiers, would be 1.0, or a joint probability of 10^{-3} of miscalibrating all three bistable amplifiers. In other words, a tightly coupled sequence of events was assumed. In this particular operation, there were several recovery factors, so that the final estimated influence of human errors on the reactor protection system was smaller that the above 10^{-3} estimate for the basic act.

An example of complete coupling is found when one basic act results in several failures. For example, one step in the written procedure calls for the operator to open two valves. The two valves are regarded as one unit by the operator. In estimating the probability of his omitting to open these valves, the same estimated error rate was given for one or both valves. That is, it was considered that if he would open one valve, he would open the other. Likewise, if he failed to open one valve, he would fail to open the other. This analysis is an approximation, of course. Absolutely complete coupling can be very unlikely--yet, in this particular example, it was assessed that human behavior would exhibit high dependency, and complete coupling was assumed as a reasonable approximation.

As a contrast to the above discussions, the following example shows how an apparent common mode error due to apparent coupling was estimated to have no resulting net effect on safety system availability. At one site two possible common mode errors for comparator calibration in the reactor containment pressure consequence limiting system were:

(1) using the wrong decade resistance for all channels, and

(2) using the wrong scale on the digital voltmeter for all channels.

Once either error is made, the calibration technician might indeed recalibrate an entire rack. The estimated error rate for either common mode error was 10^{-2}. However, when the technician went to the second rack, he would discover that the comparators in that rack, too, needed a gross recalibration, and he should suspect that something was wrong with the test procedure rather than merely proceed to recalibrate the second rack. The estimated failure rate of the recovery factor for the second rack was 10^{-2}. (This estimate was deliberately made conservative.) Since the technician typically calibrates all four racks in one shift, it can be seen that the overall rate of making one of the above two calibration errors and then failing to catch this error and incorrectly recalibrating all four racks is approximately 10^{-2} (the initial error) x 10^{-2} (second rack) x 10^{-2} (third rack) x 10^{-2} (fourth rack), or much less than 10^{-5}. (Recall that we do not use any estimates smaller than 10^{-5}.)

4.3.4.6 Type of Display Feedback - One of the most important recovery factors to mitigate the effects of an error is the type of display feedback. If an error resulted in an immediate annunciator warning, a relatively low failure rate was assigned to the recovery factors. The total task failure rate would be the product of the initial error rate and the low failure rate of the recovery factor. But if the feedback consisted of a slow rise in pressure, for example, as displayed on a meter on the vertical wall underneath the annunciator panels, a higher failure rate was assigned, in certain instances 0.5.

4.3.4.7 Personnel Redundancy - Another important recovery factor is the use of personnel redundancy (or, as it is sometimes called, human redundancy) which refers to the use of a second person to verify that the performance of a first person was correct. Personnel redundancy can vary from complete redundancy (i.e., complete independence of the initial act and the checking act) to very low degrees of redundancy (i.e., high degrees of dependency

between the initial act and the checking act). Lower recovery factor failure rates are related to higher degrees of personnel redundancy.

Beneficial use of a high degree of personnel redundancy is illustrated by the calibration of the water level sensors and drywell sensors at one site. A two-man team performs the calibration with one man reading and recording the readings on the check list while the other man does the calibration. After the calibration has been completed the two men reverse roles and perform a functional check. With this extensive use of personnel redundancy, an estimate of 10^{-5} was assigned to the joint probability of a miscalibration being made and the functional check failing to catch the miscalibration.

A low degree of personnel redundancy is illustrated by the use of a single person to perform critical actions, followed by an informal type of checking. For example, in the case of one critical manual valve located at the RWST, one man is responsible for reopening this valve after maintenance. Should he forget to open the valve, the RWST would not be available in the event of a large LOCA. At certain times a walk-around inspection is performed, but (as already noted) the estimated error rate for this type of passive monitoring task is high (0.5).

It is sometimes thought that requiring a person to sign a statement that he has accomplished a task will ensure that he really performed the task. For tasks that are frequently performed, the signing of one's name tends to become a perfunctory activity with no more meaning than checking off an item on a checklist. In general, very little reliability credit was allowed for the requirement to sign off that a procedure has been completed.

In general, the degree of personnel redundancy was high for calibration operations, lower for certain operator tasks such as manipulating MOV's, and lowest for maintenance tasks. However, in the case of the latter, a highly reliable recovery factor was the testing of maintained system components before the system was put back on line.

4.3.5 Common Events - Human Death Rates

Probabilities often become more tangible by comparison to the likelihood of familiar events which are sensitive in nature. Table 4-13 summarizes the death rate for U.S. citizens for selected causes. Table 4-14 summarizes the death rates for selected accident types.

Table 4-13 Overall U.S. Death Rates (1980)*

	Rate** Per 100,000	Probability***
From All Causes	876.0	0.9×10^{-2}
Heart Disease	436.0	0.4×10^{-2}
Cancer	184.0	0.2×10^{-2}
Pulmonary 25		
Pneumonia, Diabetes, Etc.	88.0	0.9×10^{-3}
Accidents	47.0	0.5×10^{-3}
Suicide	11.9	1.0×10^{-4}
Homicide	10.7	1.0×10^{-4}

Table 4-14 U.S. Accidental Death Rates* (1980)

	Rate** Per 100,000	Probability***
All Accidents	47.0	0.5×10^{-3}
Motor Vehicle	23.5	0.2×10^{-3}
Falls	5.9	0.6×10^{-4}
Drowning	2.7	0.3×10^{-4}
Fires	2.6	0.26×10^{-4}
Poisoning	1.1	1.0×10^{-5}
Air	0.7	0.7×10^{-5}
Boating	0.6	0.6×10^{-5}
Rail	0.3	0.3×10^{-5}
Explosives	0.1	1.0×10^{-6}

*Source: U.S. National Center for Health Statistics, "Vital Statistics of the United States" (Annual)

**Number of deaths per year per 100,000 people.

***Probability of an individual death in a one-year period of time.

4.4 REFERENCES

(1) O'Connor, Patrick, Practical Reliability Engineering (Second Edition), Wiley, 1985.

(2) AFWAL-TR-83-2079, Weibull Analysis Handbook, November 1983.

(3) Technical Report 79-1359," Development of STS Failure Probabilities - MECO to Payload Separation," J. H. Wiggins Co.," October 1979

(4) Technical Report 81-1329, "Space Shuttle Range Safety Analysis," J. H. Wiggins Co., July 1981.

(5) Technical Report 82-1404, "Development of STS Failure Probabilities - Liftoff to Centaur Separation," J. H. Wiggins Co., February 1982.

(6) AFWAL-TR-83-61, "Review of Shuttle/Centaur Failure Probability Estimates for Space Nuclear Mission Applications," R. K. Weatherwax, E. W. Colglazier (SERA, Inc), December 1983.

(7) SAND 84-1579, "Review and Evaluation of Wiggins' and SERA Space Shuttle Range Safety Hazards Reports for the Air Force Weapons Laboratory," D. D. Carlson et al (Sandia National Laboratories), December 1984.

(8) Briefing Notes, "Solid Rocket Motor Reliability," Louis J. Ullian (Easter Space and Missile Center, Patrick AFB), undated

(9) Wash 1400, "Reactor Safety Study," Nuclear Regulatory Commission, October 1975.

(10) NUREG 0492, "Fault-Tree Handbook" November 1978.

(11) "Missile Vulnerability Study - Program 624A," USAF, Range Safety Division, June 1962.

(12) JSC 16087, "Space Shuttle Data for Nuclear Safety Analysis (Revision 2)," November 1983.

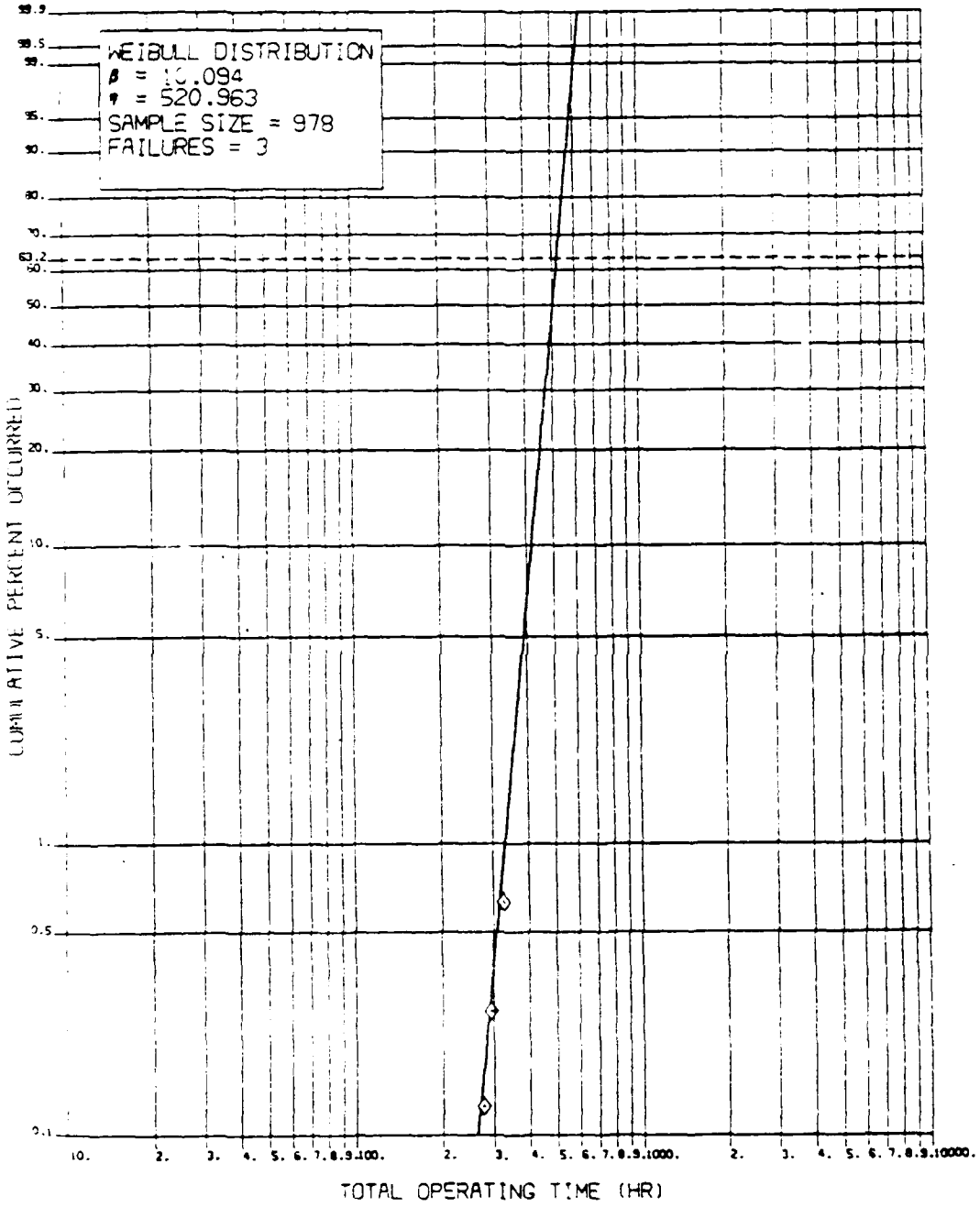


Figure 4-1 Weibull Plot for Augmentor Pump Bearing

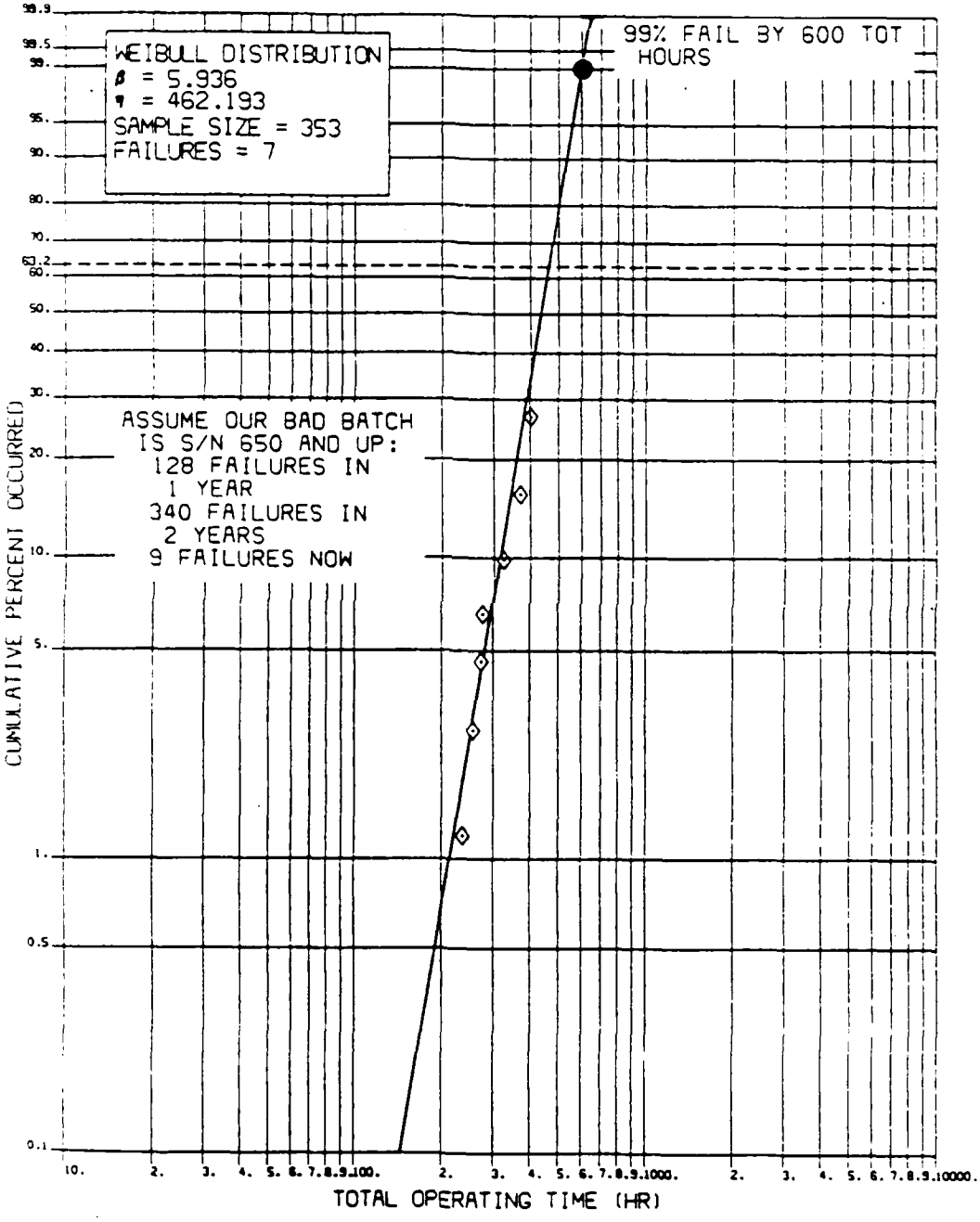


Figure 4-2 Augmentor Pump 650 and Up

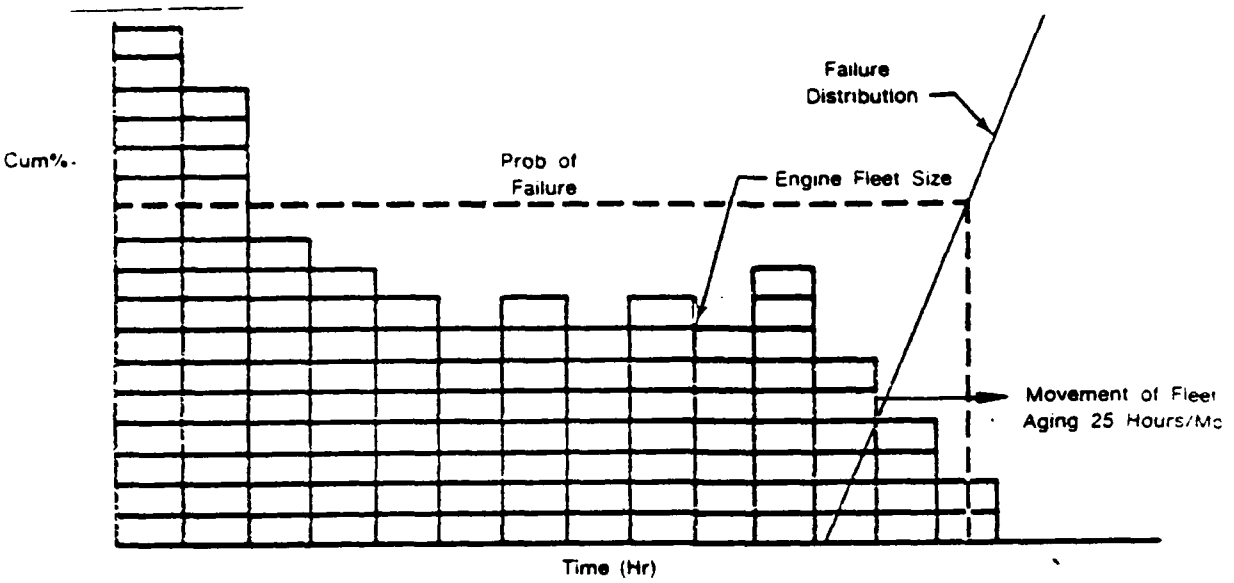


Figure 4-3 Risk Analysis

Cumulative Failures	*Forecast Future Failures*
9.17	0.0 More Failures In 0 Months
12.26	3.12 More Failures In 1 Months
16.22	7.08 More Failures In 2 Months
21.14	11.98 More Failures In 3 Months
27.18	18.02 More Failures In 4 Months
34.50	25.33 More Failures In 5 Months
45.21	34.05 More Failures In 6 Months
53.44	44.27 More Failures In 7 Months
65.24	56.07 More Failures In 8 Months
78.65	69.48 More Failures In 9 Months
93.64	84.47 More Failures In 10 Months
110.14	100.97 More Failures In 11 Months
128.01	118.85 More Failures In 12 Months
147.11	137.94 More Failures In 13 Months
167.21	158.05 More Failures In 14 Months
188.08	178.91 More Failures In 15 Months
209.40	200.24 More Failures In 16 Months
230.82	221.66 More Failures In 17 Months
251.89	242.73 More Failures In 18 Months
272.07	262.90 More Failures In 19 Months
290.75	281.58 More Failures In 20 Months
307.32	298.16 More Failures In 21 Months
321.27	312.11 More Failures In 22 Months
332.29	323.12 More Failures In 23 Months
340.34	331.18 More Failures In 24 Months
β = 5.94	η = 462.2 N = 353

Figure 4-4 Projected Pump Failures

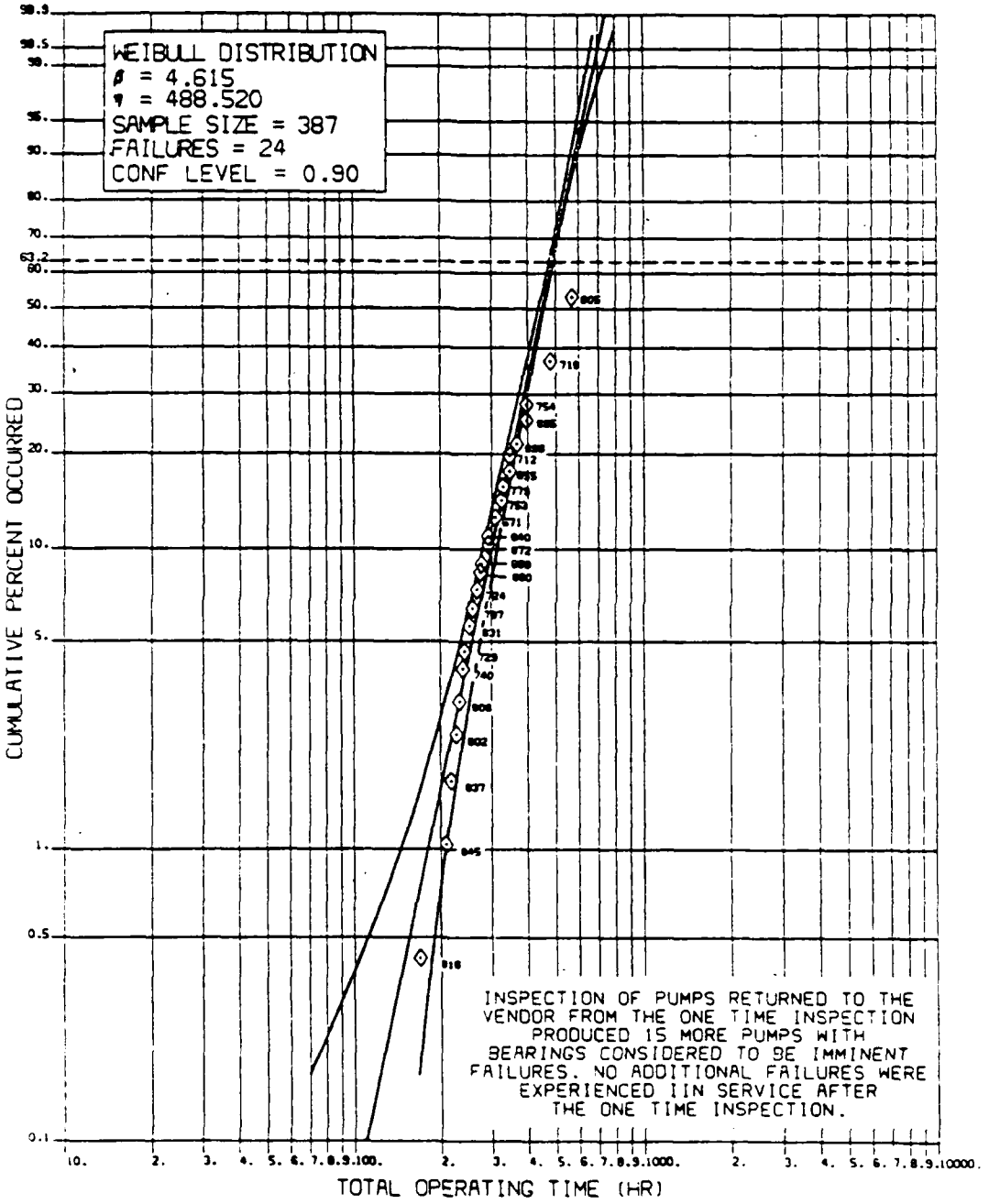


Figure 4-5 Weibull Plot For Augmentor Pump

Chapter 5
Post-Accident Environments

CHAPTER 5
POST ACCIDENT ENVIRONMENTS

TABLE OF CONTENTS

Section	Title	Page
5.0	Introduction	5-1
5.1	Blast (Overpressure)	5-1
5.1.1	Characteristics of Blasts and Explosions	5-1
5.1.1.1	TNT Equivalent Weights	5-3
5.1.2	Database for Liquid-Propellant Explosions	5-6
5.1.2.1	Pyro Project	5-6
5.1.2.2	JSC (Fletcher Analysis)	5-7
5.1.2.3	A.D. Little Tests	5-7
5.1.2.4	Sandia Laboratories	5-7
5.1.2.5	Other Investigators	5-7
5.1.3	Liquid Propellant Blast Determination Methods	5-9
5.1.3.1	LO2/LH2 Systems	5-9
5.1.3.2	LO2/RP-1 Systems	5-12
5.1.3.3	Hypergolic Bi-Propellant Systems	5-16
5.1.3.4	Overpressures and Impulse from Values of Y	5-17
5.1.4	Database for Solid-Propellant Explosions	5-18
5.1.5	Solid-Propellant Blast Determination Methods	5-19
5.1.5.1	XDT (High Velocity Impact)	5-21
5.1.5.2	Failure Other than HVI	5-22
5.2	Fragmentation	5-24
5.2.1	Solid Rocket Motor Fragmentation	5-24
5.2.2	Liquid Propellant Tank Fragmentation	5-26
5.2.3	Pressurized Tanks and General Applications	5-27
5.3	Thermal (Fire)	5-30
5.3.1	Fireball Development Time-History	5-30
5.3.2	Liquid Fireball Size and Duration	5-31
5.3.2.1	Fireball Size	5-31
5.3.2.2	Fireball Duration (Tau)	5-32
5.3.3	Solid Propellant Fireball Size and Duration	5-32
5.3.4	Fireball Thermal Effects	5-35
5.3.4.1	Adiabatic Flame Temperature	5-35
5.3.4.2	Heat Flux from Fireball	5-35
5.3.5	Roadmap	5-38
5.4	Toxicity	5-41
5.4.1	Chemical Compounds Released	5-41
5.4.2	Lifetime/Fate of Released Chemicals	5-41
5.4.3	Atmospheric Dispersion	5-42
5.4.4	Roadmap	5-42
5.5	Acoustic	5-56
5.5.1	STS Acoustic Environment Example Data	5-56
5.6	References	5-57

LIST OF FIGURES

Figure No.	Title	Page
5-1	Qualitative Variation of Shock Wave Parameters With Distance and Time	5-61
5-2	Important Shock Wave parameters	5-62
5-3	Overpressure Scaled Distance Plot Showing Typical Levels for Blast Damage	5-63
5-4	Ratio of Free Air Peak Overpressure (P-Cylinder/P-Sphere) vs Distance for Cylinders with Differing Aspect Ratios	5-64
5-5	Overpressure vs. Log Normal Probability of Occurrence for Near-Field Distances	5-65
5-6	Normalized Pressure and Impulse Yields from Explosion of N2O4/Aerozine-50	5-66
5-7	Representative Shock Impulses Showing Coalescence of Shock Waves from Dissimilar Sources (Stages (a) through (d))	5-66
5-8	Trend in Measured Equivalent TNT Weight from LOX/LH2 Propellant Explosions Compared to Design Rules	5-67
5-9	Models of Liquid Propellant Mixing Zone Thickness	5-68
5-10	Multiple Mixing Zones in a Liquid Propellant	5-69
5-11	Estimated Terminal Yield as a Function of Combined Propellant and Oxidizer Mass	5-70
5-12	Normalized Terminal Yield vs. Ignition Time for LO2/LH2 CBGS	5-71
5-13	Terminal yield vs. Ignition Time for LO2/LH2 CBM	5-72
5-14	Comparison of Prediction Equation for LO2/LH2 CBM Case with Experimental Data for All Cases but L/D of 1.8 and Do/Dt of 1 (0-200 lb., - 1,000 lb)	5-73
5-15	Therminal Yield, Upper 90% Prediction, for LO2/LH2 CBM Case	5-74
5-16	Terminal Yield vs. Scaled Time for LO2/LH2 CBGS Case as a Function of Impact Velocity	5-75
5-17	90% Prediction Terminal Yield vs. Scaled Time for LO2/LH2 CBGS Case	5-76
5-18	Maximum Terminal Yield vs Impact Velocity for LO2/LH2 CBGS Case (Fall Back)	5-77
5-19	PYRO High Velocity Tests Prediction Chart for LO2/LH2	5-78
5-20	LO2/RP-1 CBM Terminal yield (Y) vs. L/D	5-79
5-21	LO2/RP-1 CBM k Factors vs Ullage Volume (Vu) as a function of delta P	5-80
5-22	LO2/RP-1 CBM Terminal Yield (Y) vs T/(W**(1/3)) as a Function of L/D and k	5-81
5-23	LO2/RP-1 CBM Terminal Yield Upper Bound (Y90) vs t/(W**(1/3)) as a Function of L/D and K	5-82
5-24	LO2/RP-1 CBGS 90% Terminal Yield (Y) vs. T/(W**(1/3))	5-83
5-25	LO2/RP-1 CBGS Terminal Yield (Y90) vs. T/(W**(1/3))	5-84
5-26	LO2/RP-1 CBGS Terminal Yield (Y) vs. Impact Velocity	5-85
5-27	Terminal Yield vs Impact Velocity for LO2/RP-1 HVI	5-86
5-28	Terminal Yield as a Function of Impact Velocity and surface type for hypergolic propellant systems	5-87
5-29	Overpressure and Positive-Phase Impulse vs. Scaled Distance (Lambda) for TNT	5-88
5-30	Overpressure vs Cumulative Log Normal Probability of Occurrence for Near-Field Distances	5-89
5-31	Geometry vs Critical Value adjustment to the Critical diameter	5-90

LIST OF FIGURES - continued

Figure No.	Title	Page
5-32	Geometry vs Critical Value adjustment to the Critical diameter (continued)	5-91
5-33	Impact Velocity vs TNT % Equivalent	5-92
5-34	Overpressure vs Scaled Distance (Lambda) for TNT Indicating Levels of Blast Damage	5-93
5-35	Positive Impulse vs Scaled Distance (Lambda) for Hemispherical and Spherical TNT Charges located on the ground surface	5-94
5-36	Titan 34D-9 Mishap. SRM1 Fragmentation Pattern	5-95
5-37	Titan 34D-9 Mishap. SRM2 Fragmentation Pattern	5-96
5-38	Titan 34D-9 Mishap. SRM2 Frequency vs Fragment Area	5-97
5-39	Titan 34D-9 Mishap. SRM2 Frequency vs Fragment Area	5-98
5-40	Titan 34D-9 Mishap. Fragment Velocity vs Impact Distance	5-99
5-41	Titan 34D-9 Mishap. Cummulative Percent vs Fragment Velocity	5-100
5-42	"Clamshell" Opening of a SRM Case After Command Destruct	5-101
5-43	STS 51-L Mishap, SRB Fragment Size Distribution	5-102
5-44	STS 51-L Mishap, SRB Fragment Velocity Distribution	5-103
5-45	Percentage of Total Weight of Vehicle Fragments within Range Indicated	5-104
5-46	Fragment Number and Weight Distributions	5-105
5-47	Gurney Equations for Simple Geometrics	5-106
5-48	Dimensionless Velocity of Metal as a Function of Loading Factor M/C	5-106
5-49	Typical Fireball Development	5-107
5-50	Fireball Development (Liquids)	5-108
5-51	Heat flux vs dimensionless time for LO2/LH2	5-109
5-52	Heat flux and Temperature vs dimensionless time for LO2/LH2	5-110
5-53	Fireball Temperature vs Time for a Saturn V abort (LO2/RP-1)	5-111
5-54	Temperature vs Time for LO2/LH2 Example Problem	5-112
5-55	Fireball Diameter vs Time for LO2/LH2 Example Problem	5-113
5-56	Equations in Conventional Notation	5-114

LIST OF TABLES

Table No.	Title	Page
5-1	Terminal Yields for Hypergolic Bi-Propellants	5-16
5-2	Vessel Configurations for NOL Fragmentation Tests	5-28
5-3	Fragment Distribution of Bursting Gas Tanks	5-29
5-4	Fragmentation Velocity Data for Bursting Gas Tanks	5-29
5-5	Adiabatic Flame Temperatures of Propellants	5-34
5-6	Some Maximum Observed Heat Fluxes From Fireballs	5-37
5-7 thru 5-26	5-26 Chemical Toxicities (Various common liquid propellants, propellant combinations, and solid propellants)	5-44 thru 5-55

CHAPTER 5
POST ACCIDENT ENVIRONMENTS

5.0 INTRODUCTION

The available methodology and data base for predicting the post-accident environments of blast, fragments, fire, toxicity and acoustics are discussed in this chapter along with adequacies and limitations of the methods and daca. Major emphasis is given to description of the environments associated with the catastrophic failure of the complete space vehicle. CPIA Publication 394, Hazards of Chemical Rockets and Propellants, Volume I, (Reference 1) is a good source for descriptions of a large portion of the methodologies. Other pertinent methods from the Annotated Bibliography and critical reviews will be discussed.

With certain notable exceptions discussed below, the post-accident environments are reasonably well defined within certain broad regions where experimental data are available or where analytical solutions are relatively straight forward.

In order to make the text portion of this document compatible with most word processing systems, many of the equations presented are in a nonstandard format. To clarify some of these equations, their conventional forms can be found listed in Figure 5-56 by equation number. (For example, D = 11.05*Wb**0.306 is represented by Eg 5.3.2 in Figure 5-56).

5.1 BLAST (OVERPRESSURE)

The overpressure-time characteristics of the shockwave produced by the accidental detonation of propellants is dependent on a wide range of factors. These factors include type and amount of propellant, configuration of the vehicle, failure mode, distance from detonation, propellant mixing time (Bi-propellant) and several other factors. As a result, theoretical estimates of blast overpressures are just that - rough estimates. In certain specific instances there is empirical data available to be used for blast overpressure determination, but this is the exception, not the rule. In this section both empirical and theoretical methods will be discussed and combined as required.

5.1.1 Characteristics of Blasts and Explosions

Blasts and explosions range from high-order detonation of high-energy propellants to fading detonations and deflagrations of lower-energy propellants. Bursting of compressed gas containers can also cause lower level blast overpressures. The more rapid the release and the greater the available energy, the more violent is the explosion. The rate of energy release is governed by the speed that the reaction zone propagates through the propellant. If the speed is supersonic, the reaction is termed a detonation and extremely high pressures can be produced. If the speed is nearly sonic, the reaction is termed deflagration and much lower pressures are produced. The speed of the reaction zone through the propellant is not necessarily constant. When an initial high-order (fast) detonation slows down, it is a fading detonation. An initial deflagration or low-order (slow) detonation can also speed up to become a detonation of higher-order with attendant higher pressures. Normal combustion occurs at subsonic speeds.

The sequential detonations of multiple charges were investigated by J.J. Swatosh, Jr. (Ref. 2). At far-field distances two sequential detonations merge into one that has the same overpressure as a single detonation of the combined charges. If three charges are sequentially detonated the last shock wave overtakes the second, but then the combined wave still lags the initial wave. (If the combined wave is stonger than the initial wave, it will eventually overtake the initial wave.) At near-field distances all waves remain discrete.

Blast characteristics for liquid propellant explosions tend to be more dependent on the type of accident, configuration, and initiation source than do solid propellants. While the theoretical energy release of a given volume of liquid propellants remains constant, the actual energy released and rate of energy release are highly dependent on the extent of mixing (for bi-propellants) prior to ignition, and the physical properties of the propellants at the time of ignition (temperature, pressure, etc). For example, a pressurized tank of hydrazine at room temperature will most likely not detonate if suddenly ruptured. However, if the hydrazine is heated to its autoignition temperature prior to rupture, a detonation is much more likely to occur.

For bi-propellant systems, several additional factors must be considered when determining their blast characteristics. These include:

(1) Release of the maximum potential energy requires intimate mixing of the fuel and oxidizer, as well as its ignition.

(2) Mixing of the propellants is expected during a catastrophic failure. The degree of mixing that occurs is mostly dependent on the failure mode and the amount of time allowed for mixing before ignition (Hypergolics by their very nature autoignite thus relatively small amounts of mixing occur before ignition).

(3) The amount of mixing of the propellants will vary locally, so local energy release rates will also vary. Thus, both deflagrations and detonations can occur simultaneously in a propellant mass at different locations. The overall nature of the reaction process will depend on the aggregate of the local states.

(4) Testing has shown that bi-propellant systems are capable of producing high order explosions.

(5) Unlike solid propellants, the ignition source for non-hypergolic bi-propellants has little effect on the reaction rate of the reaction. (For example, it has been shown that a small spark or even an incadescent light filament can initiate a detonation in a LO2/RP-1 mixture).

(6) Some data suggests that small local zones of mixed non-hypergolic bi-propellants may self initiate under certain conditions. (Refs. 3, 4) (Note: These findings are not supported by the PYRO investigators.)

For solid propellants, more energy is required to initiate detonations than deflagrations or normal burning. The initiation energy necessary for detonations is dependent on propellant composition including:

(1) Type
(2) Composition
(3) Grain Size
(4) Presence and size of voids

Also, a critical diameter exists that influences how the solid propellant will detonate. (Critical diameter will be discussed more thoroughly in a later section.) If its diameter is greater than its critical diameter, it is capable of propagating a stable high order detonation. The transition to high-order detonation is related to a critical impact velocity (initiation energy). Stress concentration and propellant fracture or crushing during impact can increase the sensitivity of the propellant to detonation (Ref. 6). There are some data from the Eastern Test Range (Ref. 5) that indicate high-order detonations from propellants that do not normally detonate high-order.

A common characteristic of gaseous explosions is the fact that peak pressures are considerably lower than those for solid or liquid explosions, but the time duration phase of the pressure (specific impulse) is much longer. Peak overpressures can be expected to be lower when generated by explosives with lower energy densities (such as gas mixtures in comparison with liquids or solids) when the same total energy is released. The pulse duration for the liquid or solid reactions in such a case would be shorter than for the gas reaction because they represent a smaller extent of much denser material and, hence, a much shorter time for all the material to react. This leads to higher peak overpressures and shorter durations than for low density explosions involving the same total energy release.

An explosion initially creates a compact volume of high-energy gases. The outward expansion of these gases creates a shock wave that initially travels at supersonic velocity that decays with distance and time. Figure 5-1 shows the spacial and temporal variations of overpressure, density, temperature and gas particle velocity. Figure 5-2 depicts the time variation of the overpressure at a given location. The positive and negative phases of the pressure wave is shown as well as the definition of the positive phase impulse.

5.1.1.1 TNT Equivalent Weights - The explosion characteristics of different propellants and pressurized containers are commonly referenced to a standard explosive, TNT. This is done to take advantage of the large amount of experimental data that is available for TNT explosions. These data include blast information as a function of charge size, shape, orientation, charge location (air, surface or buried), measurement location (side-on, face-on, or reflected pressures) and impulse as well as the spacial and temporal attenuation.

An example of damage levels for various targets related to TNT explosions is given in Figure 5-3. It should be noted that most blast damage is a result of both peak overpressure and positive-phase impulse loading.

Figure 5-3 is meant to be used only as a rough approximation of blast damage based on peak overpressure only. In general, lower charge weights will cause damage due only to impulse loading, and higher charge weights will cause damage only due to peak overpressure. Figure 5-4 is an example of the data that is available to correct peak overpressure values for geometric effects.

TNT Equivalent Weight can be defined in three general ways. It can be based on:

(1) Total energy released;

(2) Equivalent blast parameter such as pressure or impulse at a specific location;

(3) Equivalent explosive damage such as cratering or witness plate deformation at a specific location.

In other words, TNT Equivalent Weight is defined as that amount of TNT required to produce the same energy release, blast characteristic, or explosion damage as the actual propellant or pressurized tank would upon explosion.

Unfortunately, many, if not most, of the published reports dealing with propellant blasts do not specify the reference TNT pressure-distance or impulse-distance data that is used. Nor do they specify what locations or combination of locations were used to derive the TNT equivalent weights. Thus, it is quite easy to misapply published TNT equivalent weight results.

When the TNT Equivalent Weight is determined from a blast parameter such as overpressure, it is done at a specific distance from the source. Extrapolation to any other distance using the TNT pressure-distance curves can introduce error when the rates of energy release between propellant and TNT differ. This difference is most pronounced for liquid propellants at close-in distances. When the TNT Equivalent Weight is determined from overpressure at a large distance from the explosion, the TNT Equivalent Weight is sometimes referred to as the terminal yield.

The blast overpressures for liquid propellants can vary significantly from that predicted by TNT equivalent weights in the near-field (overpressures greater than 40 psi). In the near field, shock wave characteristics are quite different. Liquid propellant mixtures produce considerably longer shock durations (impulse) but somewhat lower peak overpressures. Because of these discrepancies, project PYRO recommends that the impulse be doubled (estimated on a TNT Basis) in the near field for liquid propellant explosions. However, there were still uncertainties about near field explosion characteristics after PYRO.

"As a result of these uncertainties, NASA/MSFC and AF/ESMC derived a new characterization for the near field PYRO data. In summary, 78 experimental LH2 and LO2 tests were reviewed with respect to their near field characteristics. These involved propellant quantities ranging from 133 to 100,000 lbs and three major mixing modes; i.e., internal mixing within the tankage (CBM), spilling onto the ground (CBGS), and high velocity impact (HVI) on the ground surface.

In order to reduce the variability resulting from an obscure center of explosion, a new zone approach was used, i.e., the Diameter (D-zone) method. The zones were defined in terms of the diameter of the LH2/LO2 tankage, i.e., "1D" is a zone from the tank wall to a distance away equivalent to the diameter of the cylindrical portion of the tankage. The "2D" zone is at a distance between one and two diameters away from the tank wall in Project PYRO.

Overpressure measurements were obtained at approximately one, two, and three diameters from each explosion. One hundred and sixty six data points were obtained of which 37 were at the closest gauge position (1D); 11 of which were by internal mixing (CBM) and 26 by spill mode (CBGS). These data were averaged, standard deviations were obtained, and the results were plotted on probability paper in terms of spill mode and zones." (Ref. LASP Subpanel Review). See Figure 5-5 for a graph of these results.

Several investigators have used the concept of percent yield to denote the relationship of TNT equivalent weight defined by a blast parameter to the TNT equivalent weight defined by energy release.

$$Y = 100 * [(W(TNT) \text{ from Explosion})/(W(TNT) \text{ form Energy})]$$

$$= 100 * [\text{Mass of propellant mixed/Total mass of Propellant}]$$

Where: Y = percent yield
W(TNT) = Equivalent weight of TNT, lb.

This concept is most frequently applied to liquid propellant explosions to account for fuel and oxidizer mixing. Recall that only the mixed propellant can explode. Unfortunately, the amount of mixed propellant is not readily measured. Instead, such parameters as total propellant weight, time to ignition and impact velocity are measured. Examples of percent yield as functions of these parameters, derived from experimental data, will be presented in the data that follows.

5.1.2 Database for Liquid Propellant Explosions

The major source of liquid propellant explosion data are:

(1) PYRO Project (1964-1968)
Refs. 7, 8, 9, 10*, 11*, 1*, 48, and 12*.

(2) JSC (Bob Fletcher) Analysis of Liquid Propellant Test (1965-1968)
Refs. 13, 14, 15, 16, and 17.

(3) A.D. Little Tests (1960-1967)
Refs. 18, 19, and 20

(4) Sandia Research (1965-1966)
Refs. 21 and 22

*These reports used data generated by Project PYRO but were not written or guided by the PYRO investigators. (Reports were authored by Baker, Gunther, or Rosenfield).

5.1.2.1 PYRO Project - The PYRO Project, the most comprehensive liquid propellant test program to date, was a test program to develop a method for predicting the credible damage potential of liquid propellant missiles or space launched vehicles. Hypergolic and cryogenic propellants were studied. The cyrogenic systems included LO2/RP-1 and LO2/LH2 up to 100,000 lbs (45,350 kg) and the hypergolic system was Aerozine-50/N204. The launch vehicle stages of interest were the Saturn S-IV and Titan 1 first stage.

The PYRO tests were conducted to simulate three types of propellant mixing (failure modes).

(1) Confinement by Missile (CBM). This simulates failure of an interior bulkhead separating fuel and oxidizer in a vehicle stage;

(2) Confinement by Ground Surface (CBGS). This simulates fall back or tipover of the vehicle to the ground with subsequent tank rupture and ignition;

(3) High Velocity Impact (HVI). This simulates high velocity impact of the vehicle on the ground; both hard and soft ground surface impacts were studied.

For all of these tests where LO2/LH2 was used, the propellants were in the configuration of LH2 over LO2 as in the Saturn booster. (The STS configuration is opposite of that).

Project PYRO (Refs. 7, 8, 9) gave the results as a function of propellant type (LO2/LH2, LO2/RP1, N204/50% UDMH-50%N2H2) and failure mode (CBM, CBGS, and HVI) as well as of the other important controlling parameters such as impact velocity, time of ignition, propellant orientation, and tank L/D ratio. Rosenfield (Ref. 12) also conducted an independent evaluation of PYRO data.

5.1.2.2 JSC (Bob Fletcher Analysis of Liquid Propellant Tests (1965-1968) - The study of phenomena associated with mixing of Cryogenic Fluid (Nishibayashi, et. al., Ref. 17) supported the PYRO conclusion of Willoughby et al. The modes of mixing investigated were bulkhead-rupture and impinging stream. It was concluded in this 1965 report that there is a relatively small amount of mixing when hydrogen is spilled into oxygen, whereas mixing occurs to a greater (approximately an order of magnitude more violent) extent if the order is reversed. These tests substantiated that yield is proportional to mixing.

Fletcher also showed and discussed the difference of liquid propellant explosions from TNT explosions. Figure 5-6 shows normalized yield versus distance. Normalized yield is a measure of how the derived TNT Equivalent Weight changes with changing locations. Figure 5-7 illustrates shock impulse changes with distance and time for liquid and solid explosions.

5.1.2.3 A.D. Little Tests - The Technical Memorandum on Explosive Effects produced by Failure of Launch Vehicles (A.D. Little, Ref. 19) recommended in 1967 a program to establish modes of structural failure and the mechanisms that will cause ignition of escaping propellants during credible accident situations. This information would be necessary to best utilize the model tests results from Project PYRO.

5.1.2.4 Sandia Laboratories - Pad abort was investigated by Sandia in 1965-1966. Kite and Webb (Ref. 22) evaluated blast overpressure for the PAM vehicles. Kite and Bader (Ref. 21) used data from the PYRO project and existing data from pad aborts (including the 1965 Atlas-Centaur abort) to obtain radiant heat flux and fireball temperature information.

5.1.2.5 Other Investigators - The study of detonation induction in solid propellants by liquid propellant explosion (Irwin, Ref. 23) was reported in 1964 because of the increased production of vehicles which employ both solid and liquid stages. This pioneer work confirmed a full scale detonability test with N2O4/Aerozine-50 which gave a TNT equivalence of 33 - 47%, indicating that appreciable mixing occurred before initiation with the explosive booster. The experimental method used for the full scale testing was a concentric vessel with a L/D ratio of 4.1.

Another expression for TNT Equivalent Weight including upper and lower bounds and a comparison to design rules for LO2/LH2 was derived by Sutherland in 1978 and is shown in Figure 5-8. The result that the amount of mixed propellant is proportional to the 2/3 power of the total propellant weight is consistent with a model of mixing zone thickness that is independent of scale. Figure 5-9 illustrates two mixing zone models; one independent of scale and the other proportional to scale (Ref. 24). The 2/3 power correlation for the PYRO data is likely to be fortuitous since the mixing models can't be universal. The larger scale PYRO tests (6 each) were not truely comparable because equivalent mixing conditions were not replicated. Mixing is dependent on many parameters, such as relative density of the liquids, the manner of mixing, and the relative volumes and geometries of the liquid spills.

The ideas of multiple mixing regions is shown in Figure 5-10 (Ref. 24). This is similar to the multiple point explosion model for ground spills being developed by Mr. W. Riehl, MSFC. (Discussed Later)

For small quantities of propellants that are of nearly stoichiometric mass ratio, the total propellant mass is expected to explode. This trend was obtained from the small quantity tests of Project PYRO. Figure 5-11 shows this relationship for the three propellant combinations as derived by Baker, et al. (The yields presented in Figure 5-11 should be considered worst-case upper bound values.)

As mentioned earlier, the PYRO tests did not measure the amount of mixed propellants; instead the extent of mixing, or amount of propellant that can react, was related to measured quantities such as impact velocity and time to ignition.

Figures 5-28 and 5-19 present the percent terminal yield versus impact velocity for the hypergolic and the LO2/LH2 propellant systems, respectively. The distinction between impact on a hard or soft surface accounts for the increased confinement (and increased mixing or faster energy release) provided by the soft surface.

The current data and prediction methods available are not extremely precise. As an example of the variability of liquid propellant explosions, Figures 5-12 and 5-13 relate percent terminal yield to ignition time for the LO2/LH2 propellant for "Confined by Ground Surface" and "Confined by Missile", respectively. The large shaded region denotes the test data variability. The large variance from the theoretical analysis indicated by these figures (Figures 5-11, 5-12, and 5-13) and experimental data (PYRO and others) could be due to ignoring the observed dependence of explosive yield for such controlling variables as: impact velocity, scaled time by propellant mixture weight, degree of diaphram opening area, and the dynamic forces for pressing the mixing (i.e., impact velocity, or static gravity forces). Relating percent terminal yield to ignition time in this manner is far from precise, and using these figures can be very misleading. Much more work is required to refine the theoretical analysis techniques used to predict the blast environments of liquid propellants. Field tests now underway by NASA at the White Sands Test Facility in New Mexico should help to refine the analysis techniques for LO2/LH2 mixtures.

5.1.3 Liquid Propellant Blast Determination Methods

The majority of the methods discussed in this section were developed during Project PYRO (Ref. 9). Before the blast effects of a liquid propellant accident can be determined, several specific aspects of an accident must be determined. These include:

(1) Failure Mode

- (a) Confined by Missile (CBM)
- (b) Confined by Ground Surface (CBGS)
- (c) High Velocity Impact (HVI)

(2) Type(s) and amount(s) of propellant involved in the accident

- (a) LH2/LO2
- (b) N2O4/Amine Fuels
- (c) LO2/RP-1
- (d) Amine Fuels Alone
  - i) Hydrazine (N_2H_4)
  - ii) Monomethyl Hydrazine (MMH)
  - iii) Unsymmetrical Dimethylhydrazine (UDMH)

(3) If a bi-propellant system, the configuration and orientation of the tanks at time of accident is needed (e.g., LH2 over LO2 or vice-versa).

(4) Time of mixing if system is bi-propellant (function of failure mode, type of propellant, tank configuration, and confinement).

Once an accident scenario has been defined by the above parameters, the blast environment can be approximated.

5.1.3.1 LO2/LH2 Systems

Confined By Missile (CBM)

Parameters needed before blast calculation are propellant mixing time (t, msec), total propellant weight (W, lb), length to diameter ratio of the propellants, (L/D), and intertank bulkhead opening ratio (Do/Dt) (ratio of diameter of opening in intertank balkhead to tank diameter. If opening is non-circular, use effective circular diameter).

(1) Determine length to diameter ratio of the propellants, (L/D).

(2) Determine anticipated intertank bulkhead opening ratio (Do/Dt) (Diameter of opening in between the LO2/LH2 tanks divided by total tank diameter. If opening is non-circular, use effective circular diameter.)

(3) If L/D GTE 5.0 or L/D GTE 1.8 and Do/Dt LTE 0.45:

(NOTE: GTE = Greater Than or Equal to . LTE = Less Than or Equal to.)

(a) Obtain terminal yield (Y) and upper 90% prediction values from Figure 5-14. MSEC is the millisecond mixing time and LB **(1/3) is the TOTAL propellant weight raised to the 1/3 power.

(b) Go to Section 5.1.3.4 and find P(over) and Impluse using Y and Y90 from Step 3a.

(4) If L/D LTE 5 and Do/Dt GTE 0.45:

(a) Compute t/(W**(1/3))
(b) Determine terminal yield (Y) and upper 90% predaiction value from Figure 5-15
(c) Go to Section 5.1.3.4 and find P(over) and Impulse using Y and Y90 from Step 4b.

LO2/LH2 Confined by Ground Surface (CBGS)

Parameters needed before blast calculations are propellant mixing time (t,mesc), total propellant weight (W, lb.), propellant velocity (ft/sec.), and failure subtype. Failure subtypes are:

A. Fallback with simultaneous massive breakage of both tanks.
V = velocity of interface between propellants (ft/sec)
t = time between release of bottom propellant and ignition (msec)

B. Fallback - same as A only release of top propellant is considerably delayed over bottom

C. Non-massive tank rupture. Propellant is released through openings significantly smaller than tank cross section.

D. Fallback onto launch structure, formation of a "Pool" of mixed propellants (mixing time approx. 100msec). This analysis also requires that the depth of the pool be known. (Xpool) (Method developed by RDA and Reported in the Space Shuttle Data book, NSTS08116 Rev A).

For failure subtypes A & B where mixing times are known:

(1) Calculate t/(W**(1/3)) and find Y and Y90 from Figure 5-16 and 5-17 respectively.

(2) Go to Section 5.1.3.4 and find P(over) and Impulse based on the Y and Y90.

For failure Subtype C where mixing time is known:

(1) Calculate t/(Wf**(1/3))

Wf = weight of propellants on ground at time of ignition, NOT total propellant weight.

(2) Follow steps 1 and 2 above, but note that the terminal yield value is multiplied by Wf in place of W to get equivalent weight in pounds. In no case should an equivalent weight in lb be used that is less than that given in the first procedure (mixing time known) and t/(W**(1/3)) = 0

For failure Subtypes A, B, and C where mixing times are unknown:

(1) Calculate t/(W**(1/3))

(2) Using the approximate impact velocity of the vehicle, find Y and Y90 from Figure 5-18.

(3) Go to Section 5.1.3.4 and find P(over) and Impulse based on these Y and Y90 values.

For failure Subtype D where pool depth (Xpool) is known:

(1) Determine X, the distance above the pool that pressure impulse data is desired.

(2) Find X/Xpool

(3) Calculate Q(t=0) (heat release) and Rho(t=0) (initial reactant density).

For 2.5 GTE(X/Xpool) LTE 119

0.0056 GTE Rho (t=0) LTE 0.4 g/cc
500 GTE Q(t=0) LTE 3660 cal/g

For 1.0 GTE (X/Xpool) LTE 2.5

Rho(t=0) = Constant = 0.0056 g/cc
Q(t=0) = Constant = 1050 cal/g

(4) Calculate the static overpressure (P(over))

P(over) = 2557.7 * Rho(t=0) * Q(t=0) * [((Q(t=0)/1000))**0.25]*
[((Rho(atm) * X)/(Rho(t=0) * X(t=0)))**0.223]
*[(Rho(t=0)/Rho(atm))**-0.9] * [1+8 * ((Q(t=0)/1000)**0.5)
*((Rho(atm) * X)/(Rho(t=0) * X(t=0))]**-1.0] eq. 5.1.1

Where: Rho(atm) = ambient density of atmosphere
X(t=0) = pool depth = Xpool

NOTE: Many of the equations contained in the text are reproduced in a more conventional format in Figure 5-56, and are listed there by equation number.

(5) Calculate the static Impulse (Isp)

ISP = A*Rho(t=0)*X(t=0)*(Q(t=0)**0.5)*[(Rho(t=0)/Rho(atm))**-0.45]
*[(Q(t=0)/1000)**0.1]*[((Rho(atm)*X)/(Rho(t=0)*X(t=0)))**m]
[1+0.2((Q(t=0)/1000)**-0.3)*((Rho(atm)*X)/
(Rho(t=0)*X(t=0)))]**-1.0 eq. 5.1.2

Where: for (Rho(atm)*X)/(Rho(t=0)*X(t=0) LTE 0.1343;
A = 0.0635 and m = -0.397
for (Rho(atm) * X)/(Rho(t=0)*X(t=0)) GT 0.1343;
A = 0.271 and m = 0.326

This analysis is best used for distances (X) up to only about 65 ft. Past the 65 ft distance the plane-wave assumption that this analysis is based upon yields conservative estimates of blast severity. It is recommended for distances greater than 65 feet that the method described for Subtype A be used.

LO2/LH2 High Velocity Impact (HVI)

The parameters needed to perform this analysis are total propellant weight (W), impact velocity (V, ft/sec), and the nature of the impacted surface (Hard or Soft).

Hard Surface: Essentially no penetration of surface by impacting tankage. (Example - Rock or Concrete)

Soft Surface: Essentially complete penetration of surface by tankage (e.g. - sand or swamp area)

(1) Determine Y and Y90 using the appropriate curve(s) on Figure 5-19.

(2) Go to Section 5.1.3.4 and calculate P(over) and Impulse using these values of Y and Y90.

5.1.3.2 LO2/RP-1 Systems - LO2/RP-1 systems are very similar to LO2/LH2 systems, but different terminal yield values have been determined. Because of their similarities, the methods used to calculate blast parameters are almost identical. Parameter definition can be found in the LO2/LH2 section.

LO2/RP-1 CBM

(1) (a) For W GTE 10,000 lb, Do/Dt LTE 0.45, and mixing time unknown, obtain Ys (yield for standard conditions of Vu = 10%, P_r = 85 psi) from Figure 5-20 as a function of L/D.

(b) Using Vu (tankage ullage volume, %) and Delta Pr (tankage burst pressure - Operating pressure), obtain k value from Figure 5-21.

(c) Calculate Y:

Y = k * Ys

Calculate Y90

Y90 = k * Ys-90

(d) Go to Section 5.1.3.4 and find P(over) and Impulse using these values of Y and Y90.

(2) For W GTE 10,000 lb, Do/Dt LTE 0.45, and mixing time known.

(a) Find k value as per Step 2 above.

(b) With the k and L/D values, enter Figure 5-22 and obtain maximum allowable t/(W**(1/3)) value. Compare with t/(W**(1/3)) value derived from known ignition time and use the smallest value, but in no case use less than 5 msec/lb**(1/3). Now enter Figure 5-22 again and with t/(W**(1/3)) and L/D values determine Y. Next enter Figure 5-23 and obtain Y90.

(c) Go to Section 5.1.3.4 and find P(over) and Impulse using these values of Y and Y90.

(3) If W LTE 10,000 lb and Do/Dt LTE 0.45

(a) Obtain Ys and Ys-90 using the procedure outlined in Step A-1 (above) if the ignition time is unknown and in Step B-1 (above) if it is known.

(b) Calculate terminal yield Y and Y90:

$$Y = Ys*(1 + (217/W))$$

$$Y90 = Ys-90\ (1 + (217/W))$$

(c) Go to Section 5.1.3.4 and find P(over) and Impulse using these values of Y and Y90.

(4) If Do/Dt GTE 0.45

(a) Calculate Yield:

for Delta Pr = 85 psi
Vu = 10%

$$Y = t/(W**1/3)) * (1 + (217/W))*(0.59 - 0.092 * (L/D))$$

eq.5.1.3

Estimated max. allowable t/(W**1/3)) values:

L/D	(t/(W**(1/3))max
1.8	43
5.0	57

To correct for differences from the standard conditions of V_u = 10%, P_r = 85 psi, multiply (t/(W**(1/3)) max values by the k factor given in Figure 5-21.

(b) Go to Section 5.1.3.4 and find P(over) and Impulse using this value of Y.

LO2/RP-1 CBGS

For this section, use the same definitions as for the LOX/LH2 CBGS system.

(1) Fallback with essentially simultaneous tank rupture, and known mixing time.

(a) Compute t/(W**(1/3)), and using propellant impact Velocity (V, ft/sec), find Y (%) from Figure 5.24 and Y90(%) from Figure 5-25.

(b) Go to Section 5.1.3.4 and find P(over) and Impulse using these values of Y.

(2) Fallback with delayed release of the top propellant, and known mixing time;

(a) Calculate Y:

$$Y = Ys*(W(LO2) + W(RP-1)/W$$

Where:

W(LO2) = total weight of LO2
W(RP-1) = weight of RP-1 overlapped
W = total propellant weight
Ys is obtained from:

$LO2/RP_1$ Ratio	Ys(%)
1.5	93
2.0	113
2.5	126
3.0	132
3.5	123
4.0	115
4.5	105
5.0	96
6.0	83
7.0	70
8.0	59
10.0	43
12.0	31
14.0	22
16.0	16
18.0	12

(b) Go to Section 5.1.3.4 and find P(over) and Impulse using this value of Y.

(3) Non-massive tank rupture and mixing time is known.

(a) Use same procedure as A above, only substitute Wf for W, where,

Wf = mass of propellants on ground at time of ignition

(4) For any failure subtype where mixing time is unknown.

(a) Using impact velocity of the fuels, determine Y and Y90 using Figure 5-26.

Note - These are the maximum terminal yield values for any ignition time (worst case)

(b) Go to Section 5.1.3.4 and find P(over) and Impulse using these values of Y and Y90.

LO2/RP-1 High Velocity Impact (HVI)

(1) Determine characteristics of impacted surface. Hard (rock, concrete), or soft (sand, swamp).

(2) Using the anticipated impact velocity (ft/sec), obtain Y and Y90 from Figure 5-27.

(3) Go to Section 5.1.3.4 and determine P(over) and Impulse for these values of Y and Y90.

5.1.3.3 Hypergolic Bi-Propellant Systems - The hypergolic bi-propellant systems in use today are either A-50/N204 or MMH/N204 systems. Because of the similarity of these systems, the same numbers and methods will be used for both. (MMH/N204 will not behave exactly like A-50/N204, but because there is a lack of MMH/N204 specific data, they will be treated the same here.)

Terminal Yields

The terminal yield of a hypergolic bi-propellant explosion is a function of several variables, including failure mode, degree of confinement, total amount of propellant, and impact velocity (where applicable). Listed in Table 5-1 are the terminal yields for a variety of failure modes as recommended by Project PYRO.

Table 5-1 Terminal Yields for Hypergolic Bi-Propellants

Failure Mode	Terminal Yield (Y) Range, %(3)	Estimated Upper Limit (Y90),%
CBM	0.01 - 0.8	1.5
CBGS	0.02 - 0.3	0.5
CBGS, 310-ft drop	1.5	3
Command Destruct	0.3 - 0.35	0.5
Small Explosive Donor (1)	0.8 - 1.2	2
Large Explosive Donor(2)	3.4 - 3.7	5
High Velocity Impact		
Hard Surface	(see Fig. 5-26)	25
Soft Surface	(" " ")	60

(1) A small explosive donor is one weighing less than 0.5% of the propellant weight. (Explosive donors are detonating sources of energy)

(2) The only source of a large explosive donor is another stage of the vehicle and to achieve the listed 5% yield required an explosive donor weighing 2 to 3 times that of the hypergolic receptor. Thus this case is generally of very little interest. For explosive donors between 0.5% and 200% of propellant weight, assume a linear relationship between donor size and terminal yields (linear interpolation between data points).

(3) As a general rule of thumb, some non-PYRO investigators suggest using the lower values of Y for large propellant volumes and the higher values of Y for smaller propellant volumes.

The actual terminal yield produced by hypergolic bi-propellants (like cryogenic bi-propellants) is very dependent on the extent of fuel/oxidizer contact (mixing) prior to the explosion. Because of their hypergolic nature, very little mixing can occur before reaction, thus producing the relatively low terminal yields quoted in Table 5-1. However, if the fuels are confined by some external structure, such as a silo, the terminal yields can be much higher. (The maximum theoretical yield of 170% would never be seen in any realistic situation.) For example, Ref. 25 (1976) presents an analysis of the environment induced by the rupture of an LGM25C (Titan II) missile in a silo and the resulting damage to the silo. The investigators used a PYRO method and a 0.5% maximum terminal yield (Y). The damage levels reported by this report were far lower than those experienced in a silo accident at Damascus, Ak. Although no estimates of terminal yield based on actual damage at Damascus are known to exist, the yield experienced due to confinement has been estimated to be 5-6%. Based on this, the maximum credible terminal yield for an in silo accident is 6%, which is greater than any of the values reported in Table 5-1. Thus, under very specific circumstances, terminal yield for hypergolic propellants can exceed those values listed in Table 5-1.

The terminal yield for a hypergolic bi-propellant high velocity impact accident can be obtained from Figure 5-28, given the impact velocity (ft/sec).

Using these values of Y, go to Section 5.1.3.4 and find P(over) and Impulse.

5.1.3.4 Overpressures and Impulse from Values of Y - Once the terminal yields (Y and Y90) for a propellant type and failure mode are known, the shockwave overpressures and Impulse overpressures can be determined using the following method.

(1) Compute TNT equivalent weight, W(TNT)

W(TNT) = Y * W

Y = Terminal yield or 90% certainty yield (Decimal %)*
W = Total propellant weight, lb

*Note: If no ground surface is present for a particular scenario, divide the yield (Y) by a factor of two before calculating W(TNT)!

(2) Compute scaled distance (Lambda) for the point of interest:

Lambda = D/(W(TNT)**(1/3))
D = distance from the center of blast to point where overpressure data is needed, ft.

(3) For far field distances (D GT 3d; d = tank diameter), using Lambda, determine the overpressure (P(over), psi) of interest from Figure 5-29. Note the blast damage information.

(4) For near field distances (D LTE 3d), find the overpressure as a function of distance from tank wall in diameters and failure mode from Figure 5-30.

(5) Using Lambda, determine the theoretical positive impulse, I(TNT), from Figure 5-29.

(6) Adjust I(TNT) to I(actual) using the following multipliers:

Fuel	Lambda Value	Normalization
LO2/LH2	GTE 5	I = 1.4 * I(TNT)
LO2/LH2	LTE 5	I = 2.0 * I(TNT)
LO2/RP-1	GTE 3	I = 1.3 * I(TNT)
LO2/RP-1	LTE 3	I = 2.0 * I(TNT)

Once the values of P(over) and Impulse have been determined, the blast environment is defined and any damage incurred can be calculated using standard engineering procedures.

5.1.4 Database for Solid Propellant Explosions

The major sources of solid propellant explosion data are:

(1) Project SOPHY
Refs. 26, 27, 28, 29, and 30

(2) Naval Weapons Center/Naval Ordnance Test Station
Refs. 31, 32, 33, and 34

(3) Eastern Space and Missile Center
Ref. 35 and 5

(4) DoD Explosives Safety Board
Refs. 6, 37, 2, 38, 39, and 40

(5) Ballistic Research Laboratory
Ref. 41

Project SOPHY

Project SOPHY was conducted to determine the critical diameter of a class 2 (1.3) composite propellant (PBAN). (Class 2 is the old DOT classification, Class 1.3 is the current DOT classification). Critical diameter is the minimum diameter of a propellant grain that will sustain detonation. In SOPHY I, critical diameters were determined using propellant adulterated with varying amounts of high explosive (RDX) replacing equal weights of ammonium perchlorate (AP). An expression for critical diameter was developed in terms of RDX concentration. Extrapolation to no RDX gave critical diameter for the unadultrated propellant. SOPHY II demonstrated the critical diameter determination. A 72-inch diameter grain detonated, a 60-inch diameter grain didn't. A criticism of this result is that the explosive initiators were too large, far exceeding the energy input of many accident situations. In effect, SOPHY yielded an upper limit because of the size of the stimulus (Ref. 42).

An analytical investigation of initiation mechanisms for solid propellant detonations concluded that relatively low speed impact of flyer plates on composite and double-base propellants can initiate explosions (Ref. 40). The results indicate that small regions of propellant inhomogeneities (soft or low density material or air pockets) heat to high temperature by adiabatic compression. These high temperatures initiate the detonation (or fast deflagration).

Ballistic Research Laboratory

An update of the standard TNT spherical air burst and the hemispherical surface burst is presented (Ref. 41).

5.1.5 Solid-Propellant Blast Determination Methods

Solid propellants differ from the liquid propellants in that the fuel and oxidizer in them are already mixed in an optimum manner. The blast effects of solid propellants are not dependent on mixing effects and are not as dependent on failure mode. Also, the blast characteristics of solid propellants are almost identical to TNT (P(over) profile, Impulse).

There are two basic categories of solid propellants, class 1.1 and class 1.3. Class 1.1 propellants usually consist of a homogeneous mixture of Nitroglycerine and Nitrocellulose. They are also known as "Double Base" propellants. The class 1.1 propellants are considered mass-detonable, and are not currently used on any launch vehicles. Class 1.3 propellants are not classified as mass-detonating, but given the correct input under certain conditions, they can mass detonate. All of the solids currently used on launch vehicles are classified as 1.3 propellants. The chemical make-up of the majority of class 1.3 propellants is Ammonium Perchlorate oxidizer, aluminum fuel, and a low oxygen hydrocarbon binder such as Polybutadiene-acrylic acid-acrylonitrile (PBAN) in varying concentrations. These propellants also have low concentrations of other compounds such as Epoxy, Iron oxide, and other binders and catalysts.

Six parameters have been identified which can determine the likelihood of any solid rocket motor to detonate.

(1) Propellant toughness (structural integrity)

(2) Propellant response to direct shock (SDT)

(3) Propellant response to delayed induced shock (XDT)

(4) Propellant granular bed characteristics (susceptibility) to thermal and mechanical pyrolysis and ignition leading to convective combustion in detonation (DDT)

(5) Motor geometry including diameter, core configuration, L/D ratio, chamber pressure, case bonding technique, and propellant residual strain.

(6) Propellant critical diameter and geometry

XDT, or delayed shock induced detonation, can occur from much lower initial shock energy than that required for SDT. Computer modeling and experimental data show that the XDT threshold is influenced by both propellant grain diameter and length to diameter ratio. Threshold impact velocities can be found using the relationships:

$$VT(inf.) = (4.64 * 10^{**4})/(r^{*}0.276) \quad \text{eq. 5.1.4}$$

$$VT = VT(inf.) * [1 + (0.026/[((L/D) - (L/D)(crit))^{**}1.46)] \quad \text{eq. 5.1.5}$$

Where:

VT(inf.) = Threshold impact velocity (cm/s) for infinite L/D ratios
VT = Threshold impact velocity for finite L/D
r = radius of propellant grain
(L/D)(crit) = critical L/D = 0.5

Also, a model has been developed to predicate impact angle effects:

$$VT(theta) = [(1.634/(20-theta))^{**}1.64] * VT(o) \quad \text{eq. 5.1.6}$$

Where:

theta = angle of impact (from vertical)

VT(o) = Threshold impact velocity for flat surfaces and theta = 0° (perpendicular) to the flat surface.

NOTE: These equations were developed for class 1.1 propellants, but are reasonably accurate for large full scale class 1.3 grains.

Detonations or explosions of grains smaller than their critical diameter via the XDT mechanism tend to be fading reactions, yielding smaller overpressures than grains that exceed their critical diameter. (Critical diameter is discussed next.)

A parameter called critical diameter, d(c), has been identified for class 1.3 propellants. The critical diameter of a propellant is "the minimum diameter . . . of a solid cylindrical grain that will sustain detonation. (Ref 26) If the diameter of a propellant grain is less than its' critical diameter, no SDT input to the propellant can cause a sustained detonation. Project SOPHY (Ref. 26) determined the critical diameter for Ammonium Perchlorate/PBAN solid cylindrical grains to be 75.6 inches.

Since most of the grains in use of launch vehicles are not solid cylinders (or "End Burners"), an adjustment to the critical diameter must be made based on actual grain geometry. See Figures 5-31 and 5-32 for the correlation between grain geometry, d(c) (use 75.6 inches), and bc, tc, or hc (geometry dependent critical dimensions). For geometries not listed in Figures 5-31 and 5-32, another method of calculating critical diameters is available.

$$d(c) = 4*A/P$$

A = Crossectional area of the grain
P = Perimeter of the crossection

Using this method, d(c) GTE 72 is considered supercritical.

Once the actual critical diameter has been determined, it is obvious whether or not the propellant grain of interest is capable of sustaining a SDT detonation. If the propellant of interest is not a AP/Aluminum/PBAN type of propellant, the critical diameter for that propellant must be found using some other method, preferably an empirical method.

SDT, or direct shock induced detonation, is the most straightforward, simplest, and best understood of the detonation scenarios. SDT detonations occur at pressures of 18 to 30 kbar when the propellant grain size is at the critical diameter or critical geometry. Damaged propellant is more sensitive to direct shock induced detonation. Tests indicate that pressures an order of magnitude lower than those required for undamaged propellant will initiate damaged propellant.

SDT is the detonation mechanism tested during NOL card-gap test. As a result, the XDT mechanism is not tested even though it is the most likely detonation mechanism and requires less initiation energy. (NOTE: The information pertaining to XDT, SDT, and DDT detonations of solid rocket motors was extracted from ESMC/SEM Report #84-1, Detonability of Large Solid Rocket Motors, L. Ullian, with references to the Hercules/Thiokol Trident (C-4) Hazards Report, Project SOPHY, and others.)

To determine the blast environment of a detonating solid rocket motor, the motor size, configuration, and failure scenario must be known first.

5.1.5.1 XDT (High Velocity Impact)

(1) Find VT (inf.) using equation 5.1.4.

(2) Find VT using equation 5.1.5.

(3) Find VT (theta) if impact is not perpendicular to the impacted surface using equation 5.1.6.

(4) If the velocity of impact predicted by the failure scenario is greater than or equal to its threshold impact velocity, then detonation will occur.

(5) Go to Figure 5-33 and find TNT % equivalent (% WTNT) using the actual impact velocity predicted by the failure scenario.

(6) Find TNT equivalent weight.

W(TNT) = % W(TNT) * W

W = Total weight of unburned solid propellant at time of impact (lb)

(7) Calculate Scaled Distance (Lambda):

Lambda = D/[W(TNT)**(1/3)] eq. 5.1.7

D = Distance from center of blast to point of interest, ft.

(8) Using Lambda, find the shockwave overpressure (Pover) and specific impulse from figures 5-34 and 5-35 respectively. These values will define the blast environment at distance D from point of impact.

5.1.5.2 Failure other than HVI (SDT/Critical Diam. Method) - (For example: Explosive donor, Grain/Case failure - see NOTE below)

(1) Determine if the grain of interest at the time of accident is greater than or equal to its critical diameter. Use Figure 5-31 or 5-32 for the correlation between geometry and critical diameter. Use d(c) = 75.6 inches.

(2) If grain is GTE critical diameter, continue. If not, the grain will not produce any appreciable blast environment.

(3) Determine TNT equivalent weight W(TNT).

(a) From published empirical data

(b) Theoretically

1. Calculate the energy of reaction (delta HR) for the propellant of interest

delta HR = delta Hfi (Products) - delta Hfi (reactants) (BTU/lb)

delta Hfi = Heat of formation of compound i based on 1 lb of propellant

2. Calculate the % yield (Y)

Y = delta HR/e(TNT) eq. 5.1.8

e(TNT) = 1800 BUT/lb

(Y can theoretically be as high as 1.95 - almost twice the explosive yield per pound as TNT! However, tests have shown that a maximum yield of 175% is the highest that should be used.)

3. Calculate W(TNT)

   W(TNT) = Y * W

4. Calculate scaled distance (Lambda):

   Lambda = D/(W(TNT)**(1/3)) eq. 5.1.7
   D = Distance from center of blast to point of interest, ft.

5. Using Lambda, find the shockwave overpressure (Pover) and Specific Impulse from Figures 5-34 and 5.35 respectively. These values will define the blast environment at Distance D.

*NOTE: The initiation of a command destruct system has never initiated a propellant detonation on a class 1.3 solid rocket motor. Command destruct scenarios will not induce a propellant detonation, but subsequent impact of the solid propellant fragments onto a hard or soft surface may cause them to explode (i.e., Titan 34D-9 mishap. One of the two SRM's were command destructed at low altitude. The motor did not detonate at the time of command destruct, but several of the resulting fragments did explode upon impact.)

5.2 FRAGMENTATION

The fragmentation environmemt to be defined consists of fragment masses, sizes, shapes, trajectories, and their resulting velocities. Fragment sizes, shapes and masses are a function of several parameters including tank/structural materials tank geometry, tank configuration at time of fragmentation (full of liquids, gasses, or two-phase for liquid tanks, for example), total energy release, and the rate of energy release. In general, the larger the energy release and the greater the rate of release, the smaller the fragment.

5.2.1 Solid Rocket Motor Fragmentation

For solid rocket motors, two general types of non-detonating in-flight breakups have been observed. Both a complete breakup of the SRM (e.g., STS-51L and T34D-9) and a "clamshell" opening (e.g. Titan mishap, 1980, 100 sec into flight) have occurred during actual flight aborts. Fragmentation from the Titan T43D-9 was observed as a result of both SRM internal failure and as a result of command destruct action.

For the Titan 34D-9 accident, SRM2 was destroyed by a failure in the motor itself, causing it to explode. SRM1 was subsequently destroyed by the ISDS (inadvertant Separation Destruct System) by using a linear shaped charge to "slice" open the motor case. The fragments observed from SRM2 had a mean surface area of 36.7 sq ft, and the fragments from SRM1 had a mean surface area of 56.3 sq ft. (Surface area is the motor CASE surface area of the fragment, not the entire surface area of the fragment). This implies that the total energy released and/or the rate of energy release was slightly higher for SRM2 than SRM1. See Figures 5-36 thru 5-41 for SRM1 and SRM2 fragment "layouts" (or pattern of fragmentation), fragment size vs frequency, fragment velocity vs impact distance, and fragment velocity vs cumulative percent.

The 1980 Titan mishap was a command destruct at approximately 100 seconds into flight. In this instance the SRM cases were observed to separate into segments and open like clam shells without any evidence of fragmentation. See Figure 5-42 for a series of diagrams depicting the "clamshell" phenomena. One possible explanation as to why the Titan T34D-9 SRM-1 acted so differently is that the motor that fragmented was still largely unburned (approx. 8.7 sec burn time), whereas the 1980 Titan motors were almost burned out (approx. 100 sec burn time). This burn time difference will greatly influence the thickness of the remaining solid propellant, and as a result affect the structural stiffness of the motor. The more flexible motor (less propellant) was able to absorb the energy of command destuct by rapid deflection of the motor case (clam shell). The more rigid motor was unable to absorb this energy rapidly enough by bending, and as a result the energy was dissipated by fragmentation. An analysis has not yet to our knowledge been conducted to determine in what burn-time/thickness range that the failure mode shifts from fragmentation to clamshell.

A fragment velocity and size characterization was also done on the film data from the STS51-L (Challenger) mishap. See Figures 5-43 - 5-44 for graphs of frequency vs observed fragment size and cumulative probability vs fragment velocity for the STS 51-L mishap. A much smaller percentage of fragments were recovered from this accident than the Titan 34D-9 accident because the destruct occurred over the ocean. Also, the film data only tracked fragments over 47 sq. ft. in area. Because of this and the similarity of the STS and Titan SRMs (large, multi-segment, almost identical chemical composition), it is recommended that the data from the Titan mishaps be used to approximate the fragmentation environments in future studies dealing with non-detonating destruction of SRMs.

Other references of interest include the Giant Patriot experiments in 1971 (Refs. 43, 44, 45 and 46) which produced solid propellant fragmentation information for a Minuteman explosion. The debris data was compiled in terms of vehicle location, size, and weight distributions. Impact kinetic energy and incremental velocities were presented as functions of ballistic coefficients.

Collins et al, (Ref. 47) used the Giant Patriot data to obtain an interesting result. They determined a statistical velocity model that would produce the same scatter of fragment impacts on the ground as was observed in the test. In order to obtain a match for fragment impacts, it was necessary to assume all fragments were at the edge of the fireball at the same time and all fragment velocities were equal to gas velocities at the edge of the fireball; then start debris trajectory calculations. It is also interesting to note that few fragments were recovered from the third stage motor that was a class 1.1(7) propellant.

For solid propellant motors that explode on impact with the ground surface (HVI), the fragmentation environments would be best described using the Gurney method discussed in Section 5.2.3 of this manual. This is not a very accurate representation of this environment, however no other method specific to this situation is known of at this time.

5.2.2 Liquid Propellant Tank Fragmentation

As mentioned earlier, several factors influence the fragmentation environment of an exploding liquid propellant tank. Geometry, failure scenario, external pressure, type of propellant, tank structure, total energy release, and rate of energy release all affect the fragmentation environment. For bi-propellant systems (LO2/LH2 and the hypergolics) two tanks must be ruptured almost simultaneously to initiate a tank fragment environment. Because these bi-propellants only react (explode) in their zones of mixing, the tankage close to the mixed propellants sees a relatively high energy release, whereas the tankage further from the mixing zone(s) sees far less energy release. This situation yields relatively small high velocity fragments from the areas around the mixing zone, and much larger lower velocity fragments from the rest of the tank(s).

Two general methods have been developed to predict fragment velocities/sizes for exploding liquid propellant tanks. Baker, et al (Ref. 48) determined fragment average initial velocity and average fragment range could be determined by the correlations

```
V(t=0) = 73.96*Y**0.43 m/sec (initial velocity) eq. 5.2.1
     R = 95.93*Y**0.28 meters (range)
     Y = W(TNT)/W(total) (explosive yield)
```

These correlations were based on the data from project PYRO and seem to be valid for the various configurations studied by that project.

Anderson, et al (Ref. 49) developed models of fragment size and velocity distributions for analyzing STS accident scenarios. They made liberal use of Baker's (Ref. 48) results, but re-interpreted initial velocity data to obtain velocity in terms of scaled distance.

```
   V(50) = 139 * (Lambda**-1.46) eq. 5.2.2
   V(50) = median speed
Lambda   = scaled distance
Lambda   = D/(W(TNT)**(1/3)) eq. 5.1.7
```

Figures 5-45 and 5-46 present actual data from several aborts and a PYRO test in relation to total weight of fragments vs range of fragments and total number of fragments vs range of fragments. As always, use empirical data before theoretical methods whenever applicable.

5.2.3 Pressurized Tanks and General Applications

To predict initial fragment velocities as a function of geometry, masses, and energy per unit mass, Gurney developed correlations which are presented in Figure 5-47. Solutions to these equations over a fairly wide range are presented in Figure 5-48.

Given the initial velocity, the terminal, or striking velocity of a fragment can be determined using the equation:

$$V = V(t=0) * (e^{**}(-kx)) \quad \text{eq. 5.2.3}$$

Where:
- V = velocity of the fragment
- V(t=0) = initial fragment velocity
- x = distance traveled by the fragment
- k = (Af * Rho * Cd)/(2 * m)
- Rho = density of the atmosphere
- Af = crossectional area (frontal area) of the fragment
- Cd = aerodynamic drag coefficient
- m = mass of fragment
- e = Inverse Natural Log of 1 = 2.72

This equation ignores the affects of gravity, which would change the terminal velocity of the fragment falling to earth to a value other than that predicted using this equation. Also, some burning solid propellant fragments may tend to "rocket", or self-propel themselves, increasing their velocities.

In 1972, the Naval ordnance laboratory conducted a series of tests on bursting pressurized tanks (Ref. 50). Fragmentation data was gathered from these tests and is presented in Tables 5-2 - 5-4. Table 5-2 presents the vessel configurations tested, Table 5-3 presents fragment distributions, and Table 5-4 presents fragment velocity data. This data can be used to determine the approximate fragment environment for similar pressurized tanks at similar burst pressures.

Table 5-2 Vessel Configurations for NOL Fragmentation Tests
(Ref. 50, NOL TR72-102)

Tank Letter Designator	Vessel Type (3)	Vessel Shape	Dimensions	Pressure Data Operate	Burst (Design)	Burst(2) (Actual)
A	Aerozine 50 Fuel Tank	Cylinder with Hemi-spherical ends	Length = 24 in. Diameter = 13 in. Volume = 1.34 cu ft Weight = 8.5 lbs	188 psig	460 psig	625 psig
B	Oxidizer Tank	Same as Tank A	Length = 29 in. Diameter = 13 in. Volume = 1.68 cu ft Weight = 10.2 lbs	138 psig	460 psig	600 psig
C	Helium Tank	Sphere	Diameter = 9.2 in. Volume = 0.235cu ft Weight = 6.3 lbs	4,150 psig	7,500 psig	8,000 psig
D	Helium Pressure Vessel	Sphere	Diameter = 27 in. Volume = 6 cu ft Weight = 171 lbs	3,250 psig	8,000 psig	8,000 psig
E (1)	Helium Pressure Vessel	Sphere	Diameter = 27 in. Volume = 6 cu ft Weight = 170 lbs	3,250 psig	8,000 psig	8,130 psig

(1) This vessel was pressure cycled prior to rupture

(2) All tanks were pressured with GN_2

(3) All tanks were made of titanium, 6 Aluminum, 5 Vanadium alloy

Table 5-3 Fragment Distribution of Bursting Gas Tanks
(Ref. 50, NOL TR72-102)

Tank	Number of Frag. Rcv'd	% of Tank Wt. Recovered	Fragment Size Range	% of Skin Recovered	Fragment Weight Range	Avg	Sigma Sq
A	36	73%	10"X12" to 1"X2"	56%	1248-1.9gm	78.8	206
B	36	71%	16"X17" to 2"X1/2"	61%	1503-0.3gm	91.6	252
C	8	21%	4"X6" to 1"X2"	N/A	300-12.6gm	77.4	104
D	21	45.5%	16"X12" to 2"X2"	N/A	7321-57 gm	1644	1632
E	25	51.6%	16"X15" to 2"X2"	N/A	8143-38 gm	1588	1704

Table 5-4 Fragmentation Velocity Data for Bursting Gas Tanks
(Ref. 50, NOL TR72-102)

Tank	Fragment Size	Fragment Velocity over Time Interval 0-1.5ms	1.5-3ms	3-5ms	0-5ms
A	8" X 8", 1248 gm	1010 ft/s	1040 ft/s	750 ft/s	918 ft/s
A	11" X 11", 177 gm	1040 ft/s	1070 ft/s	930 ft/s	1000 ft/s
A	10" X 10", 149 gm	(0-3ms): 1030 ft/s		865 ft/s	967 ft/s
		0-3ms	3-4.5ms		0-4.5ms
B	8" X 8", 1503 gm	920 ft/s	860 ft/s		900 ft/s
B	17" X 16", 397 gm	986 ft/s	880 ft/s		950 ft/s
C	3" X 3", 300 gm	1200 ft/s	1020 ft/s		1150 ft/s

5.3 THERMAL (FIRE)

In the event of a catastrophic accident involving propellants, one of the more damaging environments produced is the fireball. Because of the extreme temperatures and large amounts of radiated energy, the destructive ability of a propellant fireball can be quite high in or near the fireball. In order to determine the thermal effects of a fireball, certain fireball characteristics must be known. The characteristics that will be addressed in this section include fireball size and duration, liftoff time, adiabatic flame temperatures, average fireball temperature, and radiation from the fireball.

5.3.1 Fireball Development Time-History

When an unconfined propellant fire is initiated, a specific series of events occur in its formation and growth. Initially the fireball grows in the shape of a hemisphere bounded by the Earth's surface. (If the fireball occurs above ground surface, but in the atmosphere, the fireball will assume a spherical shape from the start). The bulk of the propellants burn rapidly in all catastrophic accidents on or near its ground surface. Typically liquid explosions involve detonation or rapid deflagration in the early stages of fireball development. Such high rate reactions produce shock waves at the outer boundaries of the fireball, and low pressures behind the shock wave in the center of the fireball. These phenomena regulate the initial lateral growth pattern, infusion of air, and overall fireball upward motion. Once the initial phase of growth is complete (the shock wave has dissipated and the pressure gradient across the fireball has equalized) the fireball dynamics are controlled by bouyant forces that are a result of the high temperatures and low densities created in the first stage of development. Because of this lower density the fireball gases rise. When the upward velocity of the fireball gases exceed its growth the fireball begins to change in shape from a hemisphere to a sphere truncated on the bottom by the ground. Finally "liftoff" occurs when the height of its center exceeds its radius. As the fireball continues to rise, it creates a vortex motion which, along with natural convective forces, causes the surrounding ambient air and the propellant on the ground to be drawn into the fireball from below, forming a stem. The fireball continues to grow as it rises due to air entrainment and residual combustion. When all combustion is completed, the fireball begins to cool rapidly due to continued air entrainment and radiation from the surface of the fireball. During this same period, the induced vortex changes the shape of the fireball to an oblate spheroid and then to a toroid. (Ref. 51) Eventually the cloud cools sufficiently to eliminate any buoyant forces and the fireball attains some maximum height. See Figures 5-49 and 5-50 for diagrams depicting the growth time-history of a fireball.

5.3.2 Liquid Fireball Size and Duration

5.3.2.1 Fireball size: The size of a fireball is a necessary piece of information needed to determine the extent (size) of the thermal environment. This information can be used to determine whether or not a particular location is engulfed by the fireball.

For liquid propellants, the general equation for maximum fireball diameter is:

D(ft) = 9.56*(Wb**0.325) eq. 5.3.1 (Ref 9)

where Wb = total propellant weight, lb.

Specific correlations for LH2/LO2 and N2O4/A-50 have been developed. They are:

D = 11.05 * (Wb)**0.306 for LH2/LO2 eq. 5.3.2 (Ref. 52)
D = 8.86 * (Wb)**0.328 for N2O4/A-50 eq. 5.3.3 (Ref. 52)

For liquids other than LO2/LH2 or N2O4 equation 5.3.1 should be used.

Fireball diameter as a function of time can be determined using the following equations. During the time when propellants are reacting the equation to use is:

D(ft) = [(3Rt/4*pi*Rho)]**0.333 eq. 5.3.4 (Ref 53)

where: R = rate of propellant consumption = 5 * (Wb**(516/3))
t = time from propellant spill, dimensionless
Rho = average gas density in fireball, lb/cu. ft.
pi = 3.14159

The equation to use for fireball diameter as a function of time when reaction has terminated and the fireball has lifted off is:

D(ft) = [3*Wb)/(4*pi*Rho)]**(1/3)*(t)**(1/3) eq. 5.3.5 (Ref.53)

The radius of a liquid propellant fireball at liftoff can be found using:

DL(ft) = 3.51 * (Wb)**1/3 eq. 5.3.6 (Ref 54)

Equations 5.3.4, 5.3.5, and 5.3.6 are generalized equations that can be used for all liquid propellants with a fairly good degree of accuracy. Very little dependence on propellant type or explosive yield have been observed.

It should be noted that these fireball diameters are the average diameters, not necessarily the maximum diameters. Fireballs can be non-symmetrical due to many factors including propellant source configuration and prevailing atmospheric conditions.

5.3.2.2 Fireball duration (Tau): The duration of a fireball is considered to be the length of time that heating occurs within the fireball. This information is needed in order to evaluate the thermal environment in and around the propellant spill/accident. For liquids, a good generalized equation for fireball duration is:

Tau = 0.196 * (Wb)**0.349 eq. 5.3.7 (Refs. 9,52)

No correlation is currently available to predict fireball duration for solid propellants. This is most likely due to the wide variety of possible solid propellant accident types. These accidents could yield a variety of burn rates and degree of fragmentation of the propellant (available surface area for burning).

Another factor to consider is fireball liftoff time, Tau(0). Fireball liftoff time is the length of time between propellant ignition and fireball liftoff from the ground. This data is useful for determining the duration of heating that ground structures may be exposed to. To obtain the fireball liftoff time for a liquid propellant, use equation 5.3.8.

Tau(0)(sec) = 0.572 * (Wb)**(1/6) eq. 5.3.8 (Ref. 54)

If the total mass of propellant involved in an accident is not greater than some critical value Mc, liftoff will not occur. Critical fireball mass (Mc) has been determined to be approximately 200 lb.

In order to determine the enthalpy of a fireball as a function of time, the rate of propellant addition to the fireball is needed. For liquid propellants, the rate of propellant addition can be determined using:

R = (5/3) * [(Wb)**(5/6)] eq. 5.3.9 (Ref. 53)

where R = rate of propellant addition, lb/sec
Wb = total propellant mass, lb

5.3.3 Solid Propellant Fireball Size and Duration

Two generalized equations for a solid propellant fireball diameter have been developed. The maximum height and width of a solid propellant fireball can be determined using:

D (width, ft) = 12.4 * (W)**(1/3) eq. 5.3.10
D (height, ft) = 6.8 * (W)**(1/3) eq. 5.3.11

where W = total mass of solid propellant burned, lb.

These two equations can be used to obtain "ballpark" figures for most solid propellants. However, due to the large number of variables involved with a solid propellant burn (propellant burn rate, burning fragment size, etc.) the results generated by equations 5.3.10 and 5.3.11 should only be used as general estimates. There is no available information on fireball diameter as a function of time for solid propellants. Equations 5.3.4 and 5.3.5 could be used to generate very generalized approximations for solid propellants.

No information on fireball liftoff time, critical fireball size, or rate of propellant addition is available for solid propellants.

Table 5-5 Adiabatic Flame Temperatures of Propellants

Propellant Accident Type	Reaction Products	Maximum Flame Temp. (Deg. K)	(Deg. F)	Notes
MMH/N2O4	N2O, N2, CO	3,724	6,198	Hypergolic
MMH Fire	H2O, N2, CO	2,130	3,330	Burn with O_2
N2H4 Mono Fire	N2, H2O	2,407	3,828	Burn all H_2 to H_2O using O_2 (air)
N2H4 Mono Decomp	N2, N2	840.1	1,008	Leave all H_2 Unburned
N2H4 Mono Decomp	H2, NH3, N2	1,791.1	2,720	Leave all H_2 unburned, ammonia in products
A-50/N2O4	See Table 5.4.16	3,070	5,066	Hypergolic
LO2/RP-1		3,080	5,084	
LO2/LH2	H2O	3,720	6,236	
LH2 Fire in Air	H2O	2,900	4,760	

5.3.4 Fireball Thermal Effects - Knowing what the thermal environment in and around a fireball is, is necessary to determine what possible damage may be caused by the fireball. This information is also useful in designing safe launch facilities. The critical thermodynamic properties are adiabatic flame temperature, heat flux from the fireball, duration of heating, and average fireball temperature.

5.3.4.1 Adiabatic flame temperature: The adiabatic flame temperature is the maximum theoretical temperature obtainable by a particular combination of chemicals. The methods used to calculate this characteristic are very well defined and are based on theoretical chemistry. A good generalized equation that can be used for any propellant or propellant combination (solids or liquids) is:

delta Hf(R)-delta Hf(P) = [Sum from i=1 to i=m](n(i)*A(i)*T+n(i)*B(i)*(1/2)T**2 + n(i)*C(i)*(1/3)*T**3) -[Sum from i=1 to i=m] n(xi)*delta H(vi)

eq. 5.3.12 (Ref 55)

where:

delta Hf(R) = heat of formation of reactants, total*
delta Hf(P) = heat of formation of products, total*
n(i) = gram-moles of component i**
A(i),B(i),C(i) = heat capacity constants for component i*
T = temperature, °C
n(xi) = gram-moles of excess reactant (fuel) i**
delta H(vi) = heat of vaporization of excess fuel i*
m = number of compounds involved.

* These constants can be found in the CRC Handbook of Chemistry and Physics or equivalent.

** The stoichiometry and total reactant moles must be known before calculation.

Solving equation 5.3.12 for T yields the adiabatic flame temperature. Equation 5.3.12 can also be used to calculate average fireball temperatures by including the molar volume of entrained air in the right side of the equation. Also, the delta H(vi) term is to be used in the case where some of the propellant is unable to burn and some of the heat in the fireball is used to vaporize this excess. See Table 5-5 for a listing of adiabatic flame temperatures for some of the propellants. The easiest method for solving eq. 5.3.12 is to set the equation equal to zero (move the delta Hf term to the right side of equation) and use a computer program to solve this third order polynomial for T.

5.3.4.2 Heat flux from a fireball: Heat flux from a fireball is a function of fireball temperature and emissivity. Once heat flux, fireball size, and fireball duration are known, the degree of heating of structures in and around the fireball can be calculated.

Two methods for predicting heat flux have been used, theoretical and empirical. A theoretical approach that has worked well uses the following equations:

for t(pri) LTE 1 (liftoff occurs at t(pri) = 1):

```
[dT/dt(pri)] = [h(i) - h(fb) - ((4*Pi*E*Sigma)/(1.67*(Wb)**1/6))
               *(((3*t(pri)*R)/(4*Pi*P*MW))**(2/3))*(T**(14/3))]
               /(t(pri)*Cp)                    eq. 5.3.13
```

where:
- h(i) = total Enthalpy (H) of the reactants
- h(fb) = total Enthalpy (H) of the products
- E = emmissivity, assume worst case E = 1
- Sigma = Boltzmanns Constant
- Wb = total weight of propellant(s)
- t(pri) = t/tb = nondimensional time
- R = international gas constant
- P = ambient atmospheric pressure
- MW = average molecular weight of gaseous products
- Cp = specific heat of products
- T = absolute Temperature
- Pi = 3.14159

for t(pri) GT 1:

```
[dT/dt(pri)] = ((-4*Pi*E*Sigma)/(1.67*(Wb)**(1/6)*Cp))
               *[((3*R)/(4*Pi*P*MW))** (2/3)]*T**(14/3)
                                               eq. 5.3.14
```

Both equation 5.3.13 and 5.3.14 can be solved for T (t(pri)) by integrating numerically using a fourth order Runge-kutta method. The initial temperature T (t(pri)) = T(0) to be used for eq. 5.3.13 is the adiabatic flame temperature. The initial condition for eq. 5.3.14 should be the solution of eq. 5.3.13 at t(pri) = 1.

These equations yield the fireball temperature at time t. Once the fireball temperature is known, heat flux from the fireball can be calculated using:

```
Rh(i) = Epsilon * Sigma * A *T**4                eq 5.3.15
```

where:
- Rh(i) = radiation from fireball
- Epsilon = emmissivity, assume Epsilon = 1 for worst-case
- A = surface area of fireball = 4 * Pi * r**3
- T = temperature of fireball from eq. 5.3.13 or 5.3.14
- Sigma = Boltzmanns Constant

NOTE: Radius of fireball - use equation 5.3.4 or 5.3.5 for time = t(pri) (same t(pri) as used in 5.3.13 and 5.3.14).

If heat flux per unit area is needed, use 1 meter squared for A rather than total surface area of fireball.

This series of equations should work quite well for liquid propellants, and will also give good approximations for solid propellants.

Empirical methods to determine heat flux have been used to develop heat flux equations or maximum values for several of the propellants. Unfortunately, very little work has been done to determine heat flux values for solid propellants.

The empirical correlations and maximums that have been developed are:

Sigma = C*(Wb)**1/3 eq. 5.3.16 (Ref. (9)

where: Sigma = heat flux
C = 0.113 for LO2/RP-1
C = 0.077 for LO2/LH2

Table 5-6 Some Maximum Observed Heat Fluxes from Fireballs

Sigma (max) = 400 Btu/sq ft-sec	N2O4/A-50	(Ref. 53)
Sigma (max) = 200 Btu/sq ft-sec	LO2/RP-1	(Ref. 56)
Sigma (max) = 285 Watts/sq cm	LO2/LH2	(Ref. 57)
Sigma (max) = 12.7 Btu/sq ft-sec	LH2 Fire	(Ref. 20)

See Figure 5-51 for a graph of heat flux vs dimensionless time for LO2/LH2. (Note that the "recommended" curve drops to zero at liftoff). This is "recommended" because at liftoff the fireball begins to rise rather rapidly, moving the heat source away from any ground structures. The heat flux from the fireball is still greater than zero, but after liftoff that flux is rendered virtually harmless to ground structure due to the distances involved. See Figure 5-52 for a graph of heat flux and temperature vs dimensionless time for a LO2/LH2 fireball. Also, see Figure 5-53 for a graph of fireball temperature vs time based on actual data from a Saturn V abort. (LO2/RP-1) Note that the actual initial fireball temperature very closely resembles the adiabatic flame temperature for LO2/RP-1 (3080 K).

To obtain the heat flux at any arbitrary location or distance from the fireball, a radiation heat transfer analysis using view factors can be used based on the heat flux at the surface of the fireball and the size of the fireball.

5.3.5 Roadmap

This section presents the series of steps to be taken to evaluate the critical parameters of a solid or liquid propellant fireball.

(1) Determine type(s) and amount(s) of propellants based on vehicle involved and potential failure scenario.

(2) Calculate fireball maximum diameter. For liquid propellants, use equation 5.3.1, 5.3.2, or 5.3.3 as applicable (see text). For solid propellants use equations 5.3.10 and 5.3.11.

(3) For liquid propellants solve equation 5.3.4 for fireball diameter as a function of time at several times. Plot diameter vs time if needed. (May be needed at a later time). Fireball density (Rho) will have to be estimated using the ideal gas law or equivalent correlation. The temperature needed for the ideal gas law can be found using equation 5.3.12 or Table 5-5.

(4) If total propellant weight is less than 200 lb, liftoff will not occur - skip step #5.

(5) Calculate fireball liftoff time Tau(0) using equation 5.3.8. Also, calculate the fireball duration using equation 5.3.7. These equations are only applicable for liquid propellants.

(6) Find the rate of propellant addition to the fireball using equation 5.3.9 (also only applicable to liquid propellants).

(7) Calculate the fireball temperature using equation 5.3.12 (if it hasn't already been computed in Step #3), or if worst case results are desired, the adiabatic flame temperature for the propellant in question may be listed in Table 5-5. If not, equation 5.3.12 will have to be used (either solids or liquids).

(8) Calculate the heat flux from the fireball at several times using equations 5.3.13, 5.3.14, and 5.3.15, or use the heat flux values given by equation 5.3.16, Table 5-6, or Figures 5-51 or 5-52. Plot time vs heat flux if enough data is available or calculated.

(9) Using the information generated in steps 2, 3, 5, 7 and 8, calculate the heat transfer to any location of interest using standard engineering thermodynamic techniques.

Example Problem: Space Shuttle External Tank - Catastrophic Failure following the "Road Map":

(1) A fully fueled shuttle external tank contains 1,378,600 lb of liquid oxygen and 230,700 lb of liquid hydrogen for a total propellant weight of 1,609,300 lb.

(2) Calculate fireball maximum diameter. For LO2/LH2, use equation 5.3.2.

D(max) = 11.05 (1,609,300)**0.306 = 876 ft

(3) Calculate fireball liftoff time using equation 5.3.8 and fireball duration using equation 5.3.7.

Tau(0) = 0.572 * (Wb)**1/6 = 0.572 * (1609300)**1/6

Tau(0) = 6.19 seconds

Tau(duration) = 0.196*(Wb)**0.349 = 0.196*(1,609,300)**0.349

Tau(duration) = 28.73 seconds

(4) Generate a fireball temperature vs time graph using equation 5.3.13 and 5.3.14, or use empirical time-temperature data where available. See Figure 5-54 for a graph of time vs temperature based on the graph (data) presented in Figure 5-53.

(5) Solve equation 5.3.4 for fireball diameter as a function of time for several times.

D = ((3*R*t)/(4*Pi*Rho))**1/3
R = (5*(Wb)**(5/6))/3
  = MP/(10.2*Z*T(t))

where: M = average molecular weight of products = 18
P = pressure (atmospheric, absolute) = 14.7
Z = compressibility = 0.95 (good estimate)
T(t) = fireball temperature (a function of time)
t = time, sec.

For this example, an average fireball temperature will be used (2840°R = (5220 + 560)/2). A more accurate method would be to solve equations 5.3.13 and 5.3.14 for temperature as a function of time and use this temperature in the diameter calculations.

Substituting and Reducing:

D = (18 * 14.7/[10.2 * 0.95 * T(t)]) = 27.3/T(t) lb/cu ft

D = ((3[5*(Wb)**(5/6))/(4*Pi*27*3*T(t)))**(1/3)

D = ((5*(Wb)**(5/6)*t*T(t))/343)**(1/3)

For 1,609,300 lb propellants,

D = (5[1,609,300]**5/6*t*T(t))/343)**(1/3)=(2167*T(t)*t)**(1/3)

Solving for t = 0 to 145 seconds yields the graph presented in Figure 5-55.

(6) Total propellant weight is greater than 200 lb. Perform step 5.

(7) Find rate of propellant addition to the fireball using equation 5.3.11.

R = (5/3)*(Wb)**(5/6)

R = 247,769 lb/sec

(8) Calculate the maximum fireball temperature using equation 5.3.12, or if worst case results are desired, adiabatic flame temperature may be listed in Table 5-5.

From Table 5-5,

T (adiabatic) = 3,720K

(9) Determine heat flux from the fireball.

From Table 5-6, Sigma (max) = 285 watts/cm^2. Also see Figure 5-52 for a graph of Sigma vs dimensionless time.

NOTE: Use existing empirical data whenever possible - more reliable than theoretical in many instances.

5.4 TOXICITY

The environment around a propellant spill or burn has the potential to contain large quantities of potentially hazardous chemicals. The potential hazards include asphyxiants, poisons, carcinogens/teratogens/mutagens, and acidic or caustic conditions. There are three major areas of concern involving the toxicity of propellants and their reaction products. These are:

(1) What chemicals are produced by a specific reaction of propellants and at what concentrations are they hazardous?

(2) How long do these chemicals persist in the atmosphere (decomposition, reaction with other chemicals in the atmosphere, dispersion)?

(3) What effect do atmospheric conditions have on the dispersal of these chemicals?

5.4.1 Chemical Compounds Released

The types and quantities of chemicals that are released into the atmosphere after a propellant spill or fire are very propellant-specific and include both reaction products and un-reacted propellant. See Tables 5-7 through 5-27 for listings of reaction products, hazards posed, and ACHIH limits for the propellant combinations of interest to this manual. Due to the huge variety of possible propellant accident scenarios, only the most likely will be covered in this manual.

5.4.2 Lifetime/Fate of Released Chemicals

Several of the chemicals released by propellant accidents will either decompose or react with other chemicals in the atmosphere. The chemicals most likely to undergo reaction in the atmosphere are the hydrazine-type fuels and nitrogen tetroxide/nitrogen dioxide.

Reaction times for hydrazine fuels with oxygen in the atmosphere are so long that by the time any appreciable amount of fuel reacted, normal atmospheric diffusion/dispersion will have reduced the concentrations to unmeasurable levels. For example, the reaction of hydrazine with oxygen

$N_2O_4 + O_2$ reacting to $N_2 + H_2O + NH_3 + N_2H_3$

has a half-life of 10.8 hours in dry air. (Ref. 58)

N_2O_4/NO_2 in the atmosphere will react rapidly with water vapor to form nitric acid and NOx.

$3NO_2 + H_2O$ reacts to $2HNO_3 + NO$

The humidity of the ambient air has a strong effect on the rate and extent of N_2O_4/H_2O reaction in air. For very large N_2O_4 releases, the percentage of the cloud converted to HNO_3 will be relatively small due to the low concentration of water in the atmosphere at any given time with the

possible exception of rain storms or heavy fogs. The nitric acid mists created by this reaction pose a hazard to humans, animals, vegatation, and equipment due to the highly corrosive nature of the chemical.

5.4.3 Atmospheric Dispersion

The atmospheric dispersion of propellants and their reaction products is important information needed to determine evacuation corridors. Because of the complex nature of atmospheric dispersion, the only practical way to model it is with the use of a computer. Several dispersion models have been developed, but most are for very specific sources and configurations. One such model is HARM (Hypergol Accidental Release Model). HARM is designed to evaluate the atmospheric dispersion pattern of the chemicals released during a catastrophic failure of a Titan II ICBM. This model tracks the concentrations of UDMH, N2H4, N2O4, and their reaction products including FDH and NDMA. A fairly sophisticated program, it is available to Air Force personnel by contacting Air Force Headquarters, Ogden, Utah, Capt. J. Hoard. (The program was originally written to run on a Univac 1108, but has also been converted to run on a DEC/HCRS system.)

Another, more versatile, dispersion program that is available is CHARM (Complex Hazardous Air Release Model). CHARM is a Gaussian Puff Integration model that will work for both gaseous and liquid releases. CHARM was written to run on an IBM PC or IBM PC work alike ("clone"). CHARM is a proprietary product of the Radian Corporation. A modified version of CHARM for Air Force use may be available at AFESC/RDV, Tyndall AFB, Florida.

5.4.4 Roadmap

(1) Determine quantity and type of propellant involved for a specific scenario.

(2) Using the appropriate Table (5-7 - 5-27), find the reaction products, percent concentrations, and the hazards associated with them. If the propellant/propellant combination/failure scenario of interest is not covered in the tables, a separate literature search will need to be conducted to determine reaction products, etc.

(3) Calculate the absolute molar quantities of each reaction product by multiplying the total moles of propellants by the conversion factor in the appropriate table (5-7 - 5-27) and then multiplying by the decimal mole percentage obtained from the same table. (The conversion factor is simply the volumetric molar composition change due to reaction.)

(4) Estimate degree of air entrainment into the fireball cloud for a given time after propellant burn.

(5) Using the ideal gas law or equivalent, find the total molar volume of the vapor cloud. Once this is known, the concentration of a given reaction product can be found by dividing the moles of reaction product by the total moles of vapor in the cloud. (Include moles of air entrained.)

(6) Repeat steps 4 and 5 for as many "times" (dimensionless time, t/t(o)) as needed for the analysis. When the molar concentration of a given chemical drops below the ACHIH values given in Tables 5-7 - 5-27, that particular chemical is no longer a health concern.

Table 5-7 Chemical Toxicities

Propellant(s): Nitrogen — Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Nitrogen (N_2)	100%	Asphyxiant (3)	None	None

Table 5-8 Chemical Toxicities

Propellant(s): Helium — Conversion Factor = 1

Reaction Product	% in Products (1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Helium (He)	100%	Asphyxiant (3)	None	None

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.

Table 5-9 Chemical Toxicities

Propellant(s): Liquid Hydrogen — Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Hydrogen (H_2)	100%	Asphyxiant (3), Cryogen	None	None
Burn in Air (4)			Conversion Factor = 1	
Water (H_2O)	35%	None	None	None
Nitrogen (N_2)	65%	Asphyxiant (3)	None	None

Table 5-10 Chemical Toxicities

Propellant(s): Liquid Oxygen/Liquid Hydrogen — Conversion Factor = 2/3

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Water (H_2O)	100%	None	None	None

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.
(4) Ideal burning in air.

Table 5-11 Chemical Toxicities

Propellant(s): Liquid Fluorine (F2) — Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Fluorine (F2)	100%	Caustic irritant, Asphyxiant (3)	2ppm	1ppm

Table 5-12 Chemical Toxicities

Propellant(s): Liquid Methane — Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Methane (CH_4)	100%	Asphyxiant (3)	None	None
Burn in Air (4)			Conversion Factor = 1	
Carbon Dioxide (CO2)	9.5%	Poison	30,000ppm	5,000 ppm
Water (H20)	19%	None	None	None
Nitrogen (N2)	71.5%	Asphyxiant (3)	None	None

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.
(4) Ideal burning in air. Several other compounds will most likely be formed in trace amounts under conditions (NO_x, CO, etc.).

Table 5-13 Chemical Toxicities

Propellant(s): Carbon Dioxide (CO_2) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Carbon Dioxide	100%	Asphyxiant (3), poison	30,000ppm	5,000 ppm

Table 5-14 Chemical Toxicities

Propellant(s): Carbon Monoxide (CO) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Carbon Monoxide (CO)	100%	Asphyxiant (3), poison	400ppm	50ppm

Table 5-15 Chemical Toxicities

Propellant(s): Ammonia (NH3) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Ammonia (NH_3)	100%	Poison	35ppm	25ppm

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.

Table 5-16 Chemical Toxicities

Propellant(s): Hydrogen Peroxide (H2O2)) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Hydrogen Peroxide (H2O2)	100%	Strong oxidizer, irritant, can cause burns on skin	2.0 ppm	1.0ppm
Or:			Conversion Factor = 1.5	
Water (H2O)	66%	None	None	None
Oxygen (O2)	33%	None	None	None

Table 5-17 Chemical Toxicities

Propellant(s): Mercury (Hg) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Mercury (Hg)	100%	Poison (accumulative)	0.05 mg/m^3	None allowed

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists

Table 5-18 Chemical Toxicities

Propellant(s): Nitrogen Trifluoride (NF3) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Nitrogen Trifluoride (NF3)	100%	Moderate poison, Asphyxiant (3)	15 ppm	10 ppm

Table 5-19 Chemical Toxicities

Propellant(s): Nitrogen Tetroxide (N204) Conversion Factor = 1 to 2

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Nitrogen Tetroxide (N204) (5)	(4)	Forms nitric acid when contacted with water (eyes, lungs skin, etc.). Highly corrosive, asphyxiant.	5 ppm	3 ppm
Nitrogen Dioxide (NO2)	(4)		5 ppm	3 ppm

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.
(4) Equilibrium between N204 and NO_2 is temperature and concentration dependent.
(5) Decomposes rapidly to NO_2 in lower concentrations.

Table 5-20 Chemical Toxicities

Propellant(s): Monomethyl Hydrazine (MMH) Conversion Factor = 1

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
MMH	100%	Poison, Tetratogen, Carcinogen	0.2ppm ceiling	None allowed
Burn in Air:(4)			Conversion Factor = 1.43	
Water (H20)	20.8%	None	None	None
Carbon Dioxide (CO2)	6.9%	Asphyxiant (3) Poison	30,000ppm	5,000ppm
Nitrogen (N2)	72.2%	Asphyxiant (3)	None	None

Table 5-21 Chemical Toxicities

Propellant(s): Aerozine 50 (N2H4/UDMH)) Conversion Factor = 1

Reaction Product	% in Products (1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Hydrazine	50%	Poison, Carcinogen	0.1 ppm	None Allowed
UDMH	50%	Poison, Carcinogen	1 ppm	0.5 ppm
Burn in Air:(4)			Conversion Factor = 1.4	
Nitrogen (N2)	83.2%	Asphyxiant (3)	None	None
Water (H20)	12.6%	None	None	None
Carbon Dioxide (CO2)	4.2%	Asphyxiant (3)	30,000ppm	5,000ppm

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.
(4) Ideal burning in air. Several other compounds may be formed during nonideal (actual) conditions in trace amounts.

Table 5-22 Chemical Toxicities

Propellant(s): Hydrazine (N_2H_4) Conversion Factor = 2.333

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Mono-Decomposition:				
Nitrogen (N_2)	28%	Asphyxiant (3)	None	None
Ammonia (NH_3)	28%	Asphyxiant (3), Base W/Water	35 ppm	25 ppm
Hydrogen (H_2)	44%	Asphyxiant (3)	None	None
Hydrazine (N_2H_4)	Trace	Poison, Carcinogen	0.1 ppm	None Allowed
Burn in Air: (4)				
Nitrogen (N_2)	33%	Asphyxiant (3)	None	None
Water (H_2O)	66%	None	None	None
Hydrazine (N_2H_4)	Trace	Poison, Carcinogen	0.1 ppm	None Allowed

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.
(4) Ideal burning in air.

Table 5-23 Chemical Toxicities

Propellant(s): A-50/N204) Conversion Factor = 1.75

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Carbon Monoxide (CO)	0.061	Poison	400 ppm	50 ppm
Carbon Dioxide (CO2)	0.050	Asphyxiant**, Poison	30,000 ppm	5,000 ppm
Hydrogen Radical (H)	0.028	---	None listed	None listed
Hydrogen (H2)	0.057	Asphyxiant**	None listed	None listed
Water (H2O)	0.332	None	None listed	None listed
Nitric Oxide (NO)	0.012	Acidic	5 ppm	3 ppm
Nitrogen (N2)	0.316	Asphyxiant**	None	None
Hydroxide (OH)	0.052		None listed	None listed
Oxygen (O2)	0.094	None	None	None
Ammonia (NH3)	Trace	Powerful irritant	35 ppm	25 ppm
Nitric Acid (HNO3)	Trace	Very powerful irritant (acidic)	4 ppm	2 ppm
Hydrazine Azide (N2H5N3)	Trace	Explosive	None listed	None listed
Methyl Amine (CH3NH2)	Trace	Moderate irritant	10 ppm	None Allowed
N-Nitrosamine (NH2NO)	Trace	Carcinogenic	None listed	None listed
Formaldehyde dimethyl hydrazone	Trace	Not available	None listed	None listed
Tetrizine (N4H4)	Trace	(High Explosive)	None listed	None listed
Methyl Azide (CH3N3)	Trace	Explosive	None listed	None listed
Diazomethane (CH2N2)	Trace	Powerful Allergen, Carcinogen	0.2 ppm	None allowed
Hydrogen Cyanide (HCN)	Trace	Poison	10 ppm ceiling	None allowed
Dimethylnitrosamine (CH3)2NNO	Trace	Carcinogen, Teratogen, Poison	None allowed	None allowed
Hydrazine (N2H4)	Trace	Carcinogen, Poison	0.1 ppm	None allowed
UDMH	Trace	Carcinogen, Poison	1 ppm	0.5 ppm
NO2	Trace	Acidic, irritant	5 ppm	3 ppm

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.

Table 5-24 Chemical Toxicities

Propellant(s): TP-H-1148 (STS Solid Propellant) Conversion Factor = 4.0

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Carbon Dioxide (CO2)	2.3%	Poison, Asphyxiant (3)	30,000 ppm	5,000 ppm
Carbon Monoxide (CO)	23.1%	Poison	400 ppm	50 ppm
Water (H2O)	14.1%	None	None	None
Hydrochloric Acid (HCl)	15.9%	Acidic-Corrosive	3 ppm	1 ppm
Hydrogen (H2)	28.0%	Asphyxiant (3)	None	None
Nitrogen (N2)	8.4%	Asphyxiant (3)	None	None
Chlorine (Cl2)	Trace	Poison	3 pm	1 ppm
Iron Chloride (FeCl2)	Trace	None listed	None listed	None listed
Aluminum Oxide (Al2O3)	8.2%	None listed	20 mg/cu. meter	10 mg/cu. meter

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.

Table 5-25 Chemical Toxicities

Propellant(s): TP-H-1101 (MM Stage I Solid) Conversion Factor = 2.8

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH (2) Short Term Limit	ACHIH (2) TLV
Aluminum Chloride (AlCl2)	0.3%	Poison, Irritant	2 mg/cu. meter	None
Carbon Monoxide (CO)	23.0%	Poison	400 ppm	50 ppm
Carbon Dioxide (CO_2)	2.3%	Asphyxiant (3)	30,000 ppm	5,000 ppm
Chlorine (Cl)	0.08%	Poison, Irritant	3 ppm	1 ppm
Hydrachloric Acid (HCl)	15.9%	Acidic	3 ppm	1 ppm
Hydrogen Radical (H)	0.2%	None listed	None	None
Hydroxide ION (OH)	0.01%	None listed	None	None
Hydrogen (H2)	27.9%	Asphyxiant (3)	None	None
Water (H2O)	12.5%	None	None	None
Nitrogen (N2)	8.4%	Asphyxiant (3)	None	None
Aluminum Oxide (Al2O3)	7.9%	Irritant	20 mg/cu. meter	10 mg/cu. meter

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.

Table 5-26 Chemical Toxicities

Propellant(s): AVP-2862JM Mod II (MM Stage 2 Solid) Conversion Factor = 3

Reaction Product	% in Products(1)	Hazard(s) Posed	ACHIH/(2) Short Term Limit	ACHIH/(2) TLV
Hydrochloric Acid(HCl)	15.75%	Acidic	3 ppm	1 ppm
Nitrogen (N2)	8.31%	Asphyxiant (3)	None	None
Water (H2O)	14.30%	None	None	None
Hydrogen (H2)	33.97%	Asphyxiant (3)	None	None
Hydroxide Ion (OH)	Trace	None available	None listed	None listed
Chlorine (Cl)	Trace	Poison	3 ppm	1 ppm
Hydrogen Radical (H)	0.13%	None listed	None listed	None listed
Carbon Monoxide (CO)	25.30%	Poison	400 ppm	50 ppm
Carbon Dioxide (CO2)	2.17%	Asphyxiant, Poison	30,000 ppm	5,000 ppm
Aluminum Chloride(AlCl2)	Trace	Irritant, Poison	2 mg/cu. meter	None allowed
Aluminum Oxide (Al2O3)	9.0%	Irritant	20 mg/cu. meter	10 mg/cu. meter

(1) Where available. Assume no air entrainment.
(2) American Conference of Governmental Industrial Hygenists
(3) Asphyxiation is possible whenever breathing air is diluted to the point where the oxygen concentration drops below 18%.

5.5 ACOUSTIC

Noise level hazards were addressed mainly in large rocket motors. Walther (Ref. 59) discusses the acoustical effects of TNT explosives by defining the acoustical power as:

W = (1.355*n*m*c** 2)/2

where: n = conversion factor
m = propellant flow
c = effective exhaust velocity

the acoustical power level in db is

PWL = 10 Log(10) (w/w(o))

= SPL + 10 Log(10)(A)

W = acoustical power, watts
W(o) = reference power (0.001 watts)
SPL = sound pressure level (db)
L = distance from the source, ft
A = 4*Pi*r**2 free space radiation (surface of sphere)

5.5.1 Space Shuttle Acoustic Environment (Example Data)

From actual monitoring sites during the STS-1 launch, the following acoustic data was obtained.

Range		Maximum Sound Pressure Level
Meters	Miles	dB(A)
4,953	3.08	111
5,130	3.19	112
5,334	3.31	102
7,360	4.57	105
10,482	6.51	100
11,151	6.93	94
11,374	7.07	93
13,047	8.10	95
14,943	9.28	91
16,396	10.81	91
17,526	10.89	86
21,187	13.16	91
23,640	14.69	87

This data is representative of normal launch acoustic levels for a shuttle launch. Reference: 1981 JANNAF Safety and Environmental Protection Subcommittee Meeting, Environmental Noise Assessment, p. 267-278, CPIA Publication 348, November, 1981.

5.6 REFERENCES

(1) Update Chemical Rocket Propellant Hazards Manual, IITRI Project C06575. AFSC, May 1, 1984.

(2) Swatosh, J.J., Sequential Explosion Studies, IITRI Report #13-1971.

(3) Faber, E.A., A Mathamatical Model for Defining Explosive Yield and Mixing Probabilities of Liquid Propellants. Engineering Progress at the University of Florida Technical Paper No. 346, March, 1966.

(4) Lester, Gibbs, and Lessor. A Study of Liquid Propellant Autoignition, NAS10-8591, May 1975.

(5) Ullian, L.J., Detonability of Large Solid Rocket Motors, ESMC, Patrick AFB, Florida.

(6) Napadensky and Kennedy, A Criterion for Predicting Impact Initiation of Explosive Systems, IITRI, 1964.

(7) Willoughby, Wilton, and Mansfield, Liquid Propellant Explosive Hazards Volume 1 (Project PYRO), AFRPL-TR-68-92.

(8) Willoughby, Wilton, and Mansfield, Liquid Propellant Explosive Hazards Volume 2, AFRPL-TR-68-92, December 1968.

(9) Willoughby, Wilton, and Mansfield, Liquid Propellant Explosive Hazards Volume 3, AFRPL-TR-68-92, December 1968.

(10) Gunther, P, and Anderson, G.R., Statistical Analysis of Project Pyro Liquid Propellant Explosion Data, Bellcomm TM-69-1033-3, July, 1969.

(11) Rosenfield, M.J., The Development of Damage Indexes to Structures Due to Liquid Propellant Explosions, Phase I, April 1966. DTIC No. AD481497.

(12) Rosenfield, M.J., The Development of Damage Indexes to Structures Due to Liquid Propellant Explosions, Phase II, ORDL TR-4-75, November 1968. DTIC No. AD845513.

(13) Chemical Explosions in Space, Final Report, Houston Research Institute, NAS 9-2640, February, 1965.

(14) Fletcher, R.F., Liquid Propellant Explosions, Journal of Spacecraft and Rockets, Vol. 5, No. 10, October 1968, pp 1227-1229.

(15) Fletcher, R.F., Gerneth, D., and Goodman, C, Explosion of Propellants, AIAA Journal, Vol. 4, No. 4.

(16) Fletcher, Simmons, Gift, and Spurlock, Reactions and Expansion of Hyperogolic Propellants in a Vacuum, AIAA Journal, Vol. 6, No. 5, May, 1968.

(17) Fletcher, Characteristics of Liquid Propellant Explosion, Annuals of New York Academy of Science, Oct. 28, 1968, Vol. 152, Art. 1, pp. 432-440.

(18) Pesante and Nishibayashi, Evaluation of the Blast Parameters and Fireball Characteristics of Liquid Oxygen/Liquid Hydrogen Propellants, Aerojet General Corporation Report No. 0954-01(01) FP April 1967.

(19) Nishibayashi, M., et. al., Study of Phenomena Associated with Mixing of Cryogenic Fluids, Aerojet Report No. 0808-01 (16) FP, February, 1965. NAS8-11063.

(20) Summary Report on a Study of the Blast Effects of a Saturn Vehicle, February, 1962, ADL Control No. 101,907

(21) Technical Memorandum on Explosive Effects Produced by Failure of Launch Vehicles, A.D. Little Incorporated, February, 1967.

(22) An Investigation of Hazards Associated with the Storage and Handling of Liquid Hydrogen, March 1960, DTIC AD 324194.

(23) Kite, F., and Bader, B., Pad-Abort Thermal Flux Model for Liquid Rocket Propellants, Sandia Laboratory SC-RR-66-577, November, 1966.

(24) Kite, Webb, and Bader, Launch Hazards Assessment Program, Report on Atlas-Centaur Abort, Sandia Laboratory SC-RR-65-333, October, 1965.

(25) Irwin, O.R., and Waddell, J.L., Study of Detonation Induction in Solid Propellants by Liquid Propellant Explosions, Aerojet Report No. 0797-01 (06) QP, March, 1964.

(26) Letho, D., Fluid Flow Calculations for External Tank Destruct, NSWC, White Oak Lab, Viewgraph presentation.

(27) Holtzscheiter, Kelleher, and Tate, In-Silo Launch Abort Environment for LGM25C Missile, AFWL-TR-75-177, May 1976.

(28) Large Solid Propellant Boosters Explosive Hazards Study Program, (Project SOPHY), AFRPL TR-65-211, 1965, DTIC No. AD476617.

(29) Giesler, Irwin, Roark, and Salzman, Detonation Hazards of Large Solid Rocket Motors, Aerojet-General Report 1965, contract AF 04 (611)-9945, 1965.

(30) Valor, Irwin, Roark, Salzman, and Vail, Detonation Characteristics of Large Solid Rocket Motors, Aerojet - General Report 8-1966, 1966.

(31) Holland, N., and Peters, J., The TNT Equivalent Weight of the Solid Propellant used in the SOPHY Tests for 60" and 72" Diameter Rocket Motors, Memo.

(32) Ewell, Irwin, and Vail, Large Solid-Propellant Boosters Explosive Hazards Study Program, (Project SOPHY) Final Report, 1967.

(33) High Explosive Equivalency Tests of Large Solid Propellant Motors, GIDEP Report NWC-TP-4643, September, 1968.

(34) Rickey, H.M., High Explosive Yield Tests of Solid Propellants, NOTS Report 7-1965, 1965.

(35) Weals, F.H., and Wilson, C.H., High Explosive Equivalent Tests of Rocket Motors, NOTS-TP-3910, TR-413, 1965.

(36) Swisdak, M., et.al., Solid Rocket Booster Command Destruct System Hazards Study, 1985

(37) Benn, D.M., STS, SRM Propellant Detonation Probability, Letter from D. Benn to L. Ullian, June 1983.

(38) Swisdak, MM, Explosion Effects and Properties, Part 1-Explosion Effects in Air, NSWC, White Oak Laboratory, NSWC/WOL/TR 75-116, October 1975.

(39) Weals, F.H., Titan III Solid Motor Impact Test, Technical Memo, U.S. Naval Ordnance Test Station (NOTS), 1964.

(40) Zaker, T.A., Trajectory Calculations in Fragment Hazard Analysis, Technical Memorandum, Armed Services Explosives Safety Board, August, 1971.

(41) Richmond, D.R., and Fletcher, E.R., Blast Criteria For Personnel in Relation to Quantity-Distance, Lovelace Foundation for Medical Education & Research, Technical Report, 1971.

(42) Napadensky, Kot, Shikari, and Wiedermann, Initiation Mechanisms of Solid Rocket Propellant Detonation, IITRI Technical Report, 1973.

(43) Kingery, C.N., and Bulmash, G., Airblast Parameters From Spherical Air Burst and Hemispherical Surface Burst, Ballistic Research Laboratory Technical Report ARBRL-TR-02555, April, 1984.

(44) Dale, C., et.al., Status Report on Hazard Evaluation of Large Solid Rocket Motors, Naval Ordnance Station, 1967.

(45) Giant Patriot - Incremental Velocity Curves, TRW Memo 71-4342.2-21, March, 1971.

(46) Giant Patriot - Incremental Velocity of Destruct, TRW Memo 71-4342.2-18, March, 1971.

(47) Data Correlation and Velocity Calculations for Giant Patriot Debris, TRW Memo 8522.5-71-6, April, 1971.

(48) Giant Patriot - Incremental Velocities of Destruct Debris, TRW Memo 71-4342.2-18, March, 1971.

(49) Collins, Gabler, and Kennedy, Development of an Explosion Velocity Model Using Debris Impact Scatter, J.H. Wiggins Co. Technical Report No. 74-3029-1, November, 1974.

(50) Baker, W.E., et.al., Workbook for Predicting Pressure Wave and Fragment Effects of Exploding Propellant Tanks and Gas Storage Vessels, Southwest Research Institute Report No. N76-19296, Contract NAS 3-19231, September 1977.

(51) Anderson, Olsen, and Owings, Fragment Environments For Postulated Accidents of the STS and Postulated Accidents of the Orbiting Vehicle, Teledyne Energy Systems Report TES-16018-04, October, 1980, NAS 9-16018.

(52) Blast and Fragment Hazards from Bursting High Pressure Tanks, NOLTR-72-102, May, 1972.

(53) Van Nice and Carpenter, Thermal Radiation from Saturn Fireballs, TRW Task ASPO-24, Contract NAS9-4810, December, 1965.

(54) Gayle, J., and Bransford, J., Size and Duration of Fireballs from Propellant Explosions, NASA-TM-X-53314, August, 1965.

(55) High The Saturn Fireball Annals of New York Academy of Sciences, Oct. 28, 1968, Vol. 152, Art. 1, pp. 441-451.

(56) Prince, S., Atmospheric Dispersion of Hypergolic Rocket Fuels, Phase I Final Report, Martin Marietta Technical Report, Contract F42600-81-D-1379, September 1982.

(57) Bader, Donaldson, et. al., Liquid Propellant Rocket Abort Fire Model, Journal of Astronautics and Aeronautics, December 1971.

(58) Banning, D., Propellant Spill Analysis, Martin Marietta Technical Report, July 1983.

(59) Williams, D.C., Vaporization of Radioisotope Fules in Launch Vehicle Abort Fires, Sandia Laboratories Report SC-RR-71-0118, December 1971.

(60) Mansfield, J.A., Heat Transfer Hazards of Liquid Rocket Propellant Explosions, AFRPL-TR-69-89, February 1969.

(61) Prince, S., and Haas, W.R., Atmospheric Dispersion of Hypergolic Rocket Fuel, Phase II, Martin Marietta Technical Report, Contract F42600-81-D-1379, March 1984.

(62) Walther, L.C., Accoustical Effects of Large Rocket Motors, Aerojet-General Technical Report, 1962.

(63) Strehlow, et. al, The Characterization and Evaluation of Accidental Explosions, NTIS No. N75-32191, NASA CR134779, June 1975.

(64) American National Standard: Estimating Airblast Characteristics for Single Point Explosions in Air, With a Guide to Evaluation of Atmospheric Propagation Effects, ANSI S2.20-1983 (ASA 20-1983).

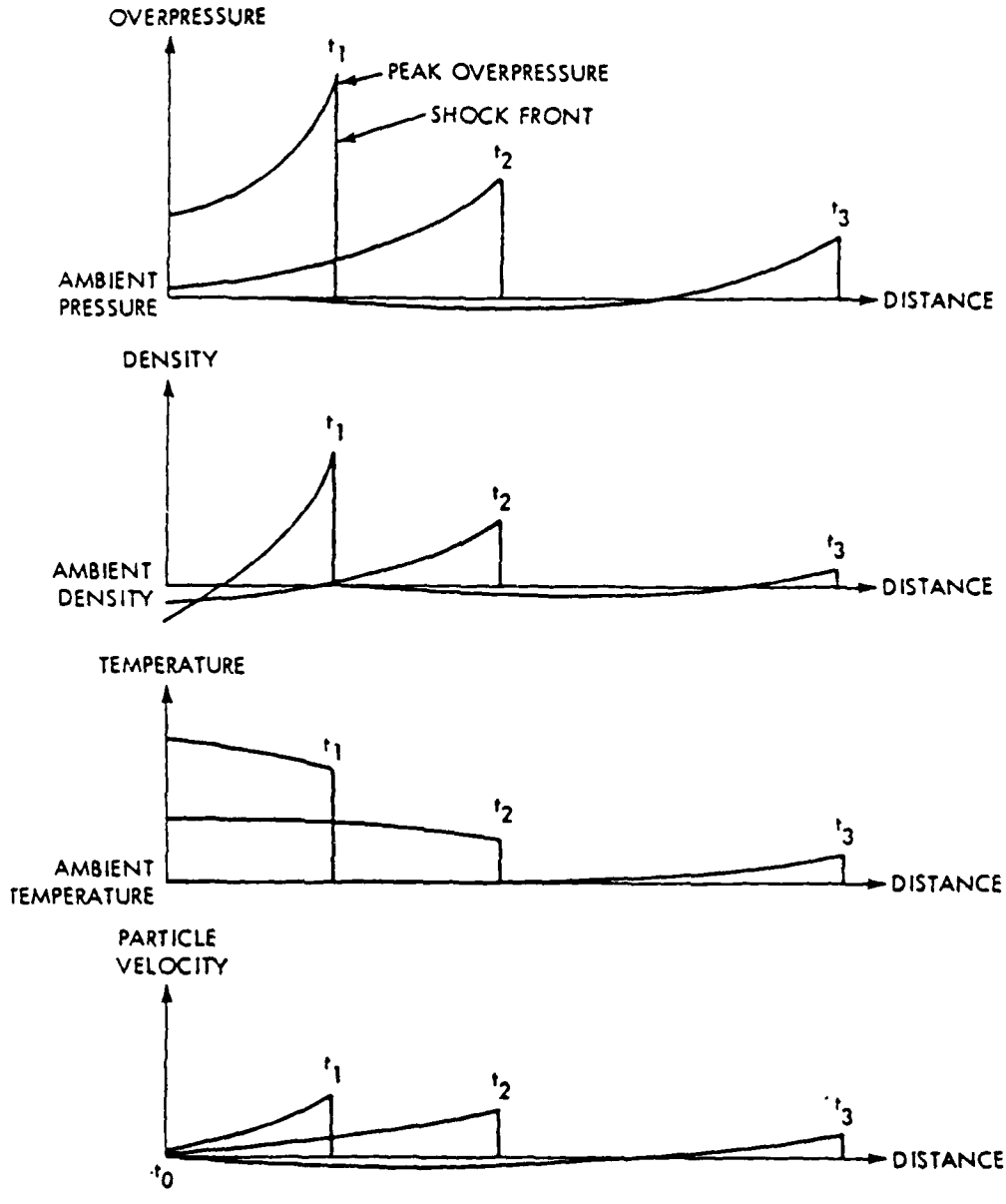
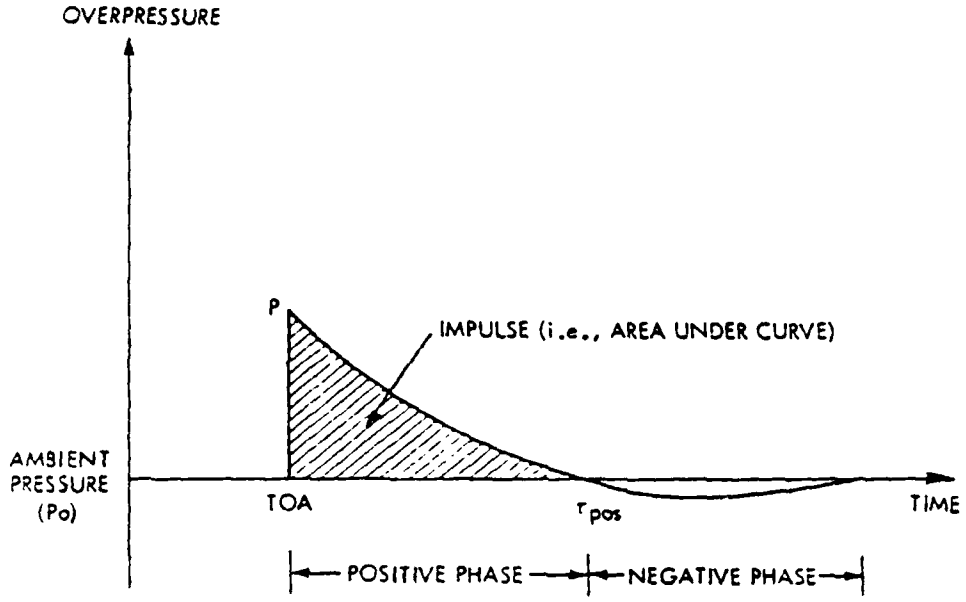


Figure 5-1 Qualitative Variation of Shock Wave Parameters With Distance and Time (Ref. 36)

From: Swisdak, M.M., Explosion Effects and Properties, Part 1 - Explosion Effects in Air, Naval Service Weapons Center, White Oak Laboratory, NSWC/WOL/TR 75-116, 6 October 1975.



(1) TOA (TIME-OF-ARRIVAL) ≡ THE TIME REQUIRED FOR THE SHOCK WAVE TO TRANSIT THE DISTANCE FROM THE CENTER OF THE EXPLOSION TO THE POINT AT WHICH THE MEASUREMENT IS TO BE MADE.

(2) P (OVERPRESSURE) ≡ PEAK PRESSURE ABOVE AMBIENT CONDITIONS.

(3) τ ≡ POSITIVE PHASE DURATION - THE LENGTH OF TIME (MEASURED FROM THE FIRST PRESSURE RISE) NECESSARY FOR THE OVERPRESSURE TO RETURN TO THE AMBIENT PRESSURE.

(4) POSITIVE PHASE IMPULSE ≡ $\int_0^{\tau} P(t)\, dt$

Figure 5-2 Important Shock Wave Parameters (Ref. 1)

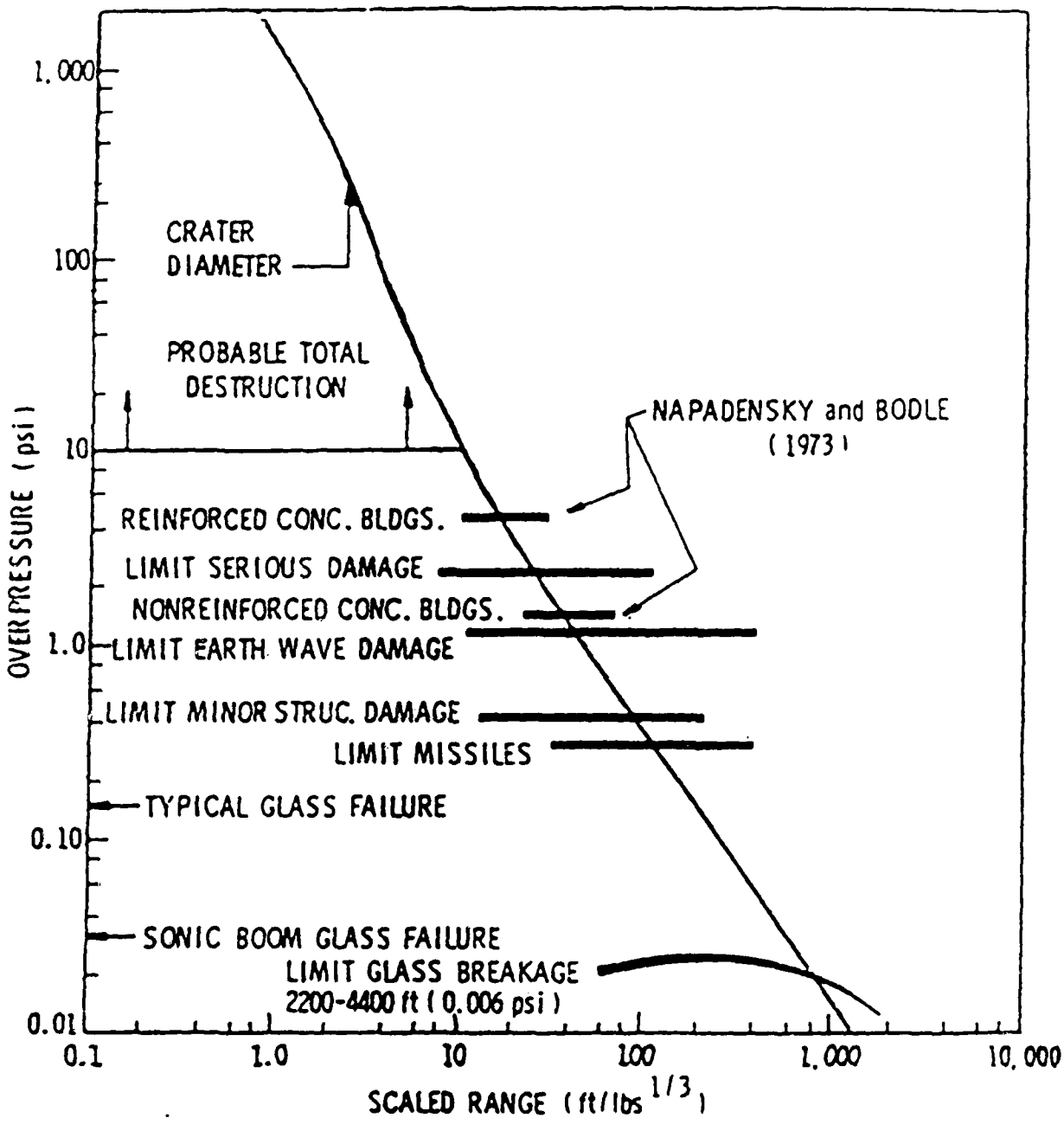


Figure 5-3 Overpressure Scaled Distance Plot Showing Typical Levels for Blast Damage (Ref. 1)

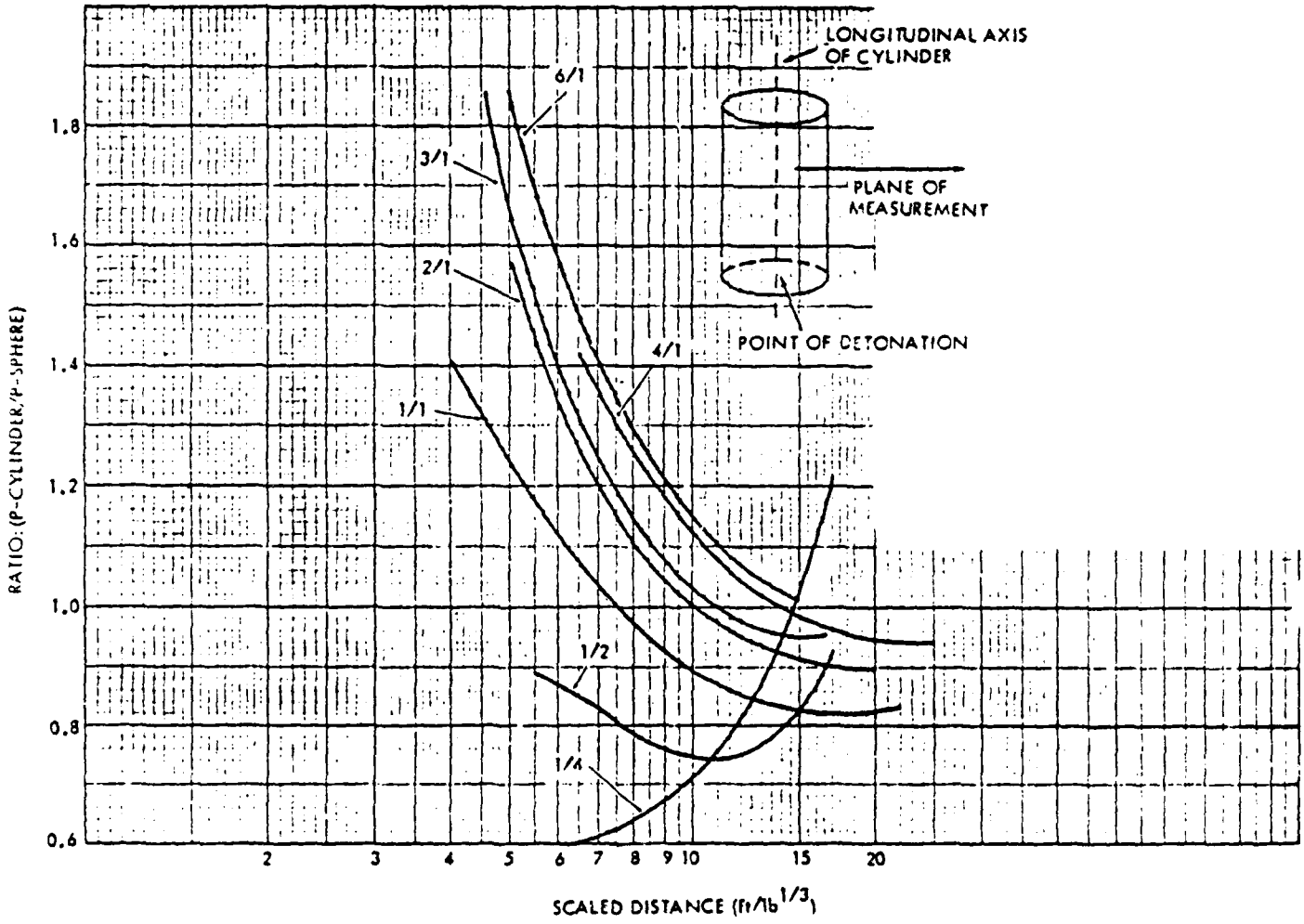


Figure 5-4 Ratio of Free Air Peak Overpressure (P-Cylinder/P-Sphere) vs Distance for Cylinders with Differing Aspect Ratios (L/D) (Ref. 36)

From: Swisdak, M.M., Explosion Effects and Properties, Part 1 - Explosion Effects in Air, Naval Service Weapons Center, White Oak Laboratory, NSWC/WOL/TR 75-116, October 1975.

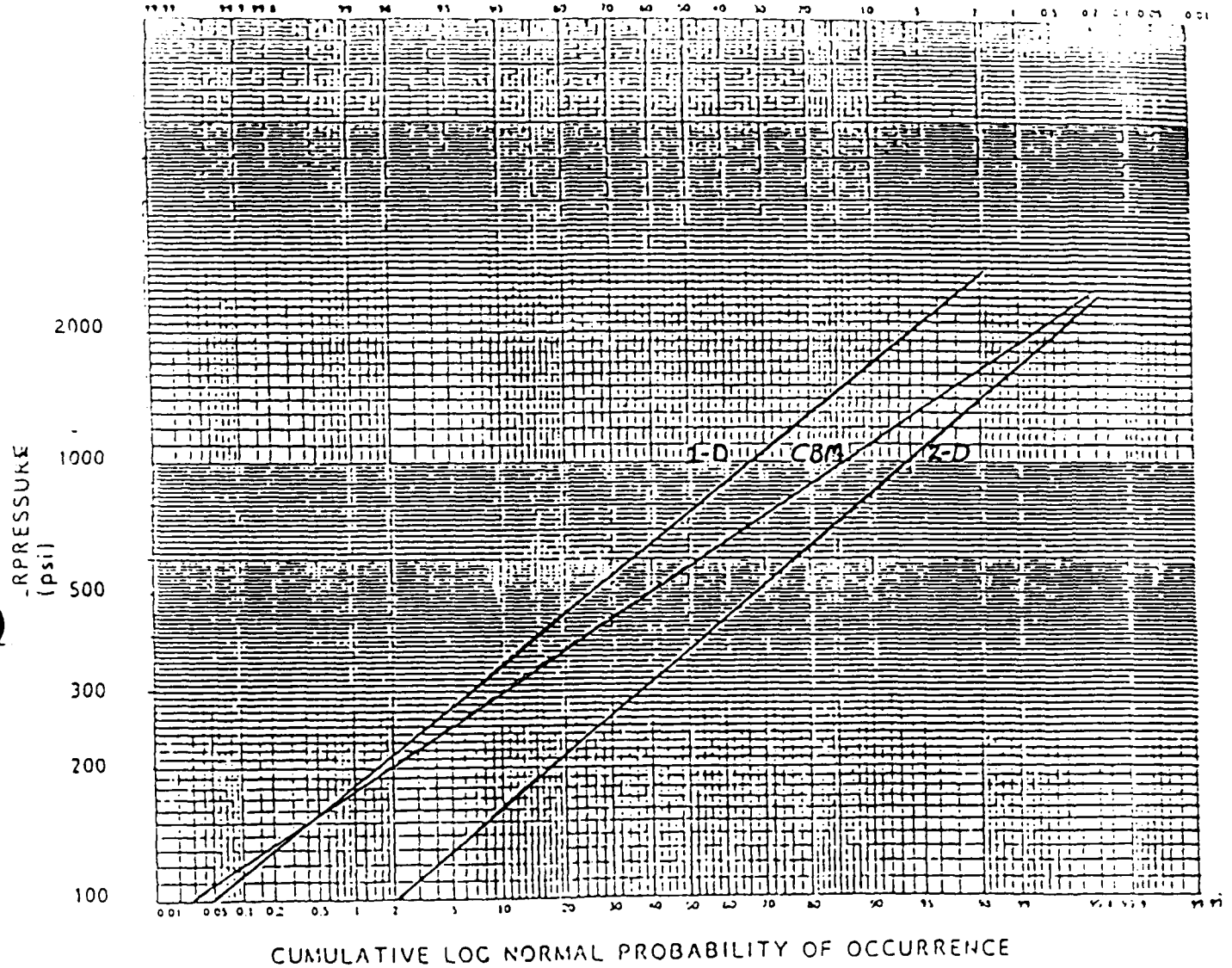


Figure 5-5 Overpressure vs. Log Normal Probability of Occurrence for Near-Field Distances

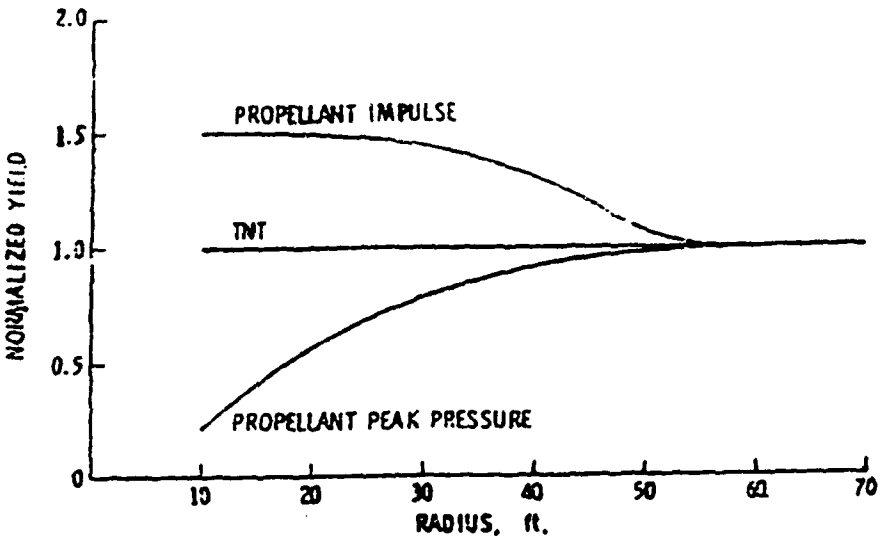


Figure 5-6 Normalized Pressure and Impulse Yields from Explosion of N204/Aerozine-50. Fletcher (1968) (Ref. 14)

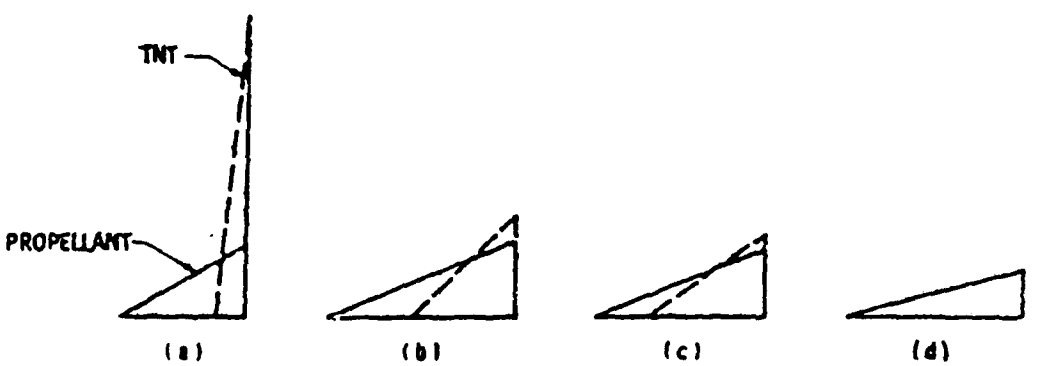


Figure 5-7 Representative Shock Impulses Showing Coalescence of Shock Waves from Dissimilar Sources (Stages (a) through (d)). Fletcher (1968) (Ref. 14)

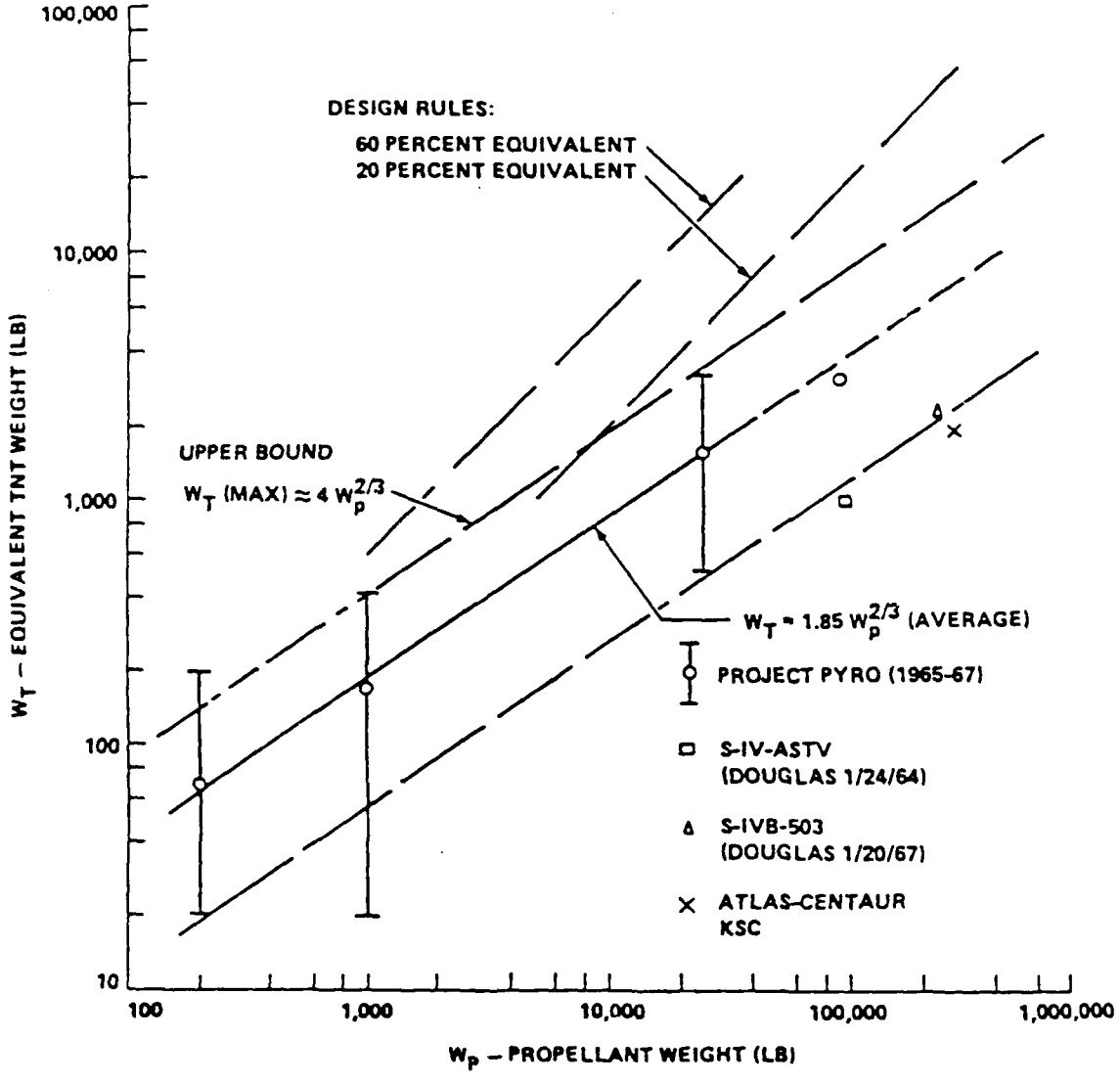
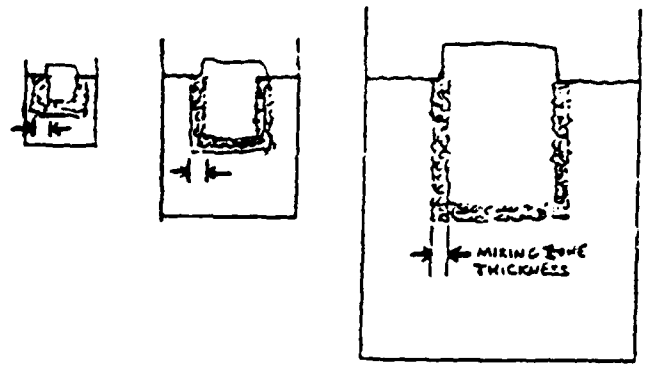


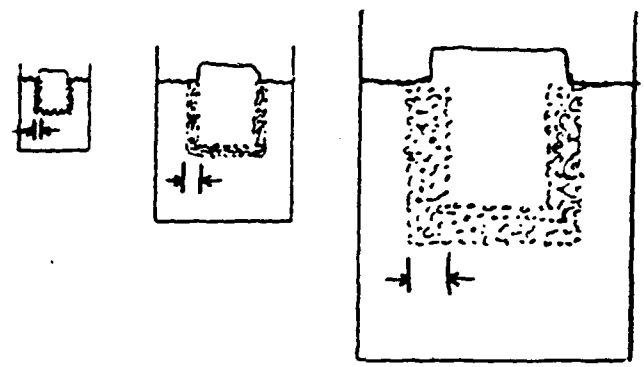
Figure 5-8 Trend in Measured Equivalent TNT Weight from LOX/LH2 Propellant Explosions Compared to Design Rules

From: Sutherland, L.C. Scaling Law for Estimating Liquid Propellant Explosive Yields, Journal of Spacecraft and Rockets, Volume 15, No. 2 March/April 1980.



MIXING ZONE THICKNESS INDEPENDENT OF SCALE

GIVES $W_T \propto W_P^{2/3}$



MIXING ZONE THICKNESS $\propto$ SCALE

GIVES $W_T \propto W_P$

W_T = EQUIVALENT WEIGHT OF EXPLOSION

W_P = PROPELLANT WEIGHT

Figure 5-9 Models of Liquid Propellant Mixing Zone Thickness

From: Letho, D., Fluid Flow Calculations for External Tank Destruct, Naval Surface Weapons Center, White Oak Lab (Ref. 24).

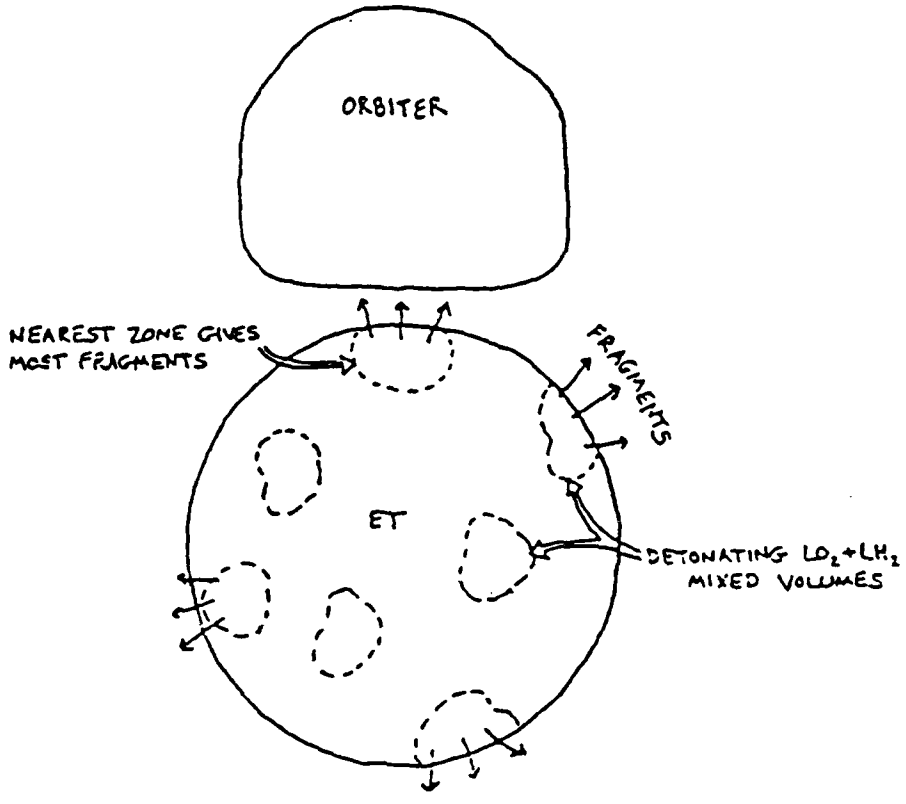
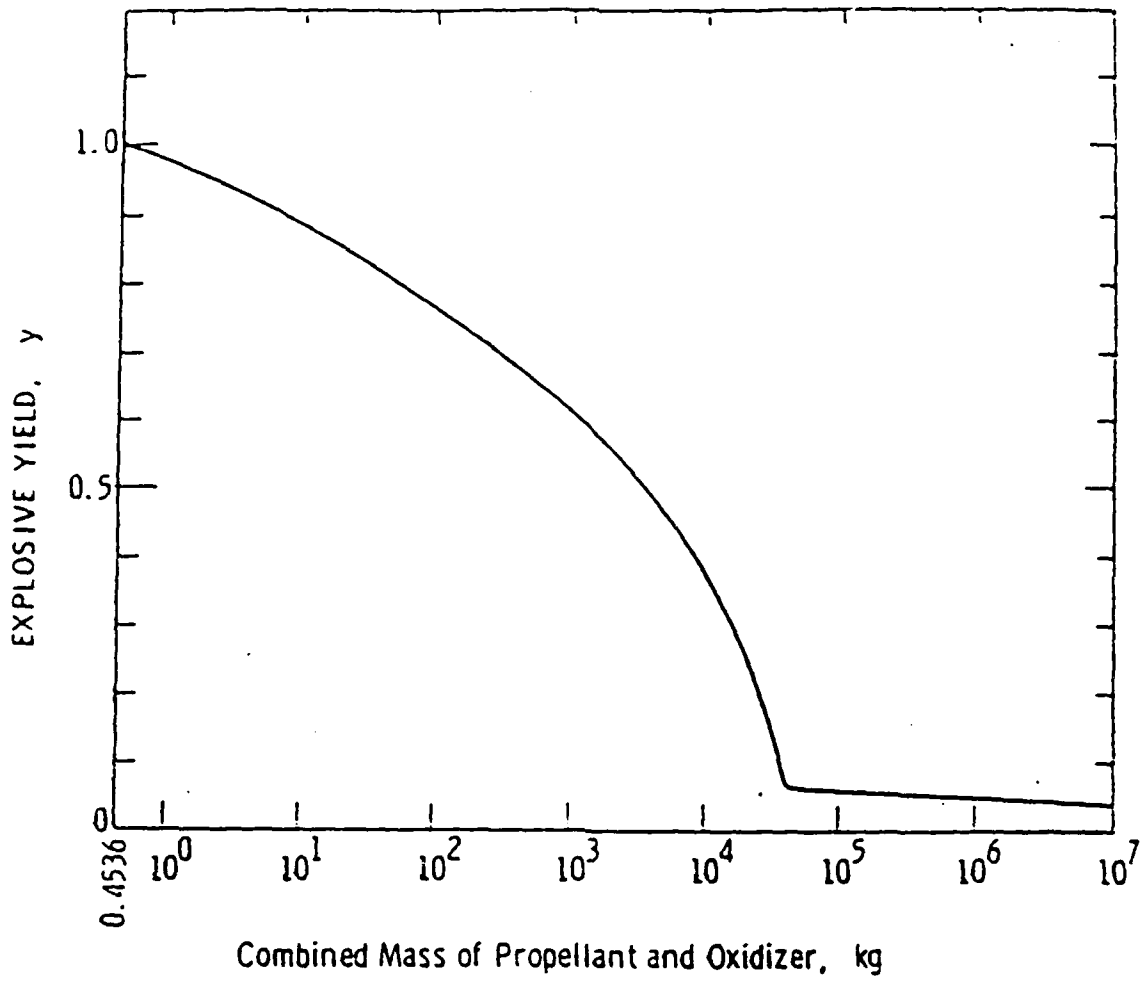


Figure 5-10 Multiple Mixing Zones in a Liquid Propellant

From: Letho, D., Fluid Flow Calculations for External Tank Destruct, Naval Surface Weapons Center, White Oak Lab (Ref. 24).



Multiplier Factors:

(1) Hypergolic - 240%

(2) $LO_2/RP\text{-}1$ - 125%

(3) LO_2/LH_2 - 370%

Figure 5-11 Estimated Terminal Yield as a Function of Combined Propellant and Oxidizer Mass (Ref. 48)

From: Baker et. al. Work book for Predicting Pressure Wave and Fragment Effects of Exploding Propellant Tanks and Gas Storage Vessels, NASA CR-134906, Sept. 1977.

NOTE: See pages 5-8 for discussion on limitations or use of this data.

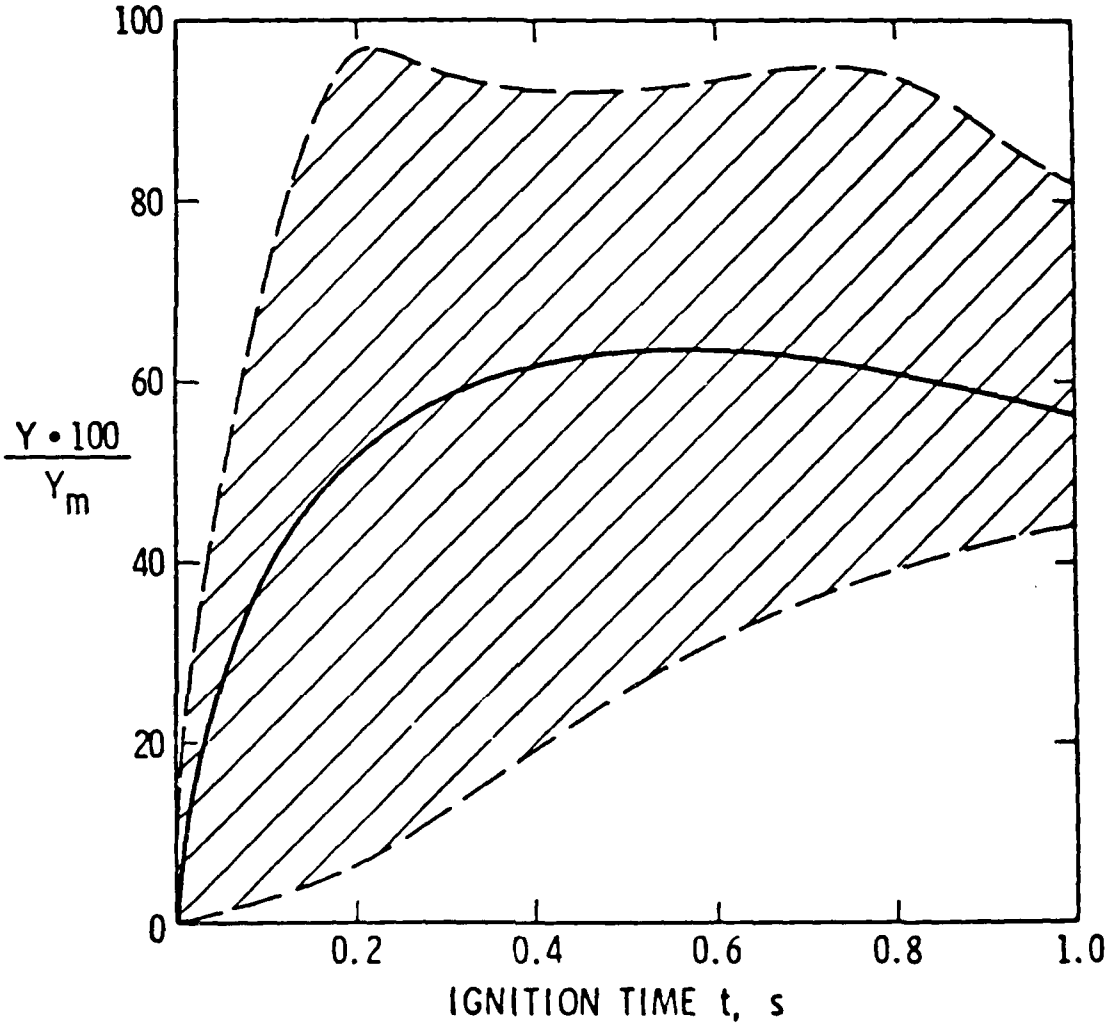


Figure 5-12 Normalized Terminal Yield vs. Ignition Time for LO2/LH2 CBGS (Ref. 48)

NOTE: See pages 5-8 for discussion on limitations or use of this data.

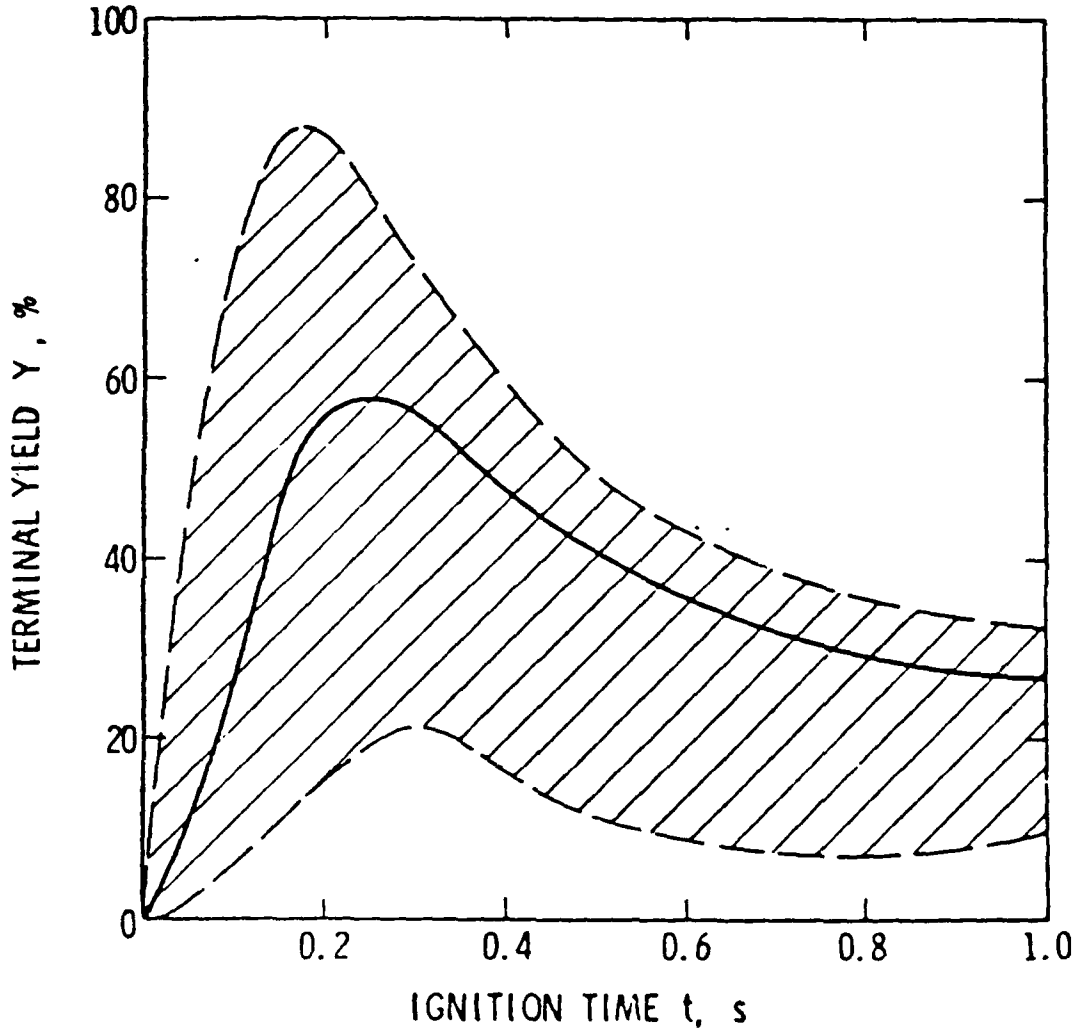


Figure 5-13 Terminal Yield vs. Ignition Time for LO2/LH2 CBM (Ref. 48)

NOTE: See pages 5-8 for discussion on limitations or use of this data.

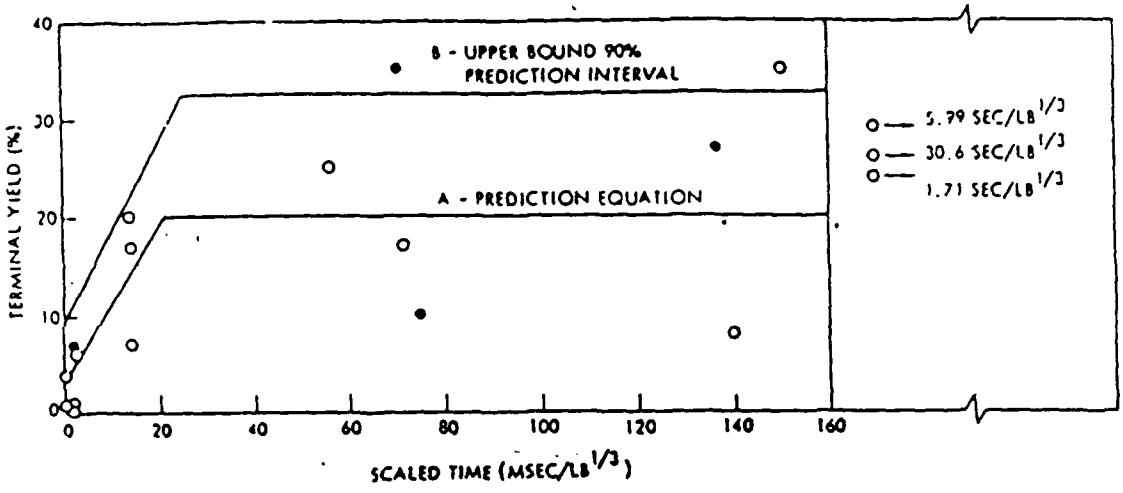


Figure 5-14 Comparison of Prediction Equation for LO2/LH2 CBM Case with Experimental Data for All Cases but L/D of 1.8 and Do/Dt of 1 (0-200 lb, - 1,000 lb)

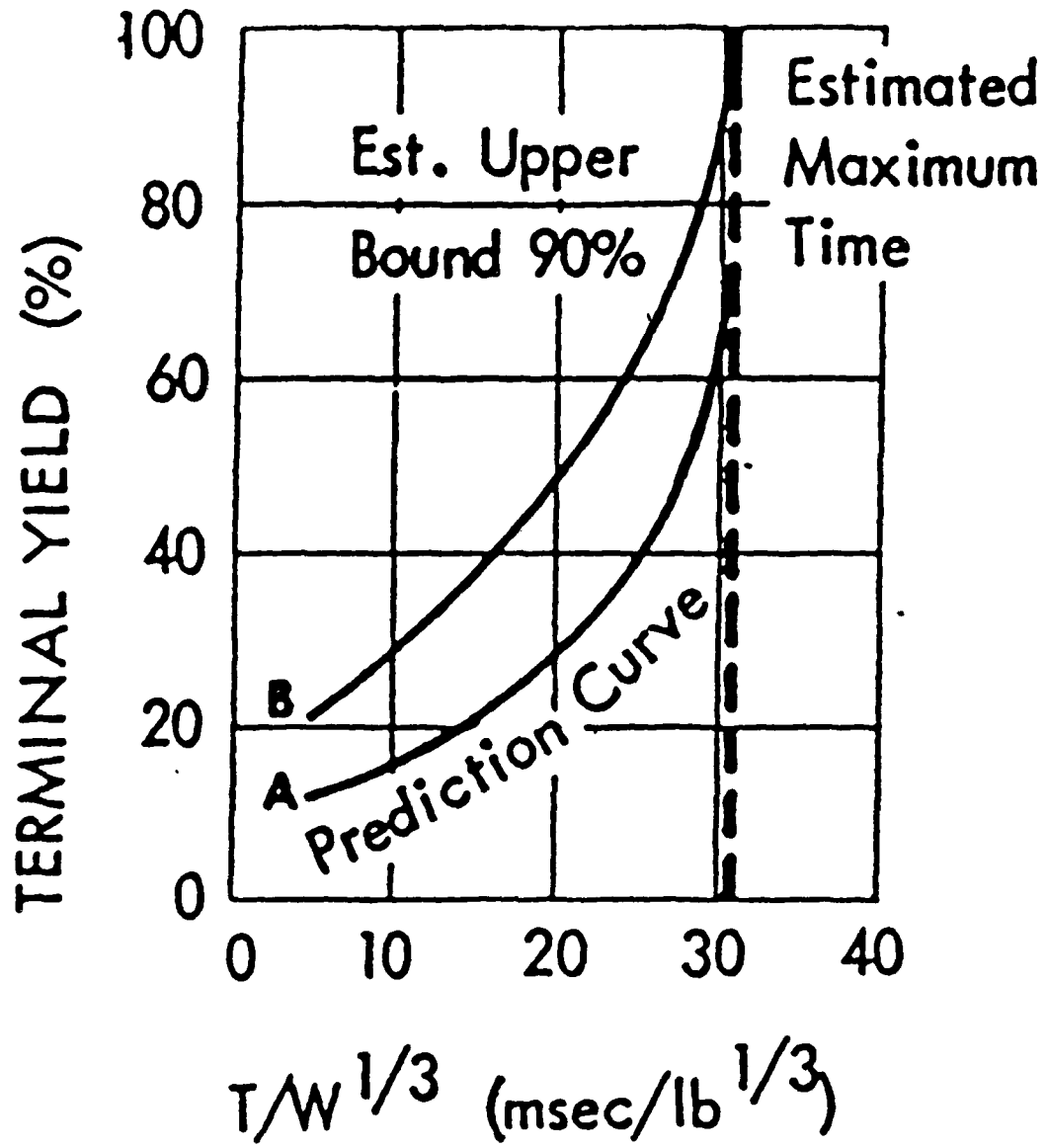


Figure 5-15 Terminal Yield, Upper 90% Prediction, for LO2/LH2 CBM Case (Ref. 9)

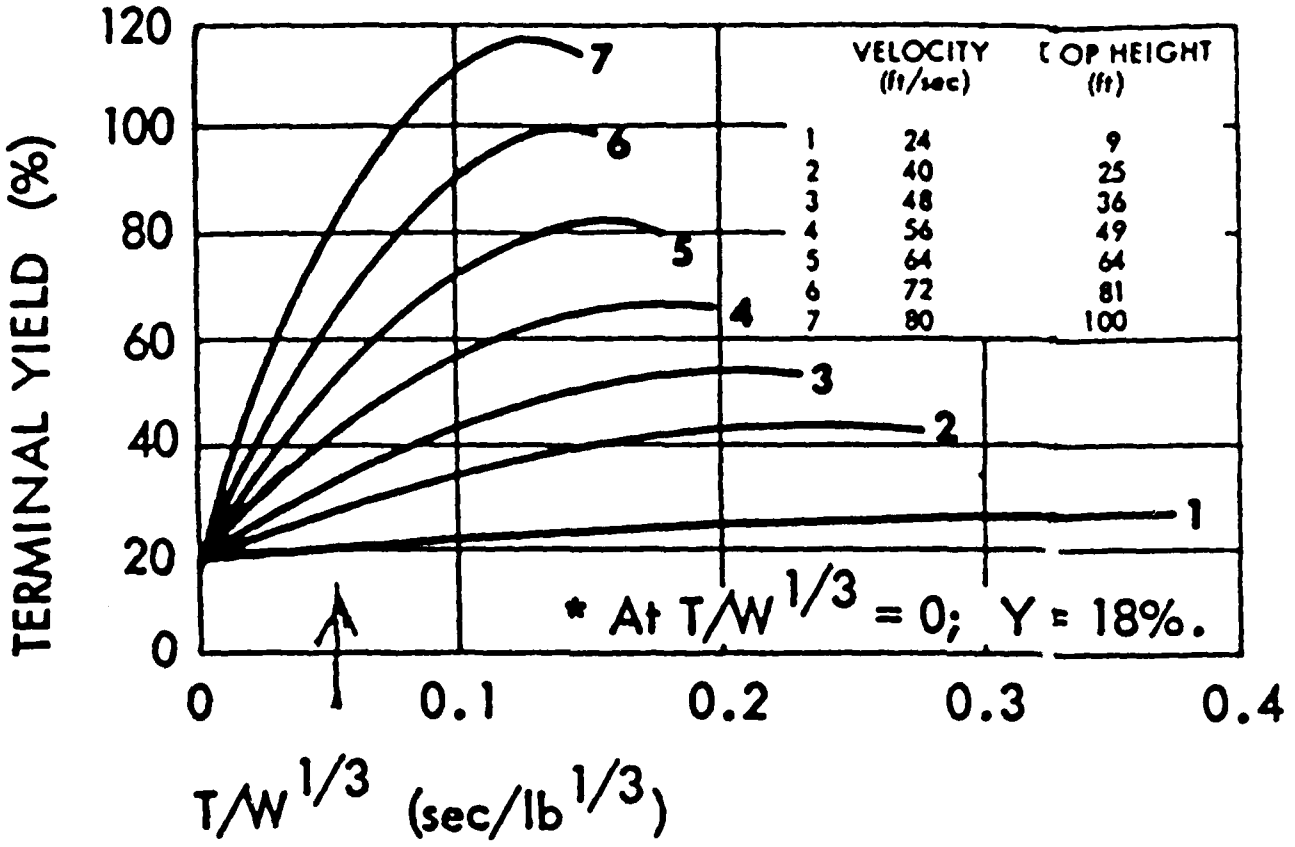


Figure 5-16 Terminal Yield vs. Scaled Time for LO2/LH2 CBGS Case as a Function of Impact Velocity (Ref. 9)

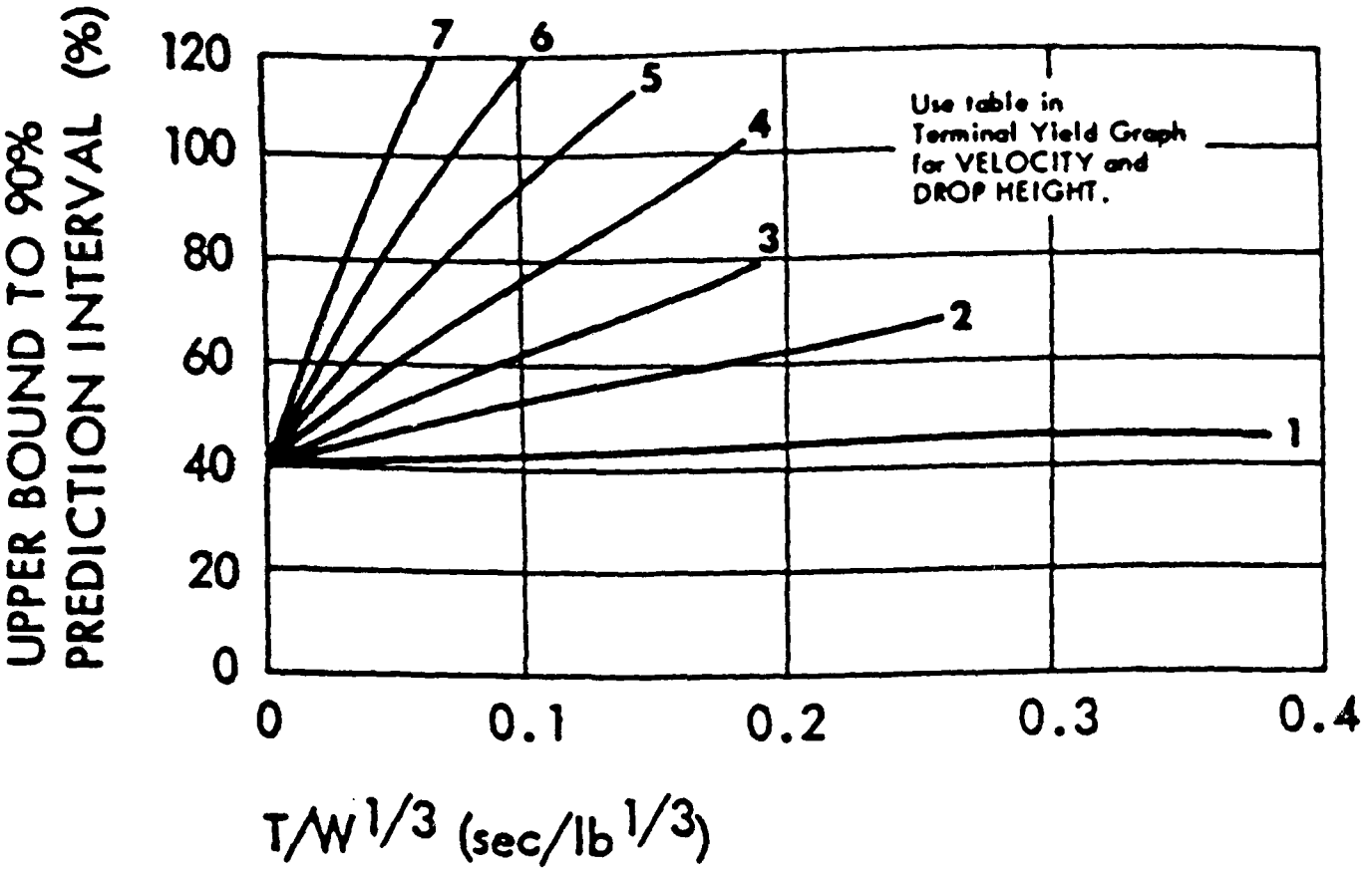


Figure 5-17 90% Prediction Terminal Yield vs. Scaled Time for LO2/LH2 CBGS Case (Ref. 9)

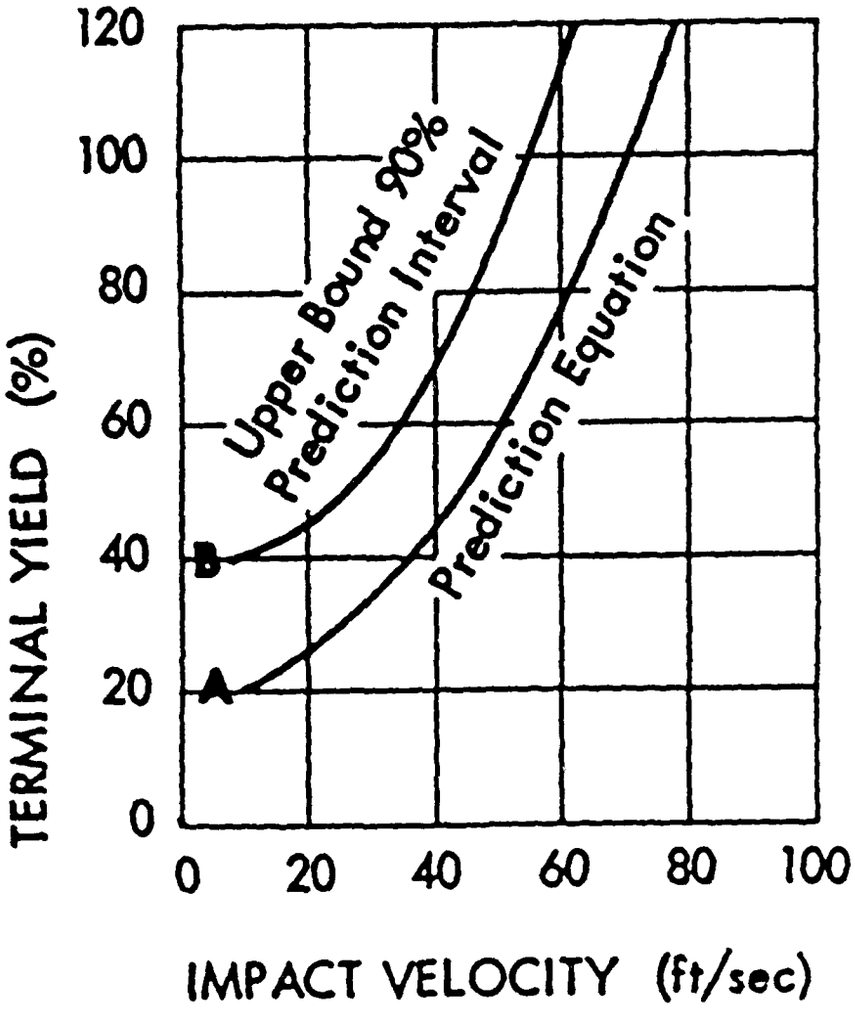


Figure 5-18 Maximum Terminal Yield vs. Impact Velocity for LO2/LH2 CBGS Case (Fall Back) (Ref. 9)

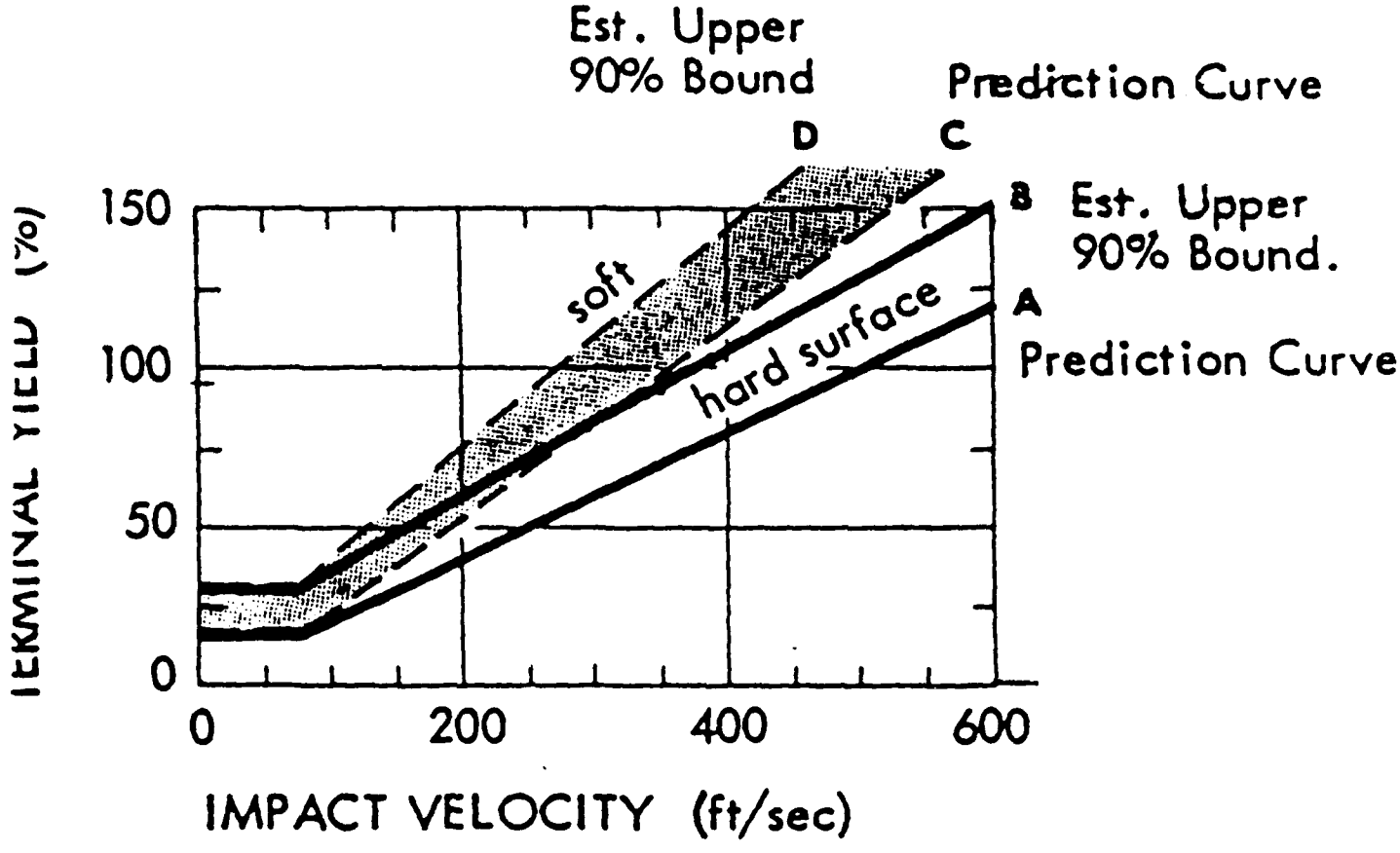


Figure 5-19 PYRO High Velocity Tests Prediction Chart for LO2/LH2 (Ref. 9)

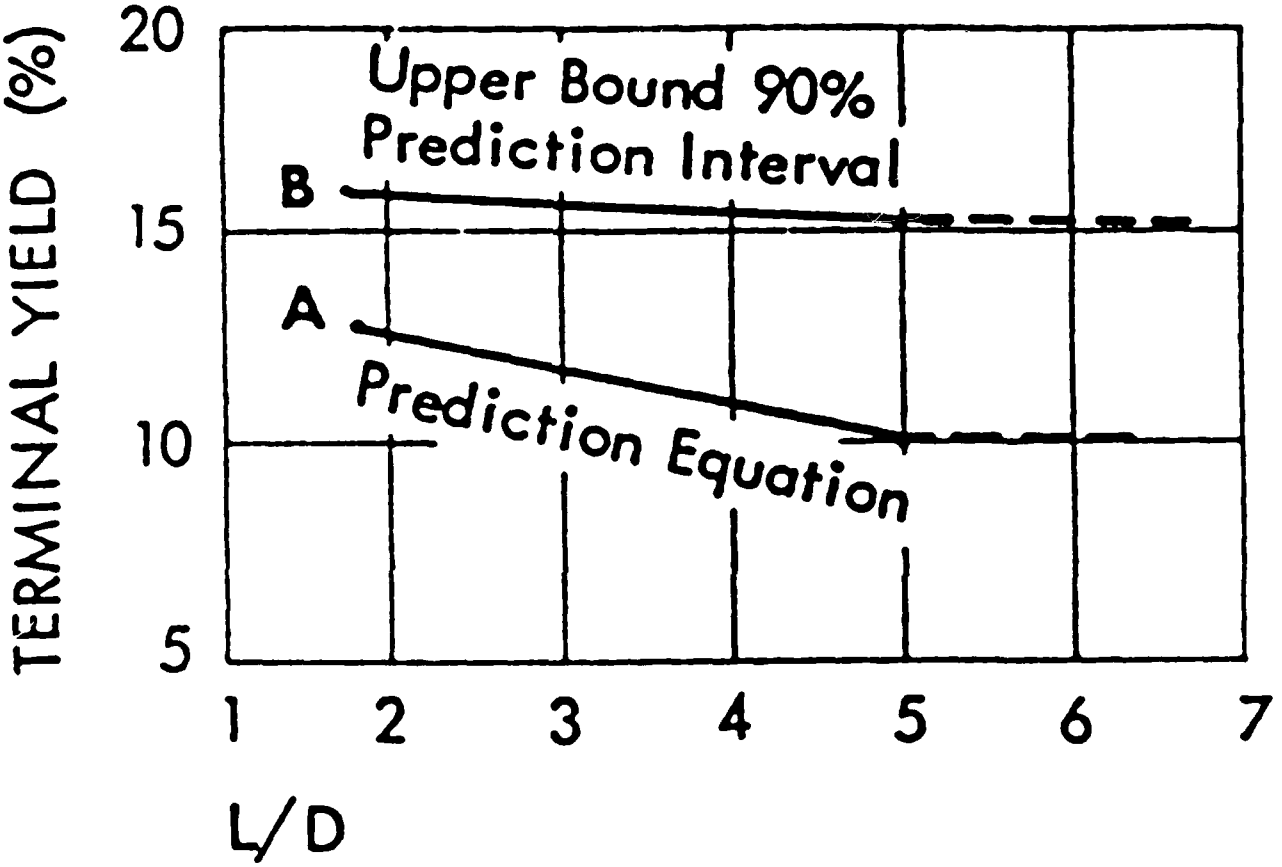


Figure 5-20 LO2/RP-1 CBM Terminal Yield (Y) vs. L/D (Ref 9)

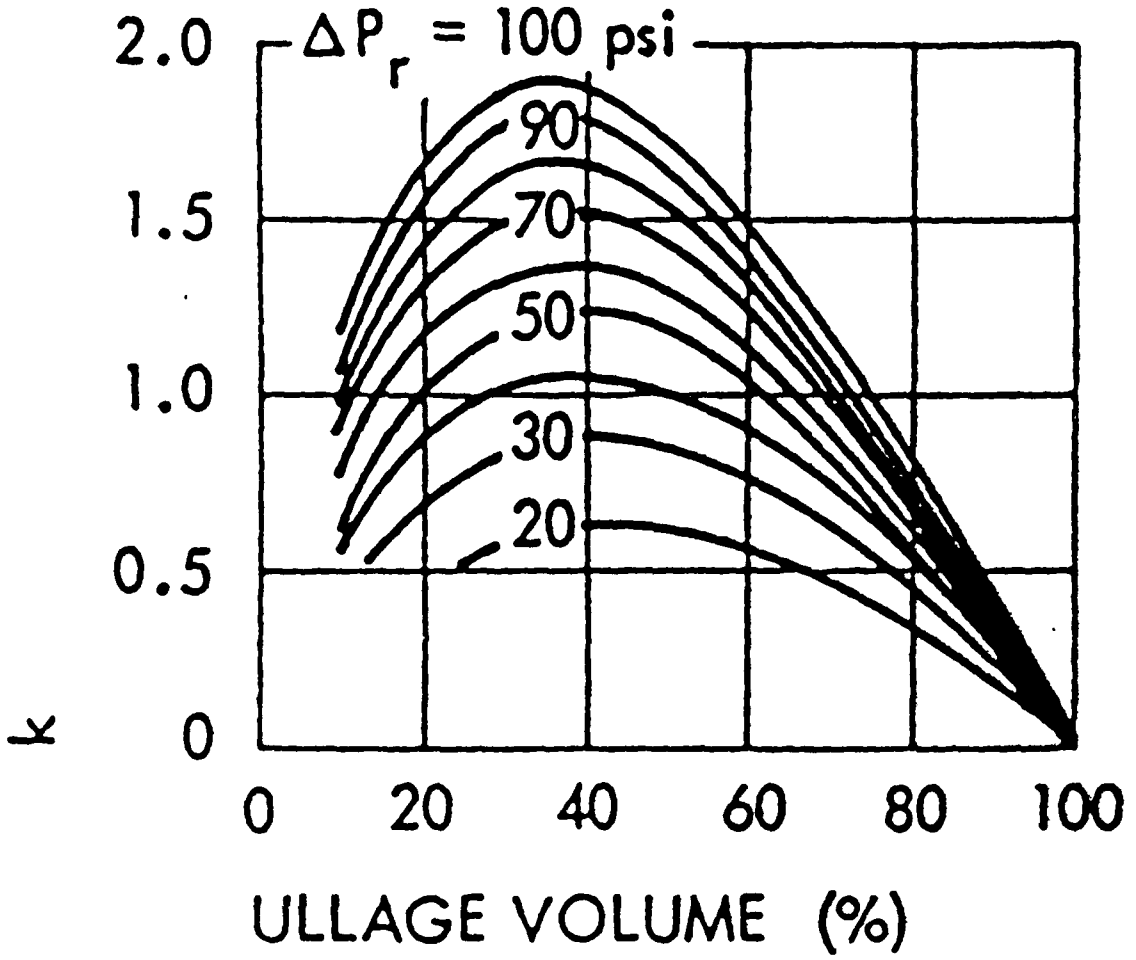


Figure 5-21 LO2/RP-1 CBM k Factors vs Ullage Volume (Vu) as a function of delta P (Ref. 9)

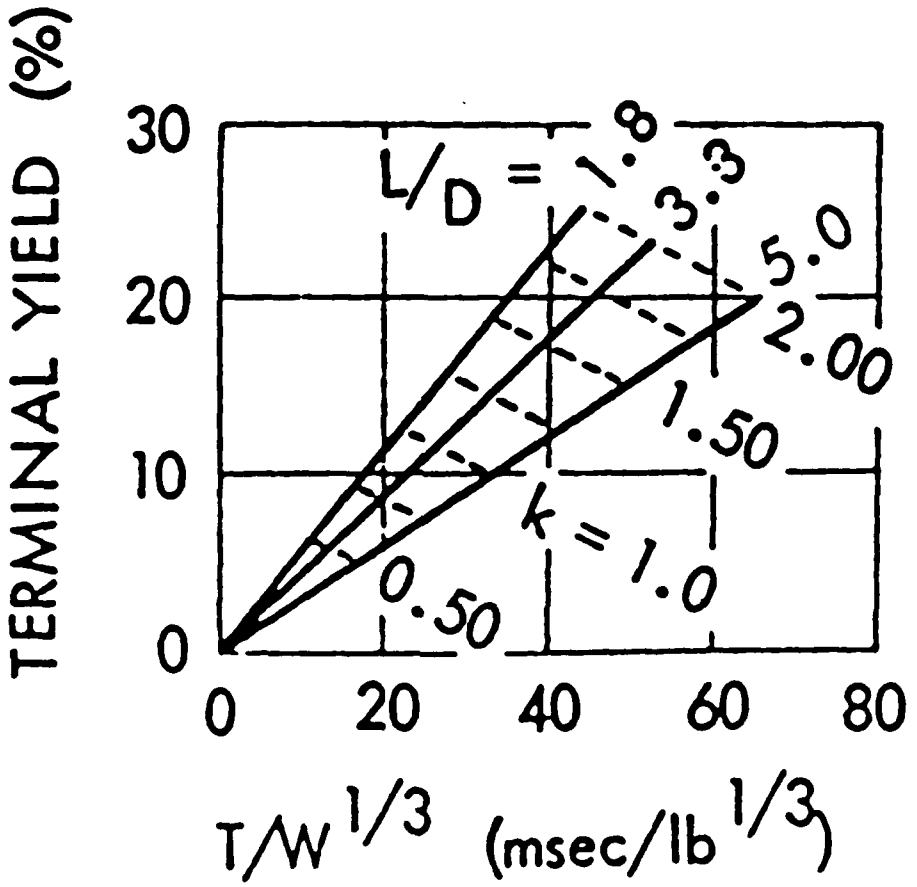


Figure 5-22 LO2/RP-1 CBM Terminal Yield (Y) vs T/(W**(1/3)) as a Function of L/D and k (Ref. 9)

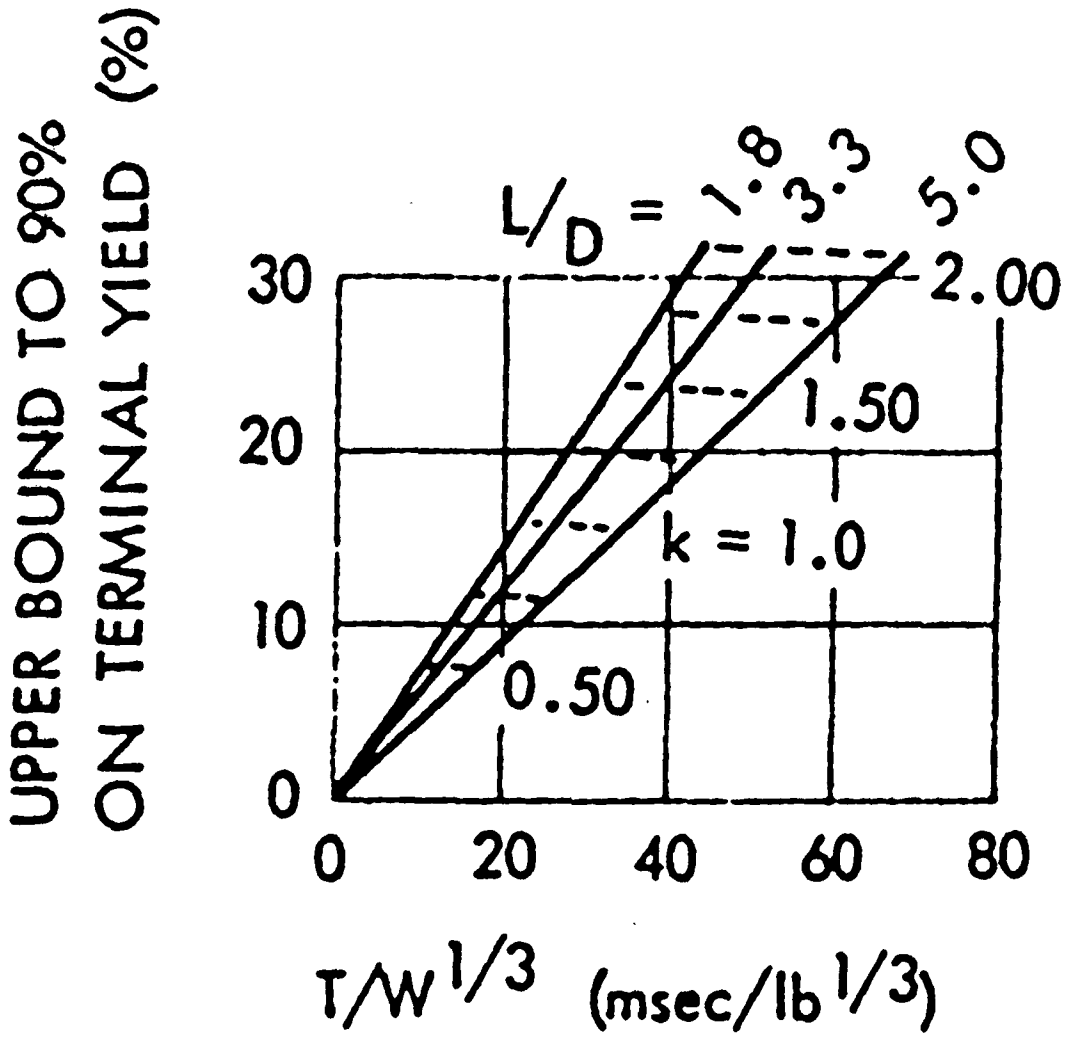
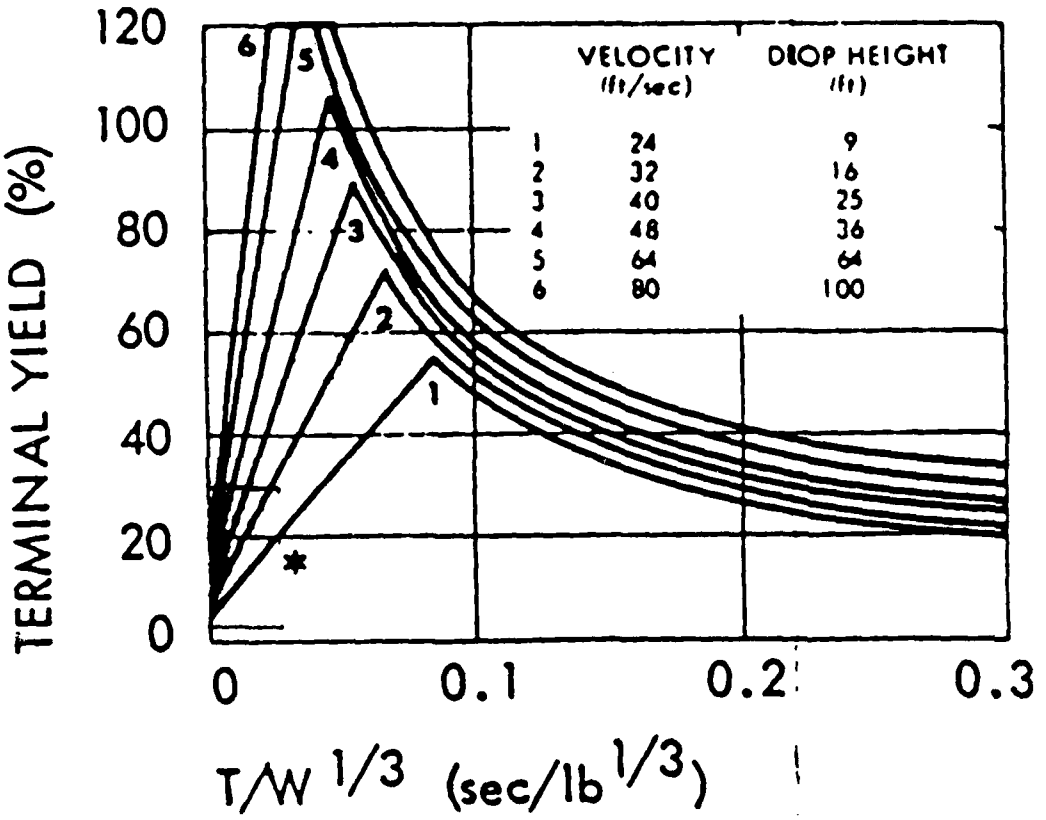


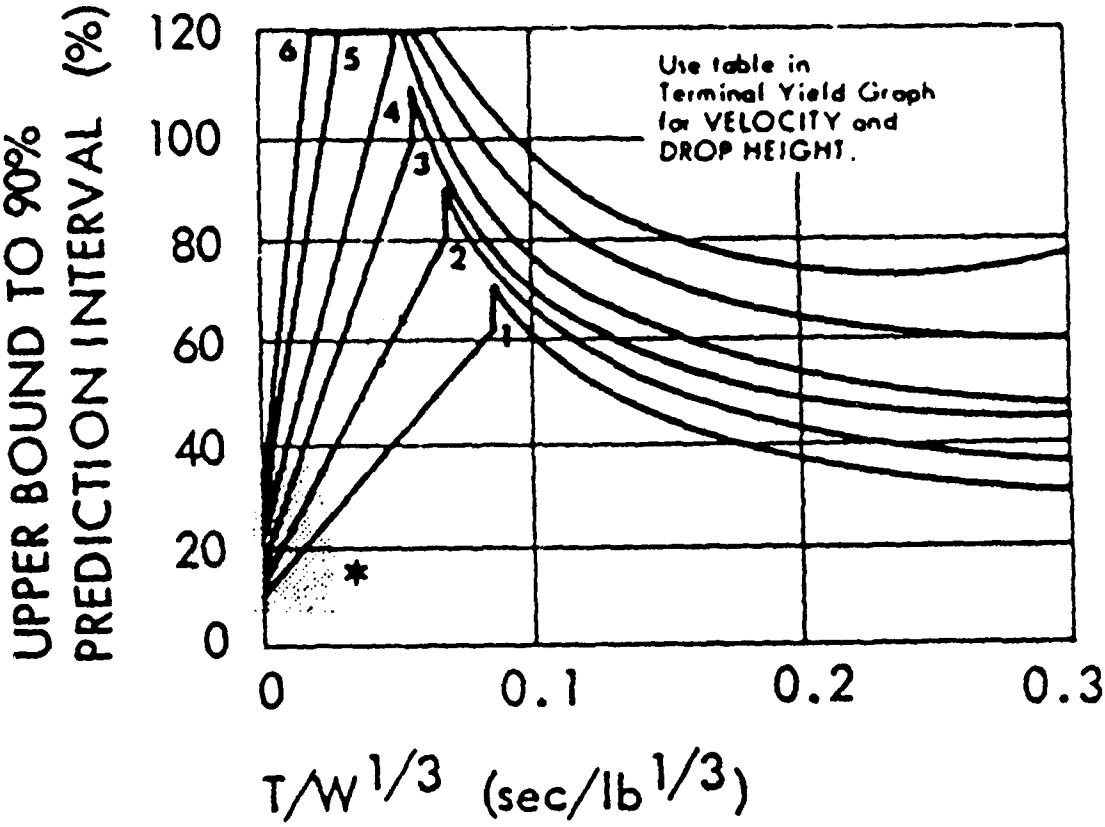
Figure 5-23 LO2/RP-1 CBM Terminal Yield Upper Bound (Y90) vs. T/(W**(1/3)) as a Function of L/D and k (Ref. 9)



* YIELD FOR $T/W^{1/3} = 0$

V (ft/sec)	Y (%)
24	4
32	5
40	6
48	7
64	9
80	12

Figure 5-24 LO2/RP-1 CBGS Terminal Yield (Y) vs. T/(W**(1/3)) (Ref. 9)



*UPPER BOUND VALUE FOR $T/W^{1/3} = 0$

V (ft/sec)	Y_{90} (%)
24	10
32	13
40	15
48	18
64	24
80	29

Figure 5-25 LO2/RP-1 CBGS 90% Terminal Yield (Y90) vs T/(W**(1/3)) (Ref. 9)

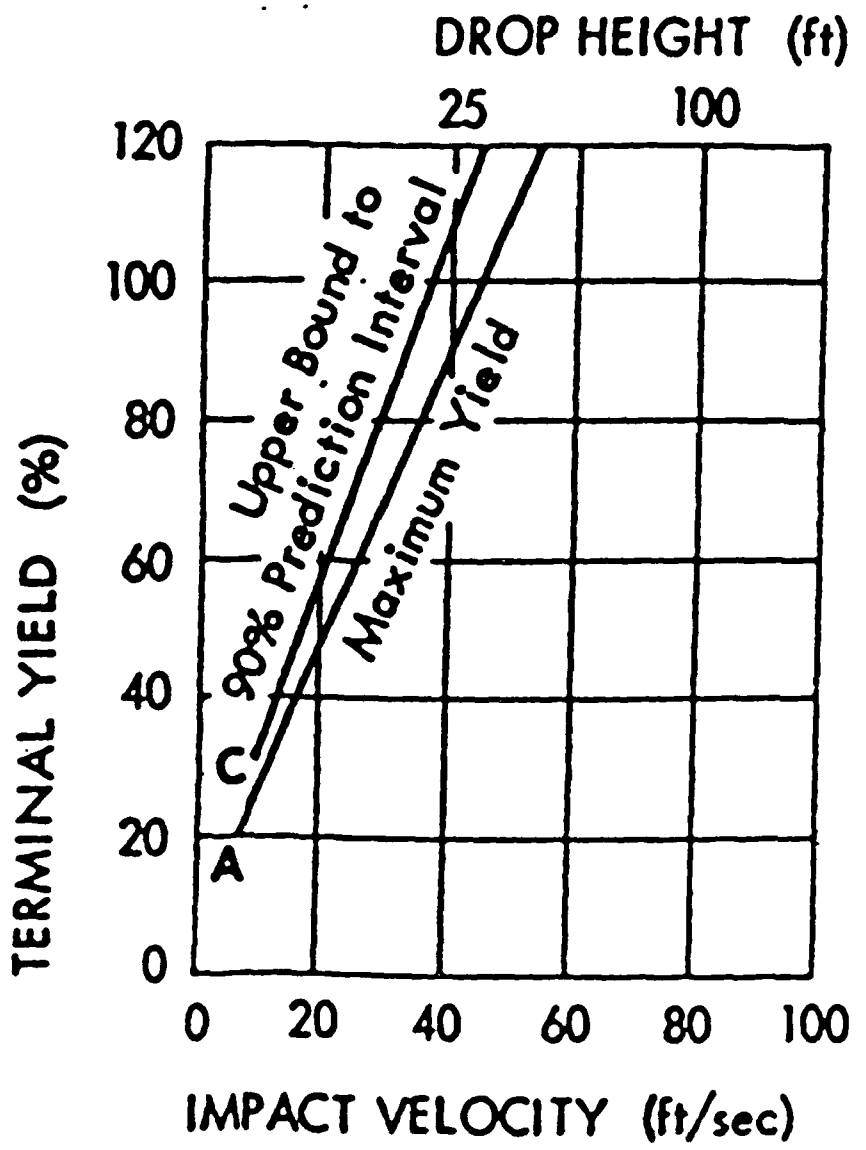


Figure 5-26 LO2/RP-1 CBGS Terminal Yield (Y) vs. Impact Velocity (Ref. 9)

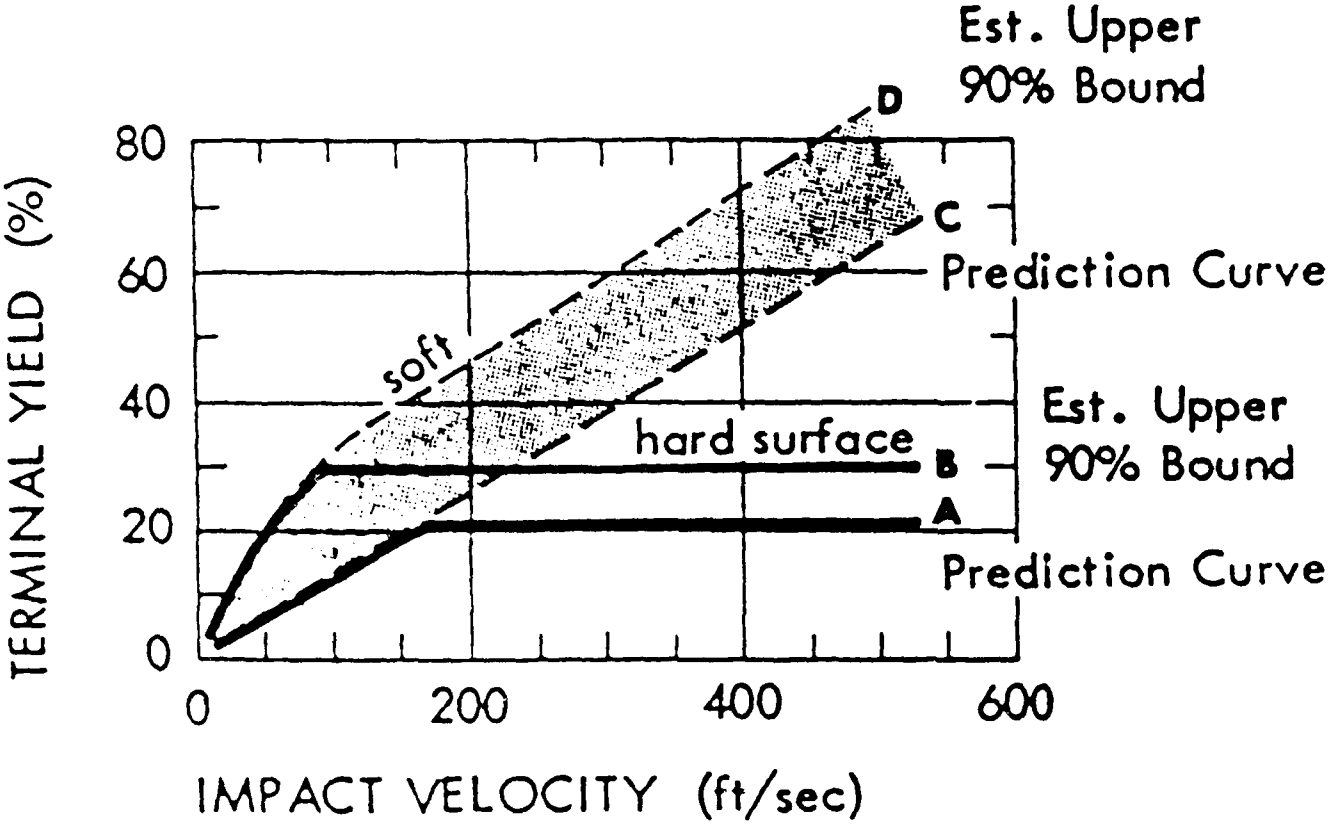


Figure 5-27 Terminal Yield vs Impact Velocity for LO2/RP-1 HVI (Ref 9)

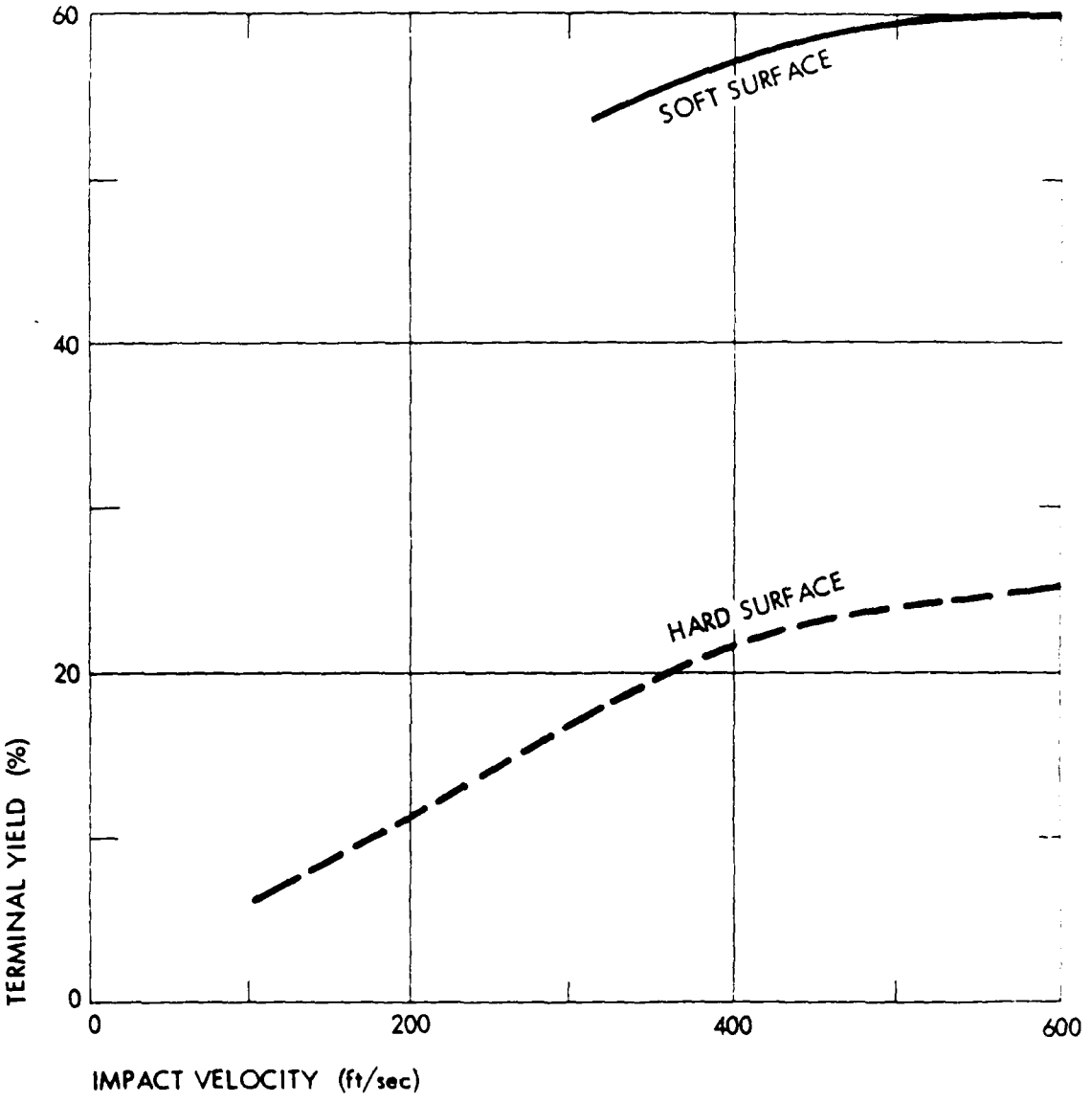


Figure 5-28 Terminal Yield as a Function of Impact Velocity and surface type for hypergolic propellant systems (Ref. 48)

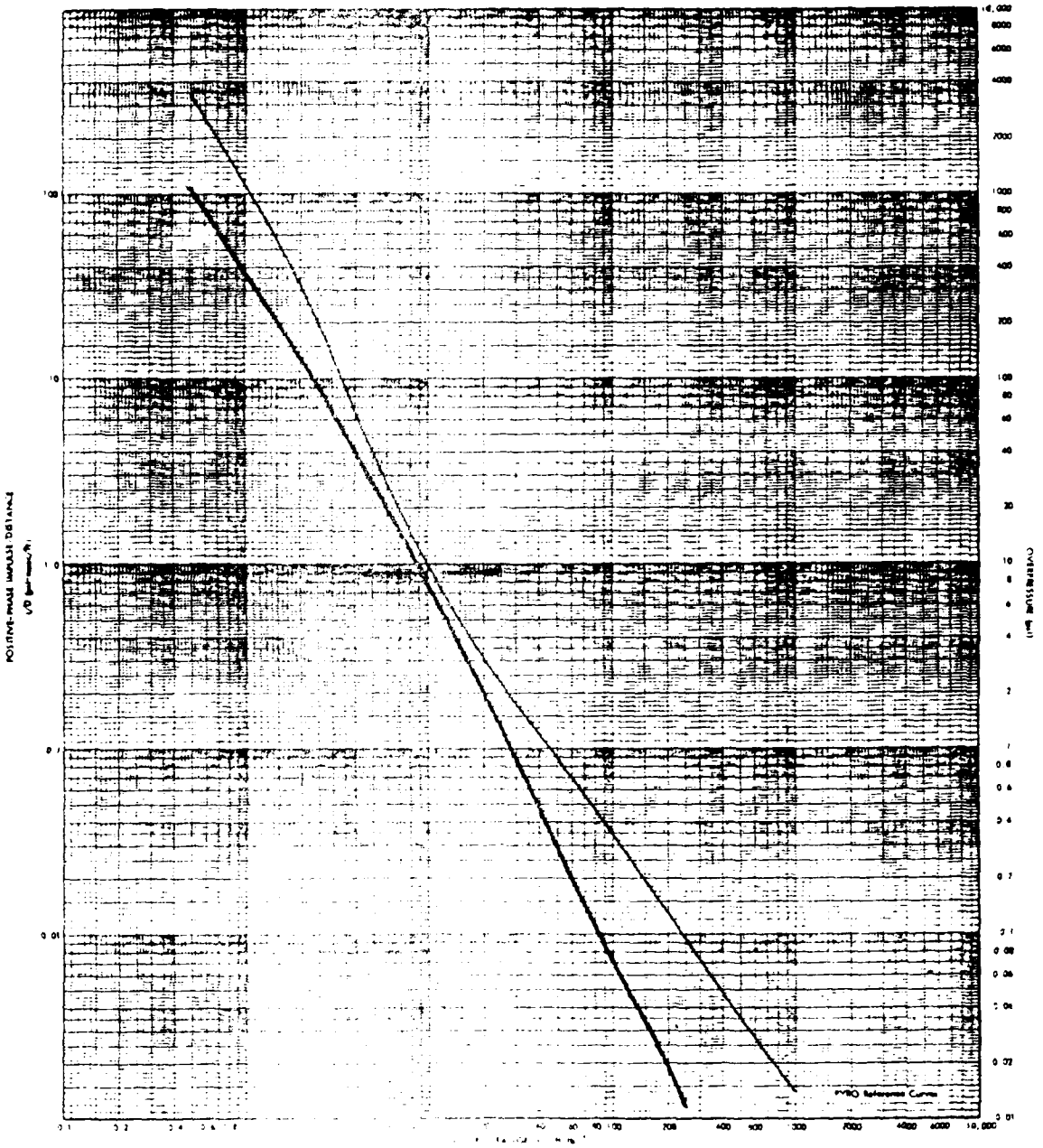


Figure 5-29 [illegible] and Positive-Phase Impulse vs. [illegible] Distance (Lambda) for TNT. (For use with [illegible] Liquid Propellant prediction methods only.)

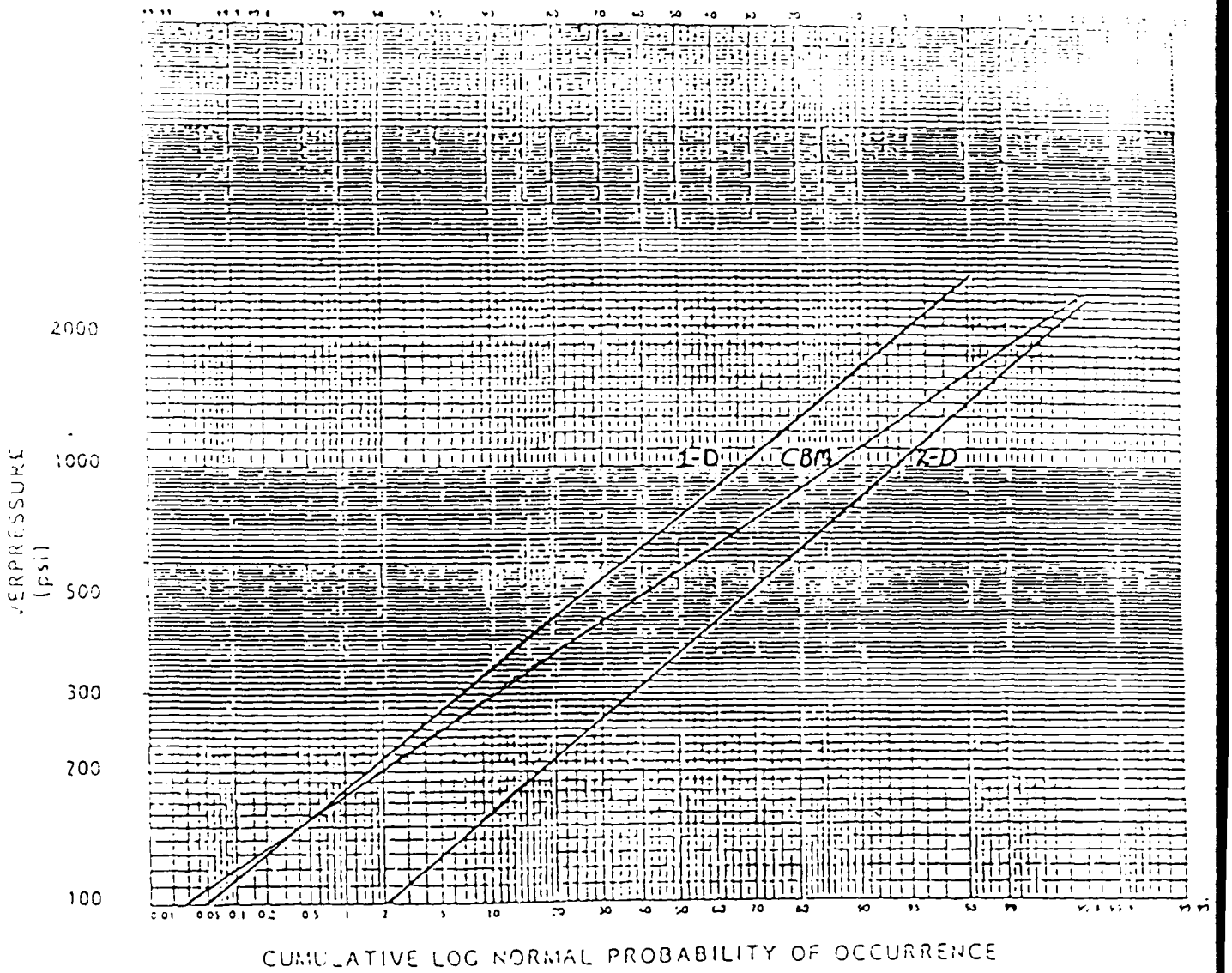


Figure 5-30 Overpressure vs Cumulative Log Normal Probability of Occurrance for Near-Field Distances

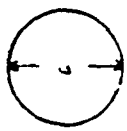
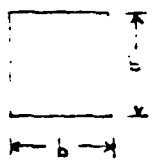
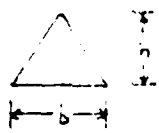
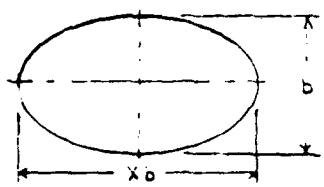
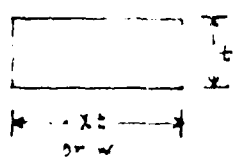
Shape and Characteristic Dimensions	Critical Value of Characterizing Dimensions
Circle 	$d_c = a_c$
Square 	$b_c = a_c$
Equilateral Triangle 	$b_c = \sqrt{3}\, a_c$ or $h_c = \frac{3}{2} a_c$
Ellipse 	$b_c = \dfrac{\int_0^{\pi/2} \sqrt{1 - \frac{x^2-1}{x^2} \sin^2\phi}\; d\phi}{x}$ $b_{c\infty} = \lim_{x\to\infty} b_c = \dfrac{a_c}{\pi}$
Rectangle  Where $x > 1$	$t_c = \left(\frac{x+1}{2x}\right) a_c$ $t_{c\infty} = \lim_{x\to\infty} t_c = \frac{a_c}{2}$ or, if w is fixed $t_c = \dfrac{w\, a_c}{2w - a_c}$

Figure 5-31 Geometry vs Critical Value adjustment to the Critical diameter.

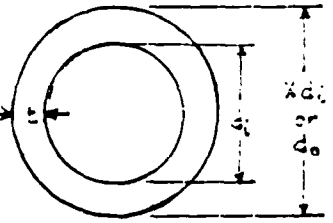
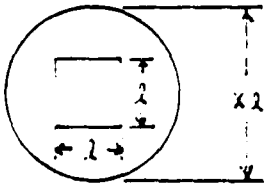
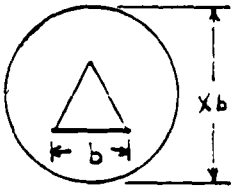
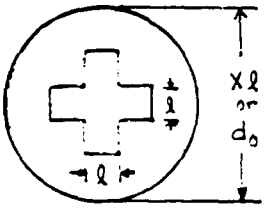
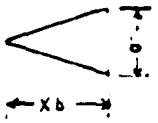
Shape and Characteristic Dimensions	Critical Value of Characteristic Dimensions
Circular Core  Where $x > 1$	$d_{i_c} = \left(\frac{1}{x-1}\right) d_c$ or $t_c = \frac{d_c}{2}$ or, if d_i is fixed $d_{o_c} = d_i + d_c$
Square Core  	$\ell_c = \left(\frac{\pi x + 4}{\pi x^2 - 4}\right) d_c$
Equilateral Triangle Core  	$b_c = \left(\frac{\pi x + 3}{\pi x^2 - \sqrt{3}}\right) d_c$
Cross Core  where $x > 1$	$\ell_c = \left(\frac{\pi x + 12}{\pi x^2 - 20}\right) d_c$ or, if ℓ is fixed $d_{o_c} = \frac{d_c}{2}\left[\sqrt{1 + \frac{16\ell}{\pi d_c}\left(6\frac{\ell}{d_c} + 3\right)} + 1\right]$
Isosceles Triangle  Where $x > 1$	$b_c = \sqrt{\frac{2x+1}{2x-1}}\, d_c$ $b_{c_\infty} = \lim_{x \to \infty} b_c = 1.$

Figure 5-32 Geometry vs Critical Value adjustment to the Critical diameter (continued.)

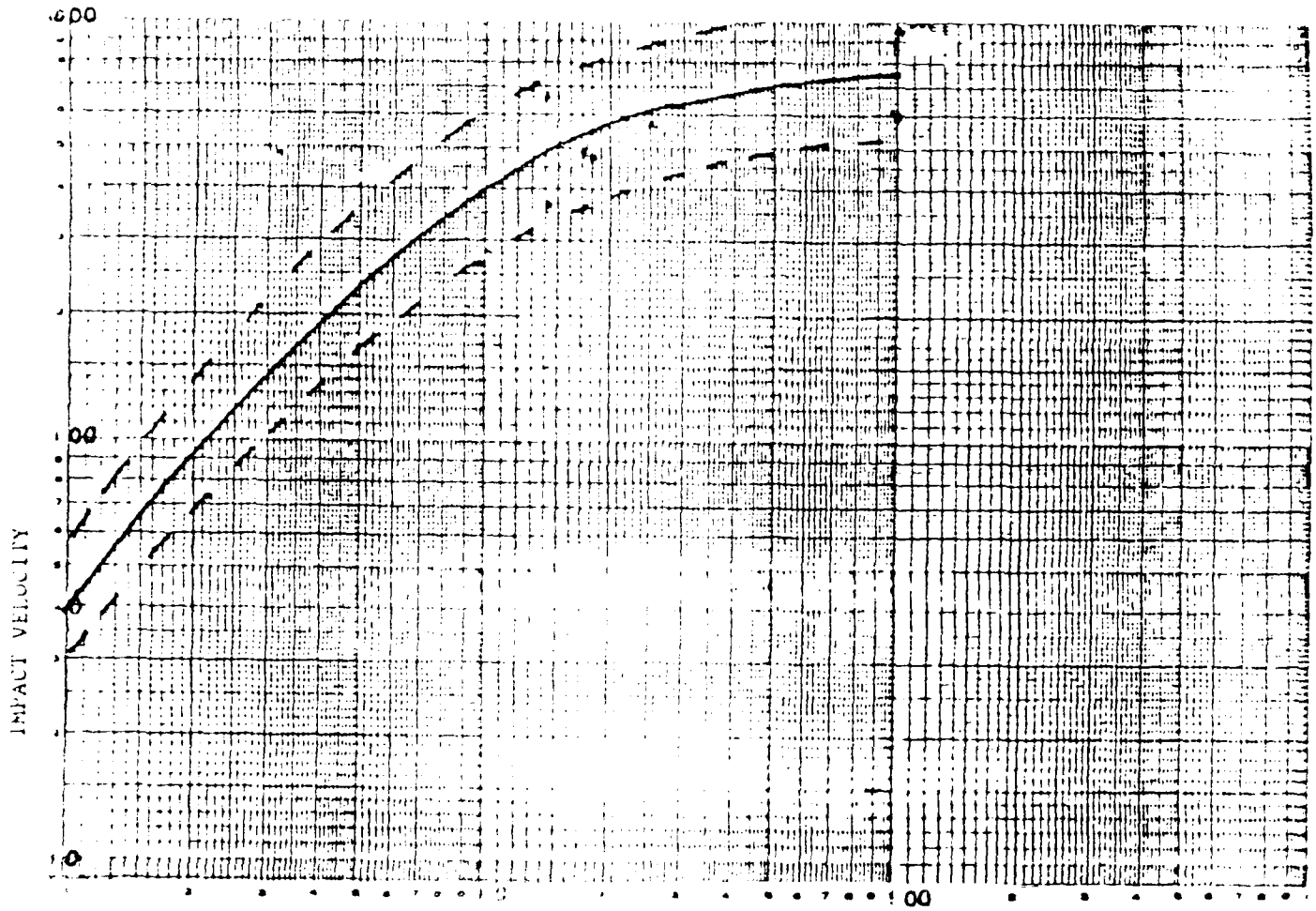


Figure [illegible] Impact Velocity vs TNT % Equivalent For Solid Rocket Motors Showing the Upper and Lower bounds.

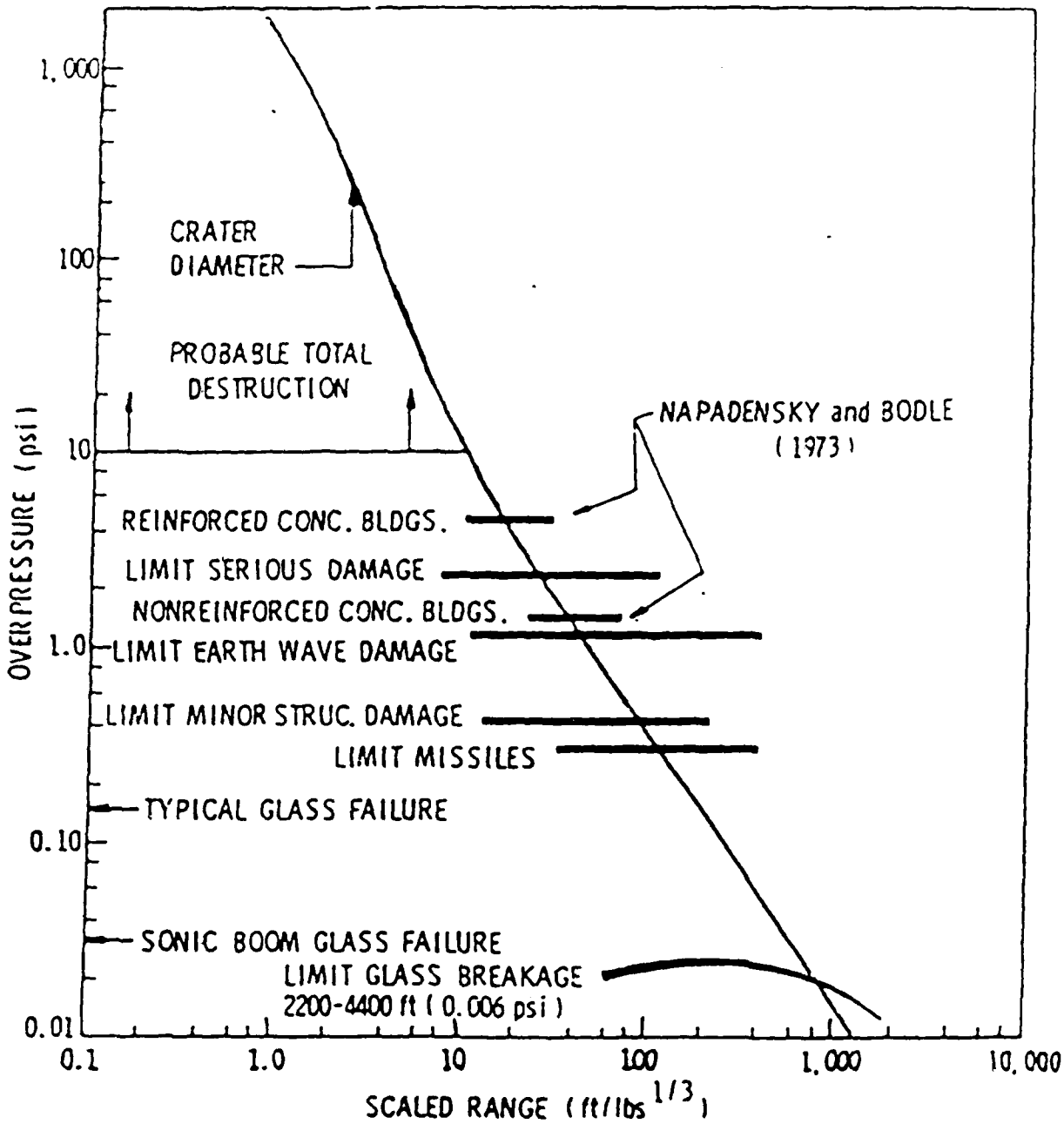


Figure 5-34 Overpressure vs Scaled Distance (Lambda) for TNT Indicating Levels of Blast Damage (For Use With Solid Propellant Prediction Methods Only.) (Ref. 1)

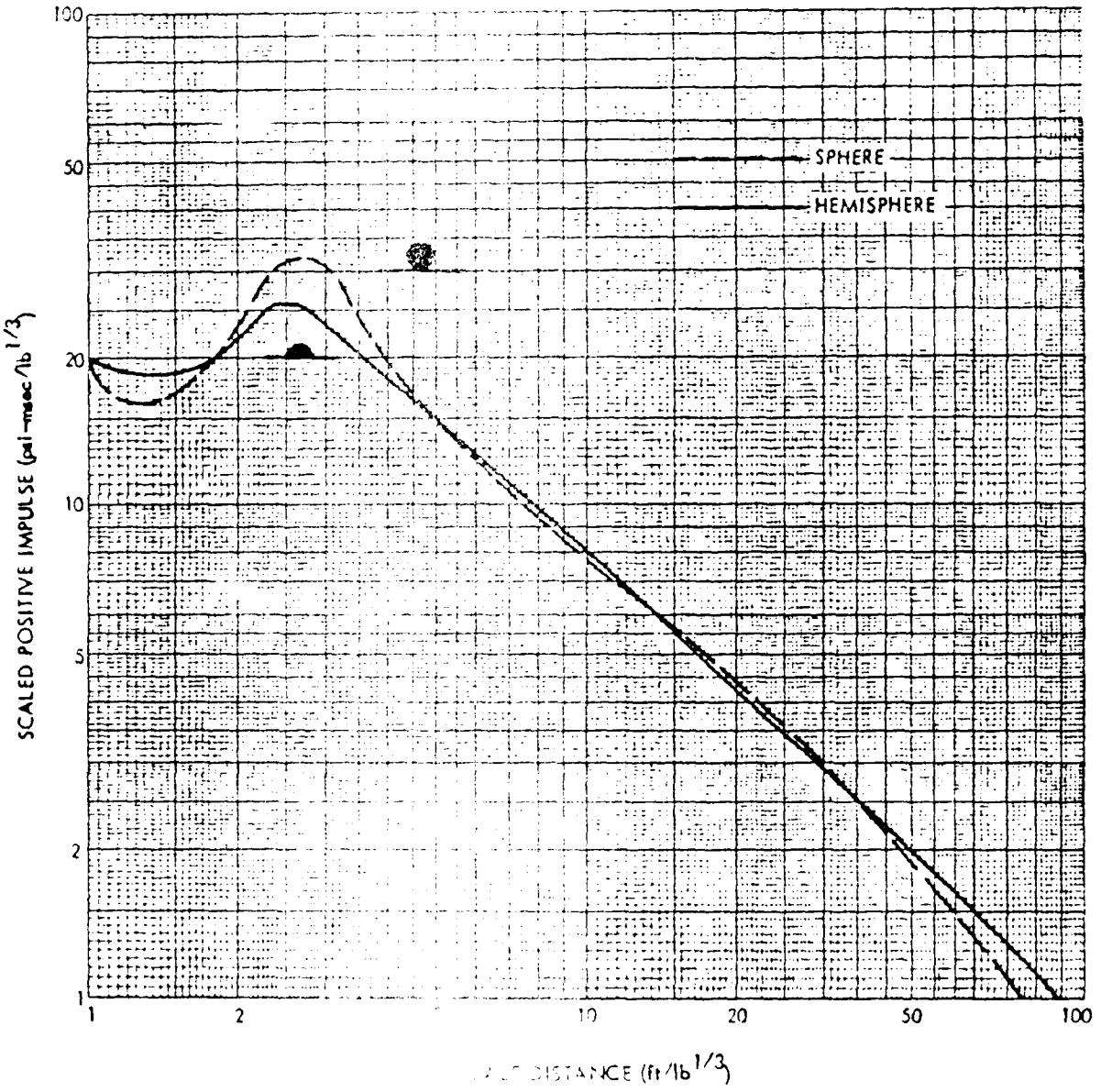


Figure 5-35 Positive [illegible] Scaled Distance (Lambda) for Hemispherical and Spherical TNT Charges located on the ground surface. (Ref. [illegible])

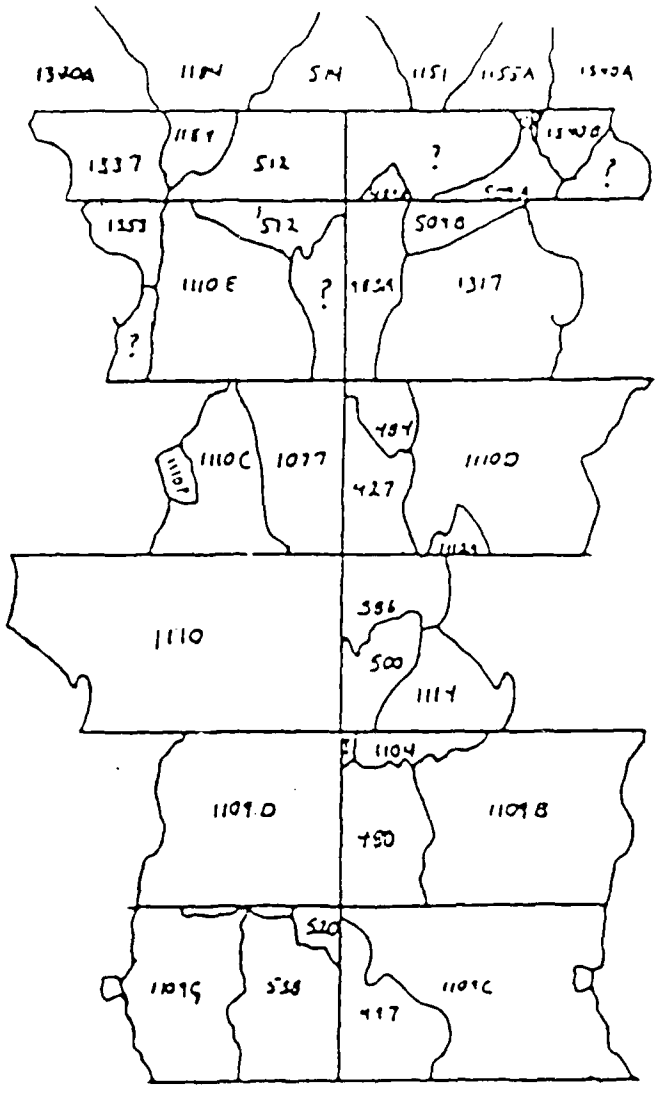


Figure 5-36 Titan 34D-9 Mishap. SRM1 Fragmentation Pattern. (Note straight vertical break - this is where the destruct charge cut the motor open.) Ref. LASP Subpanel Review.

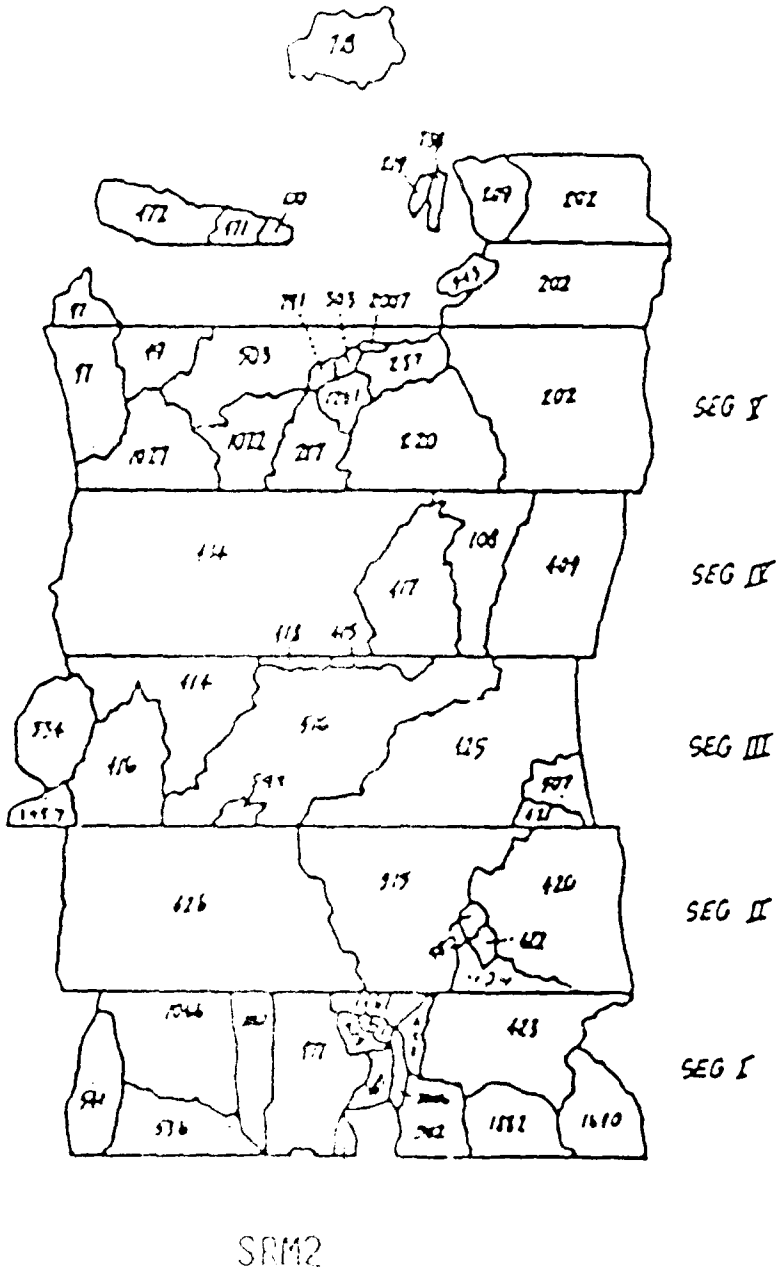


Figure 5-37 Titan 34D-9 Mishap. SRM2 Fragmentation Pattern. Ref. LASP Subpanel Review.

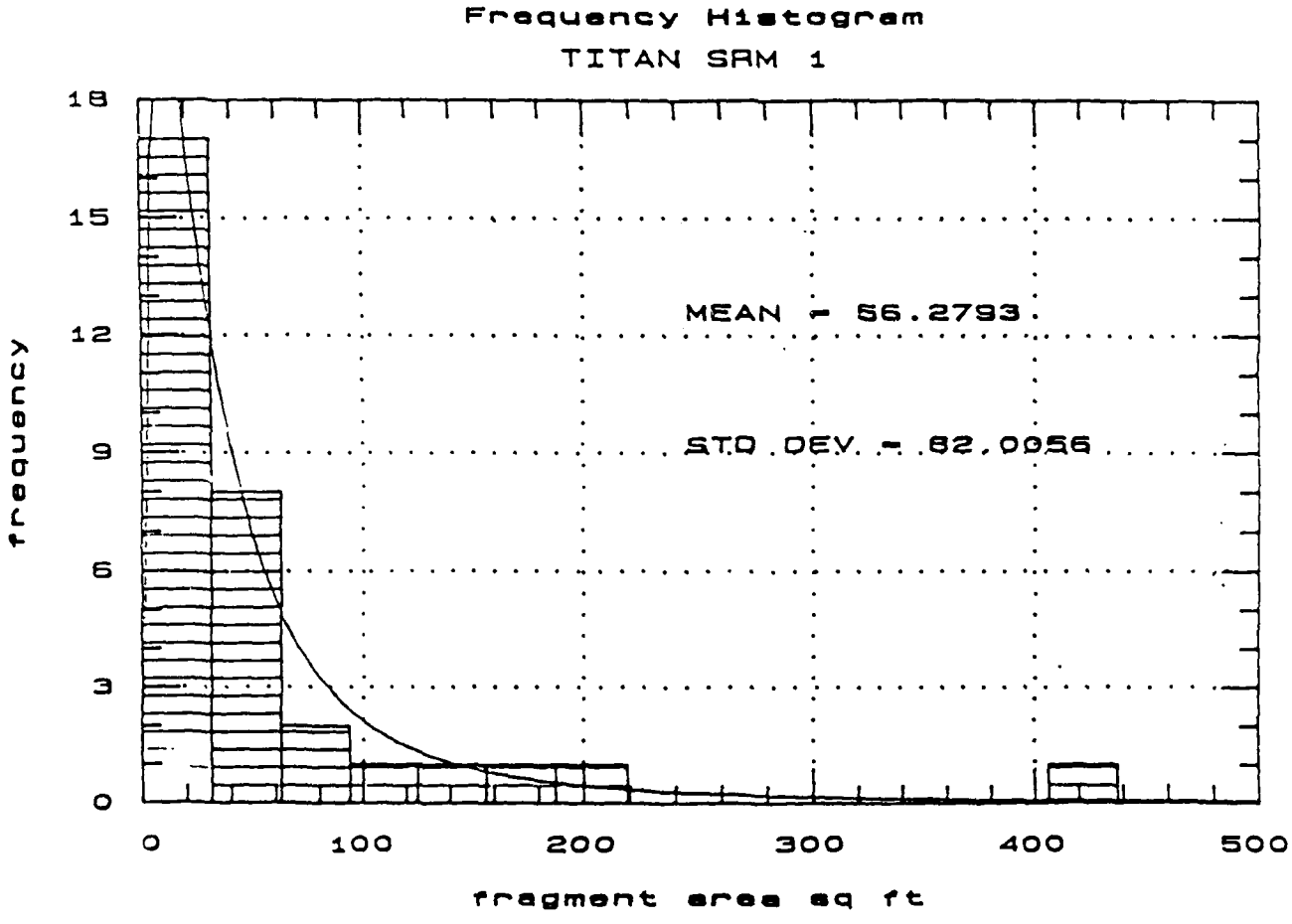


Figure 5-38 Titan 34D-9 Mishap. SRM1 Frequency vs Fragment Area. Ref. LASP Subpanel Review.

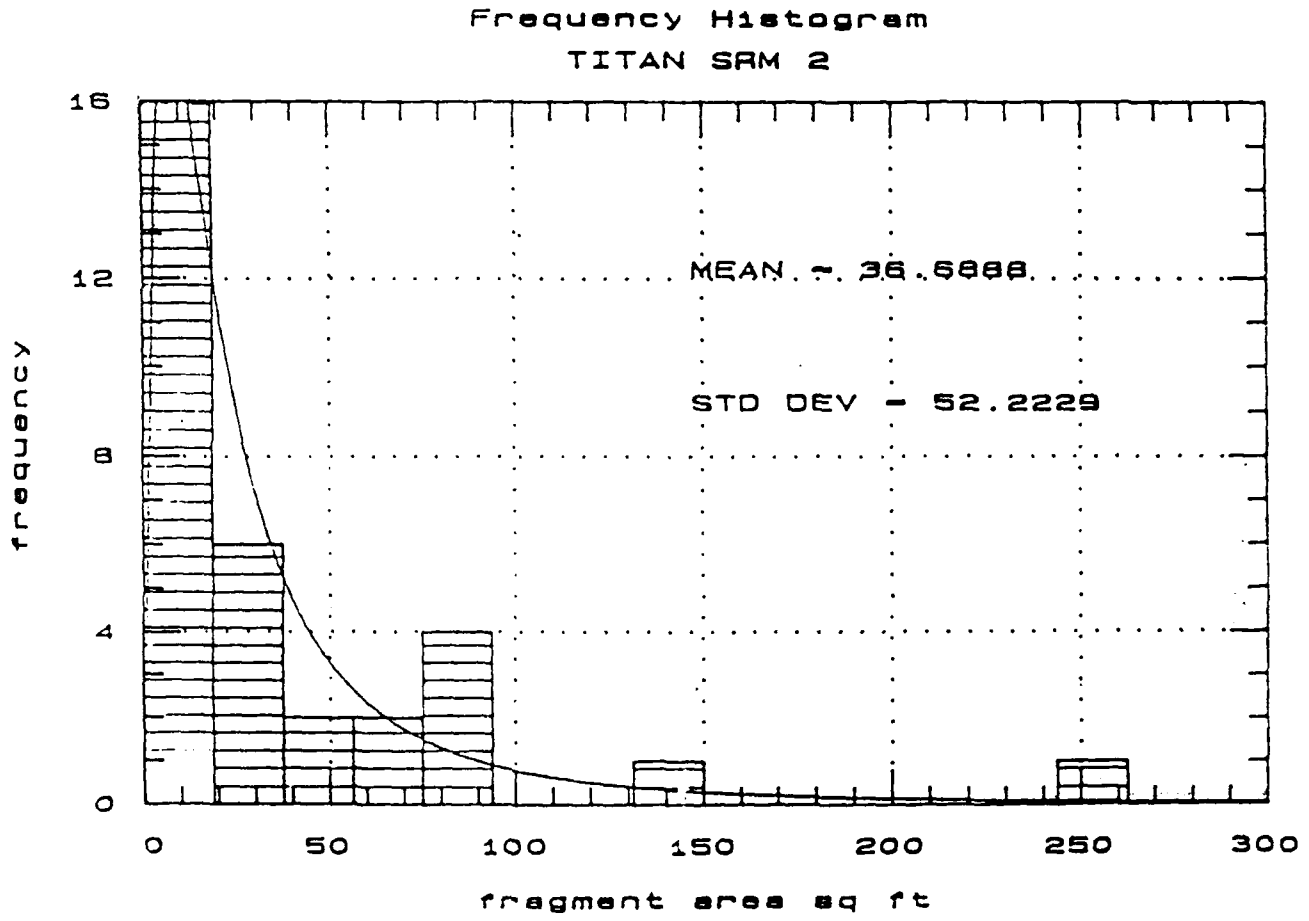


Figure 5-39 Titan 34D-9 Mishap. SRM2 Frequency vs Fragment Area. Ref. LASP Subpanel Review.

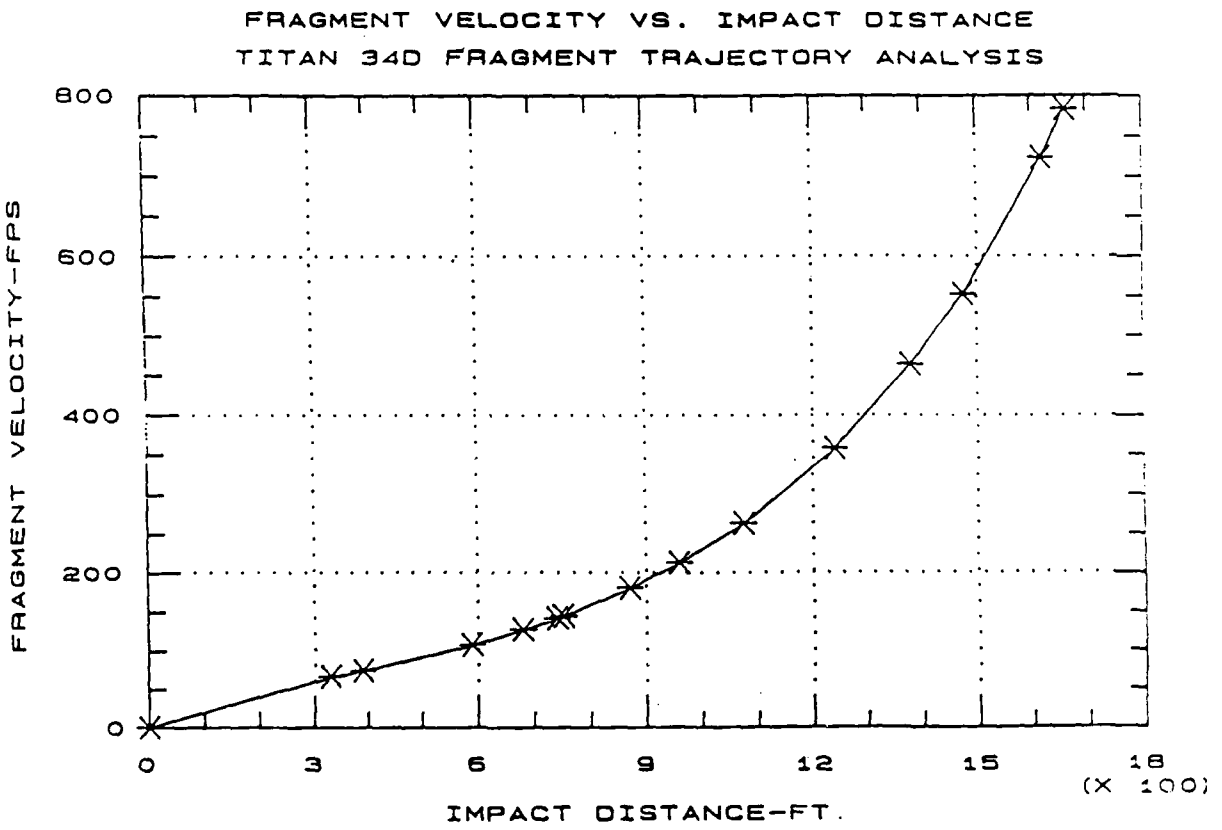


Figure 5-40 Titan 34D-9 Mishap. Fragment Velocity vs Impact Distance. Ref. LASP Subpanel Review.

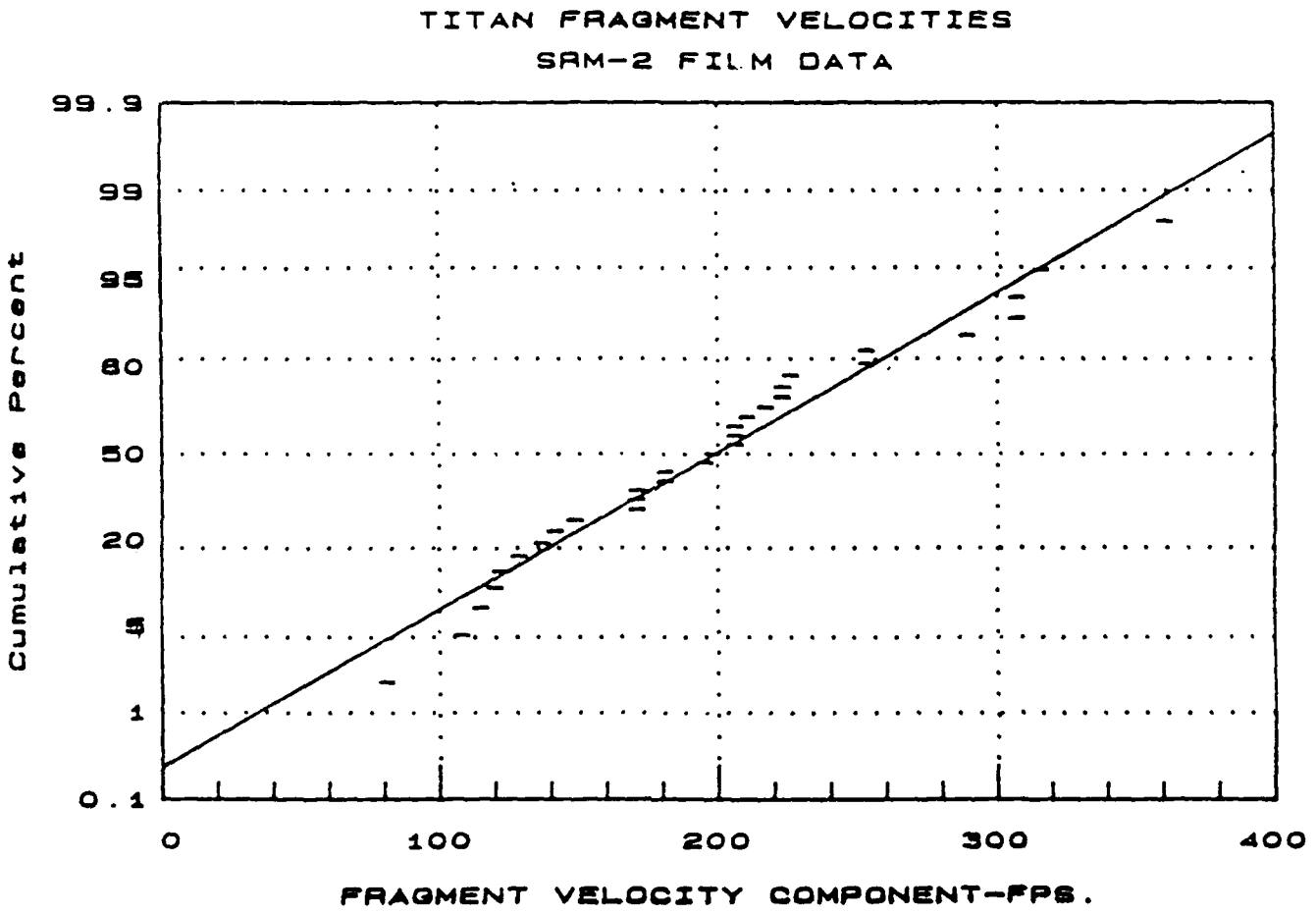
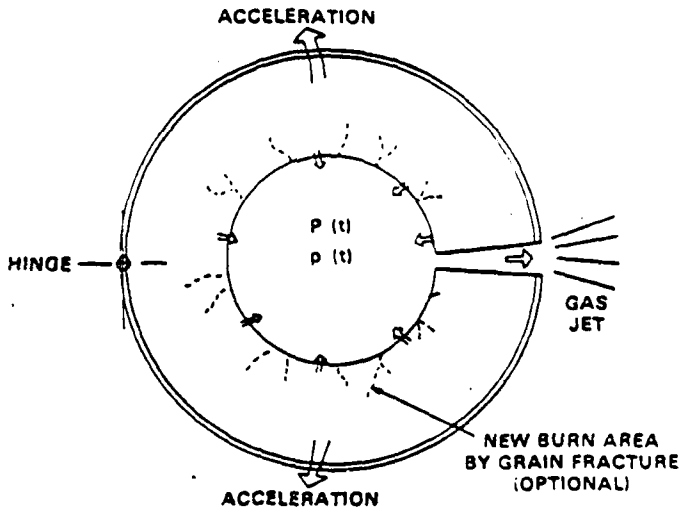


Figure 5-41 Titan 34D-9 Mishap. Cummulative Percent vs Fragment Velocity. Ref. LASP Subpanel Review.



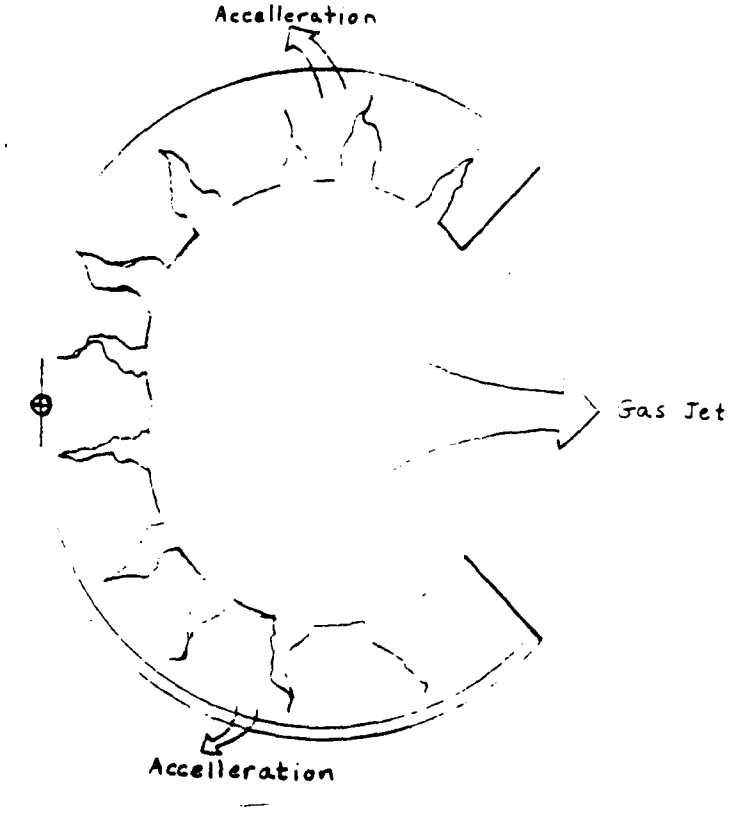


Figure 5-42 "Clamshell" Opening of a SRM Case After Command Destruct.

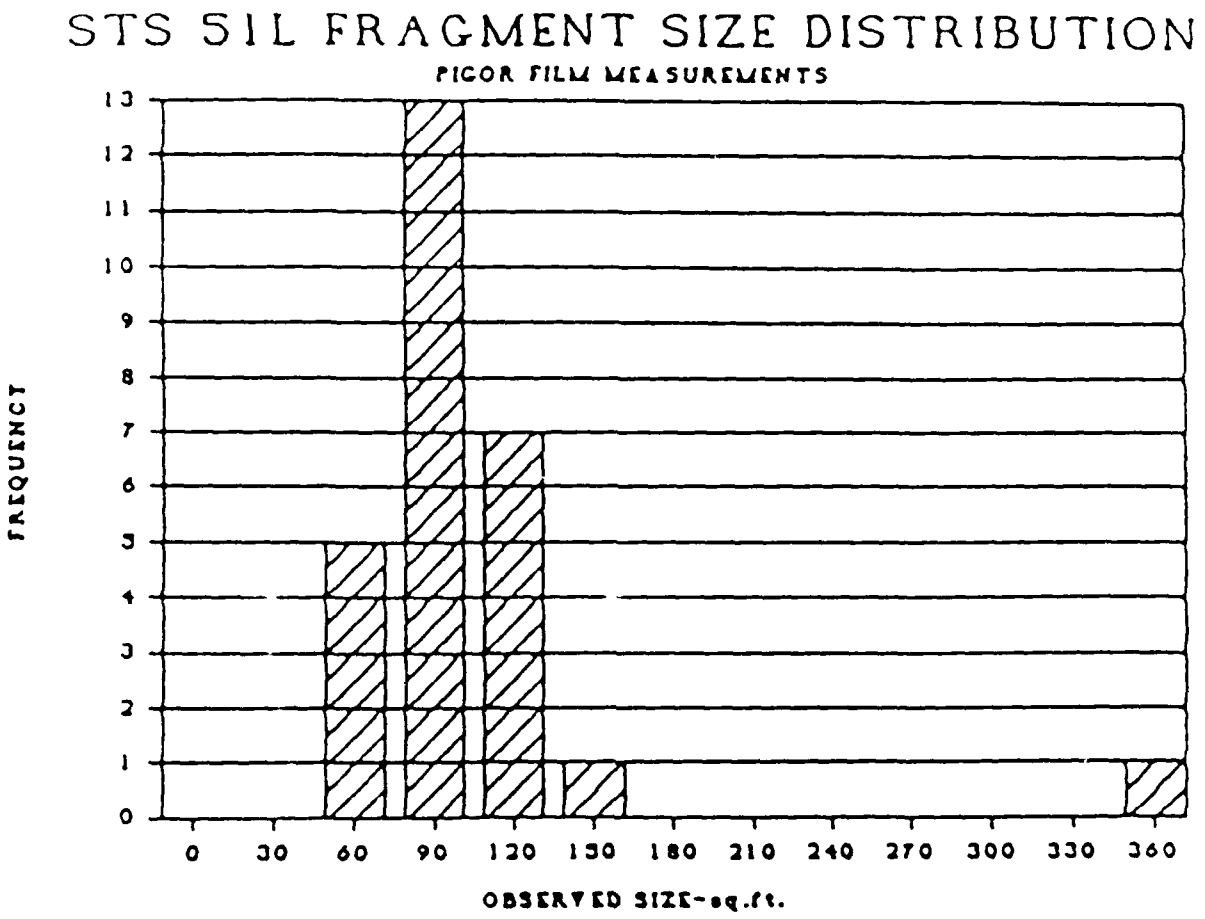


Figure 5-43 STS 51-L Mishap, SRB Fragment Size Distribution
Ref. Space Shuttle Data Book Rev A, NSTS08116.

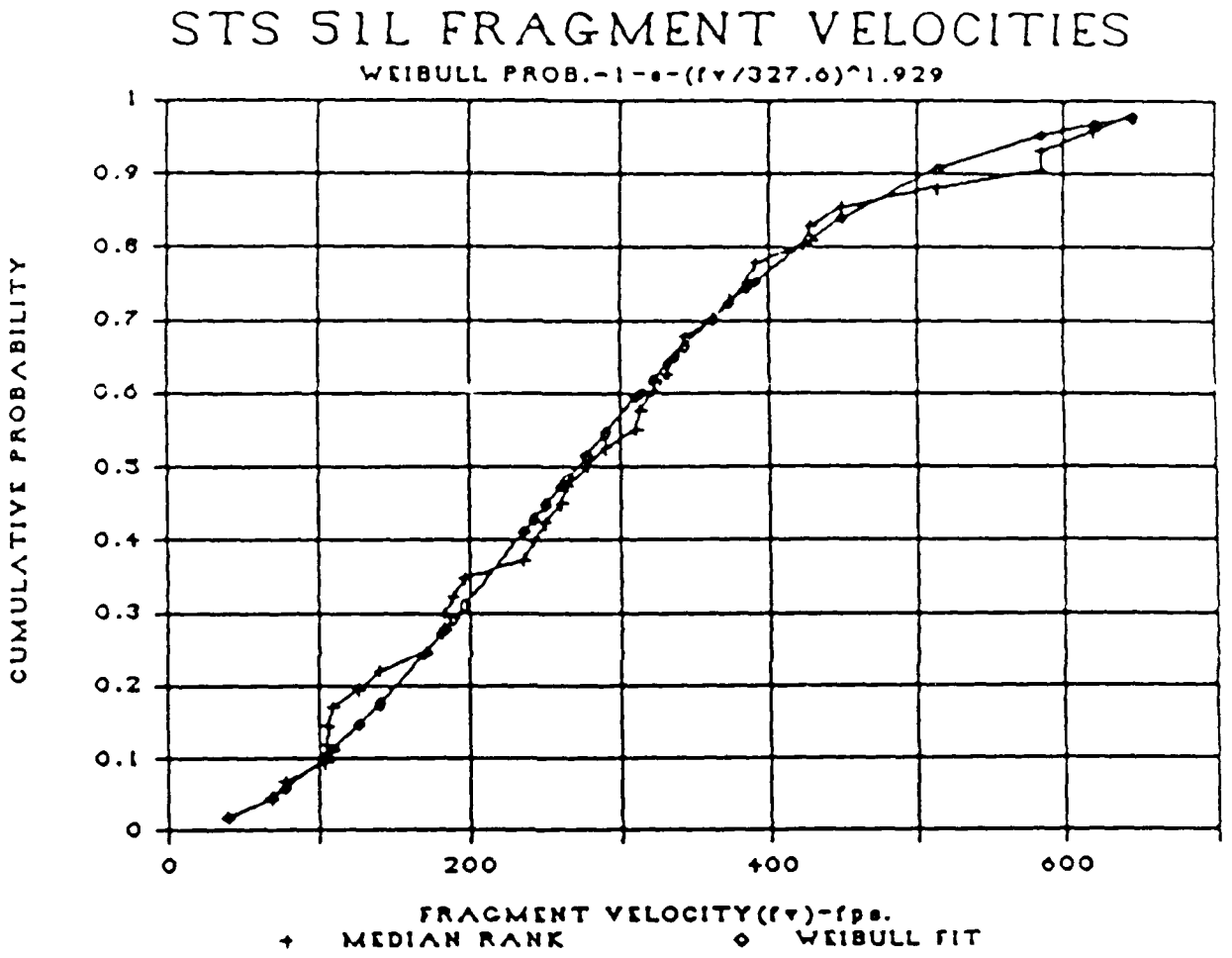


Figure 5-44 STS 51-L Mishap. SRB Fragment Velocity Distribution
Ref. Space Shuttle Data Book, Rev A, NSTS 08116

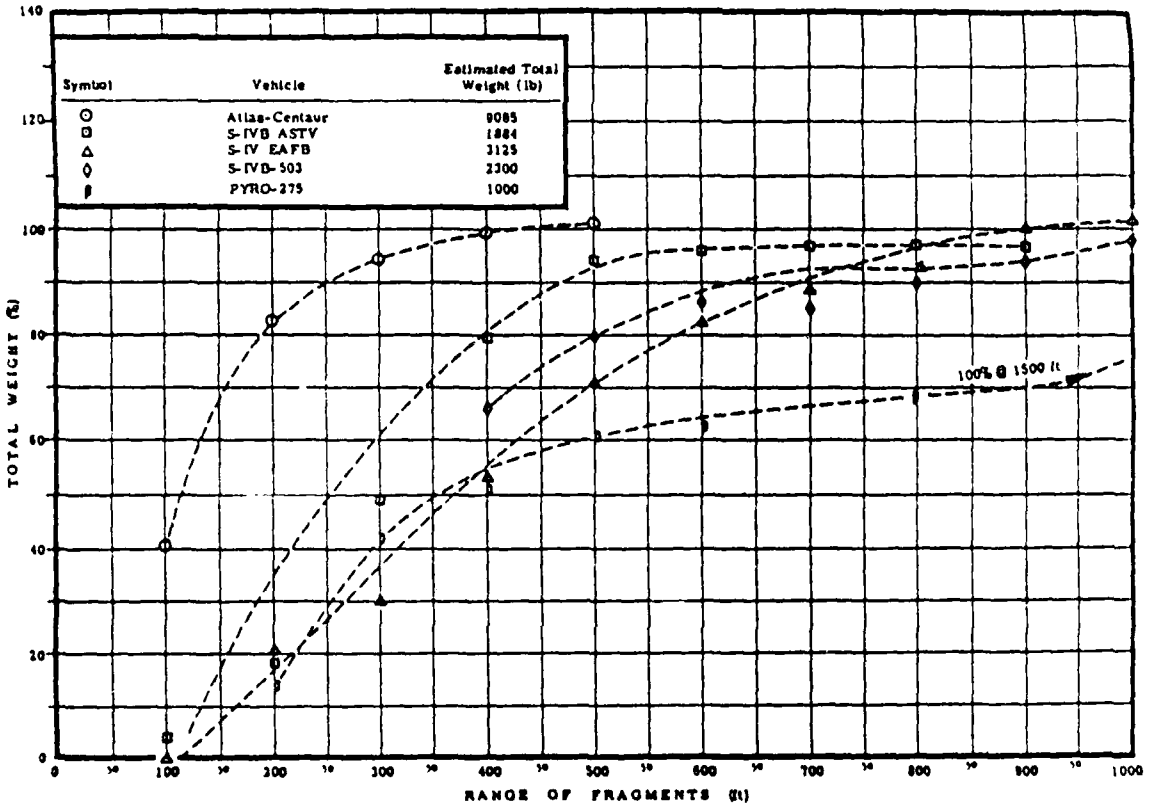


Figure 5-45 Percentage of Total Weight of Vehicle Fragments within Range Indicated. (Ref. 1)

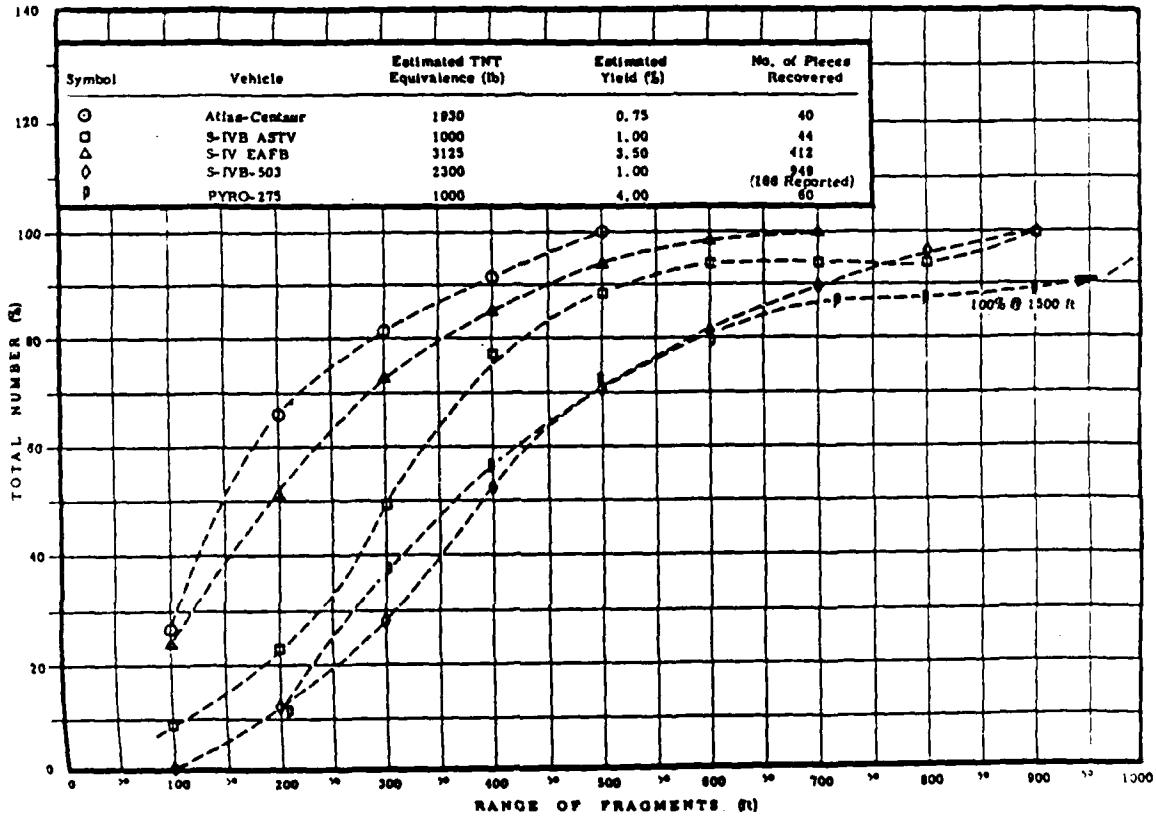


Figure 5-46 Fragment Number and Weight Distributions. (Ref. 1)

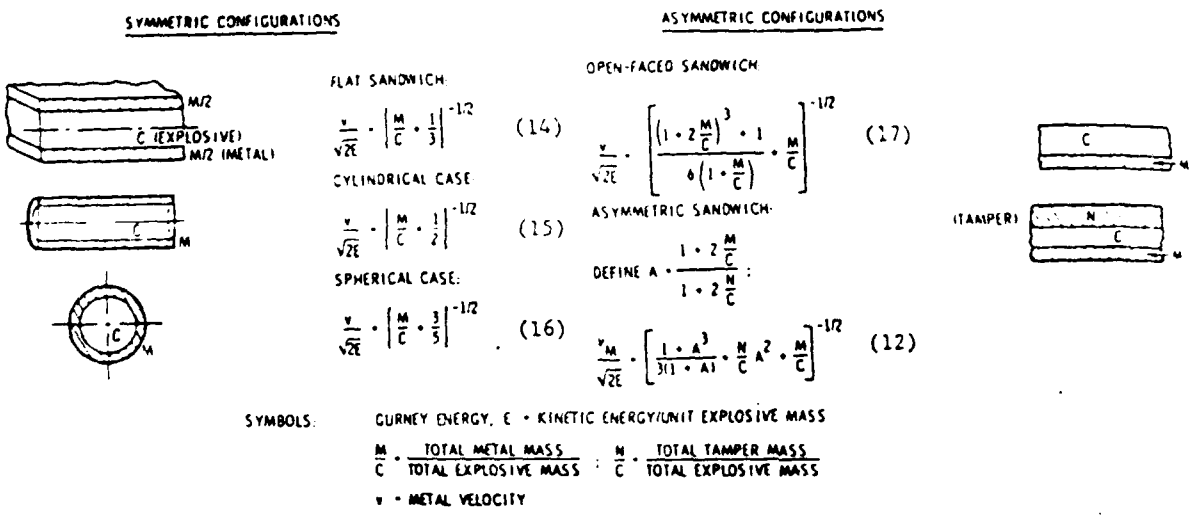


Figure 5.47: Gurney Equations for Simple Geometries. (Ref. 1)

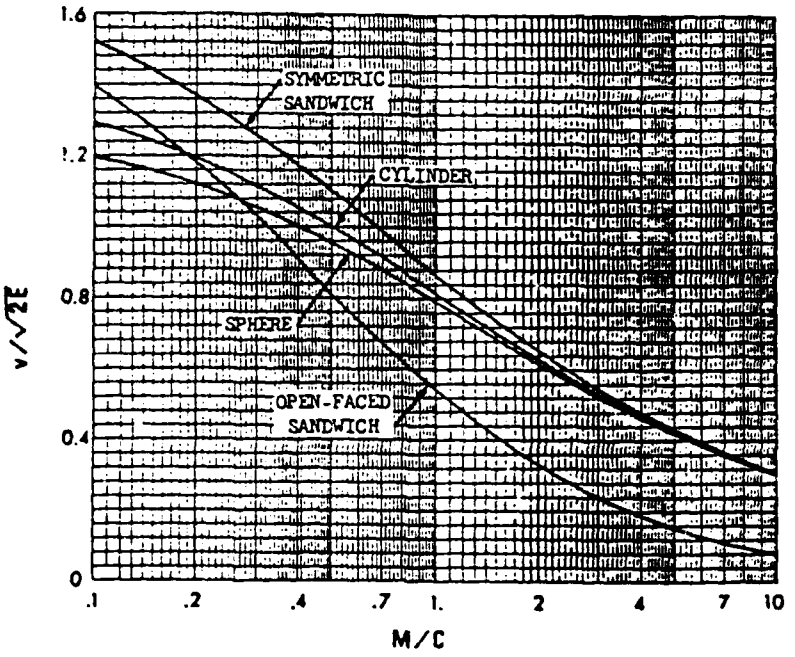


Figure 5-48 Dimensionless Velocity of Metal as a Function of Loading Factor M/C. (Ref. 1)

From: Jacobs, S. J., "The Gurney Formula" variation on a theme by LaGrange, NOLTR 74086, June 1974

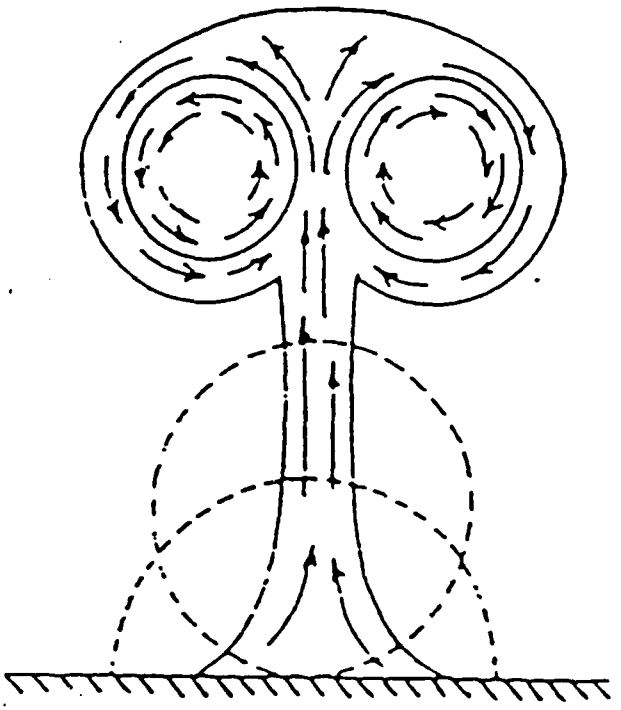


Figure 5-49 Typical Fireball Development

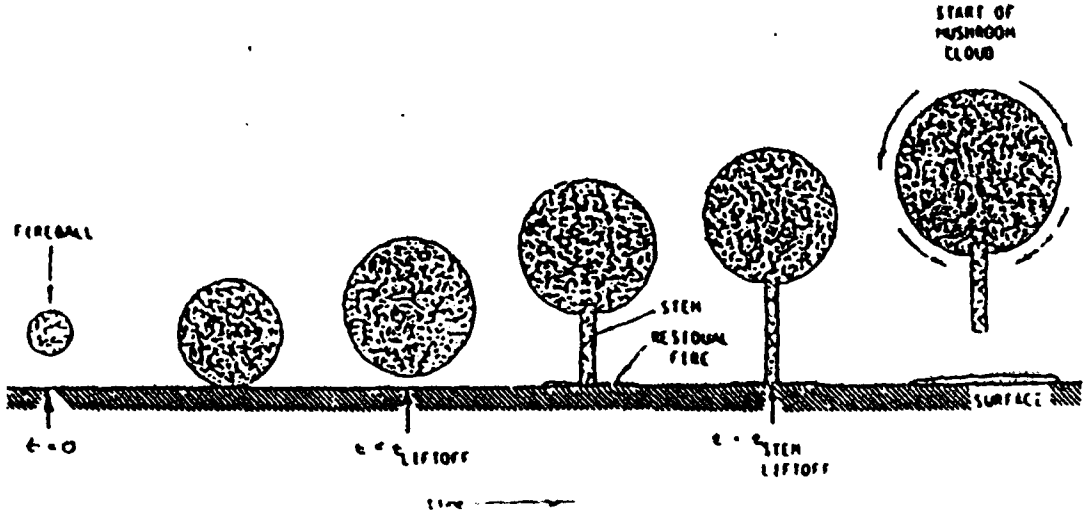


Figure 5-50 Fireball Development (Liquids)

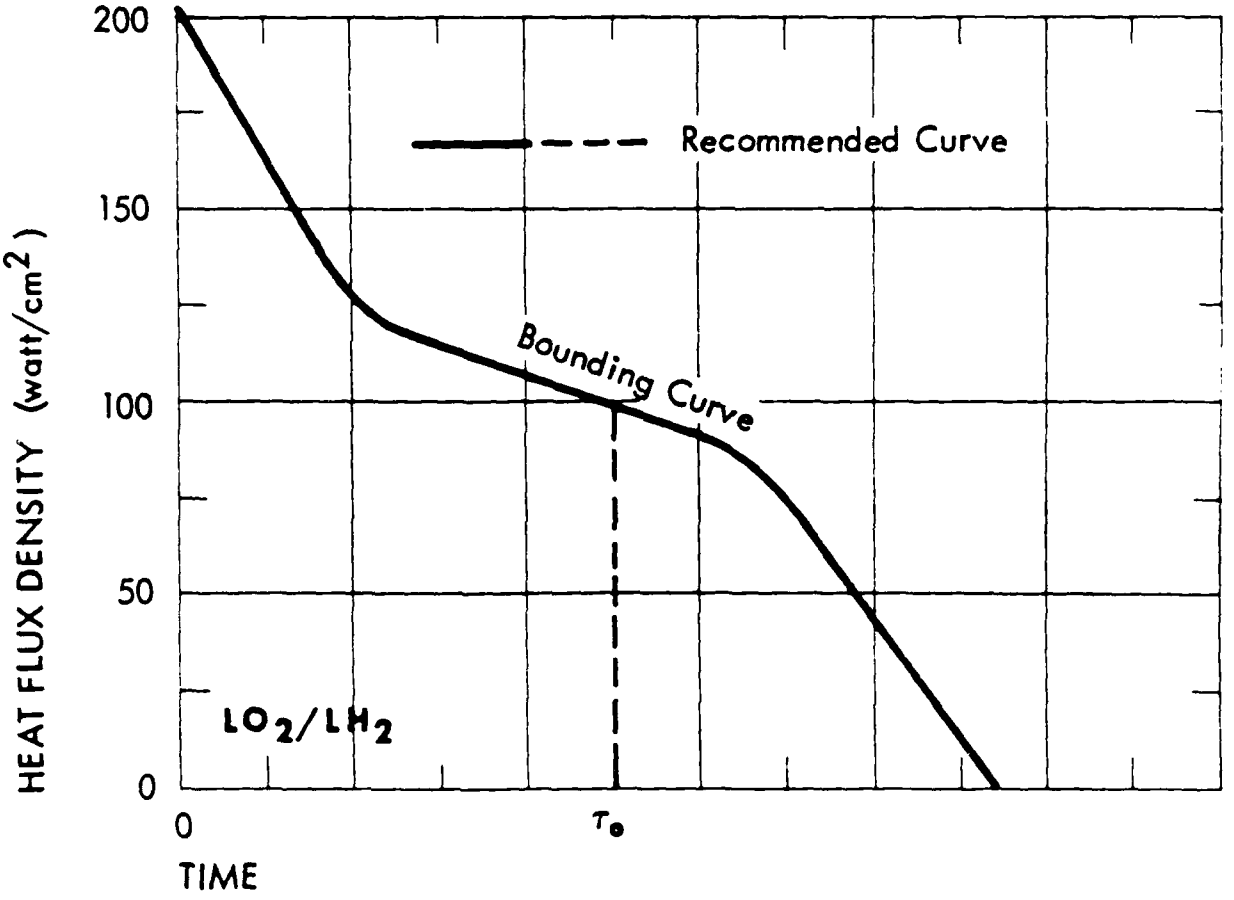


Figure 5-51 Heat flux vs dimensionless time for LO2/LH2

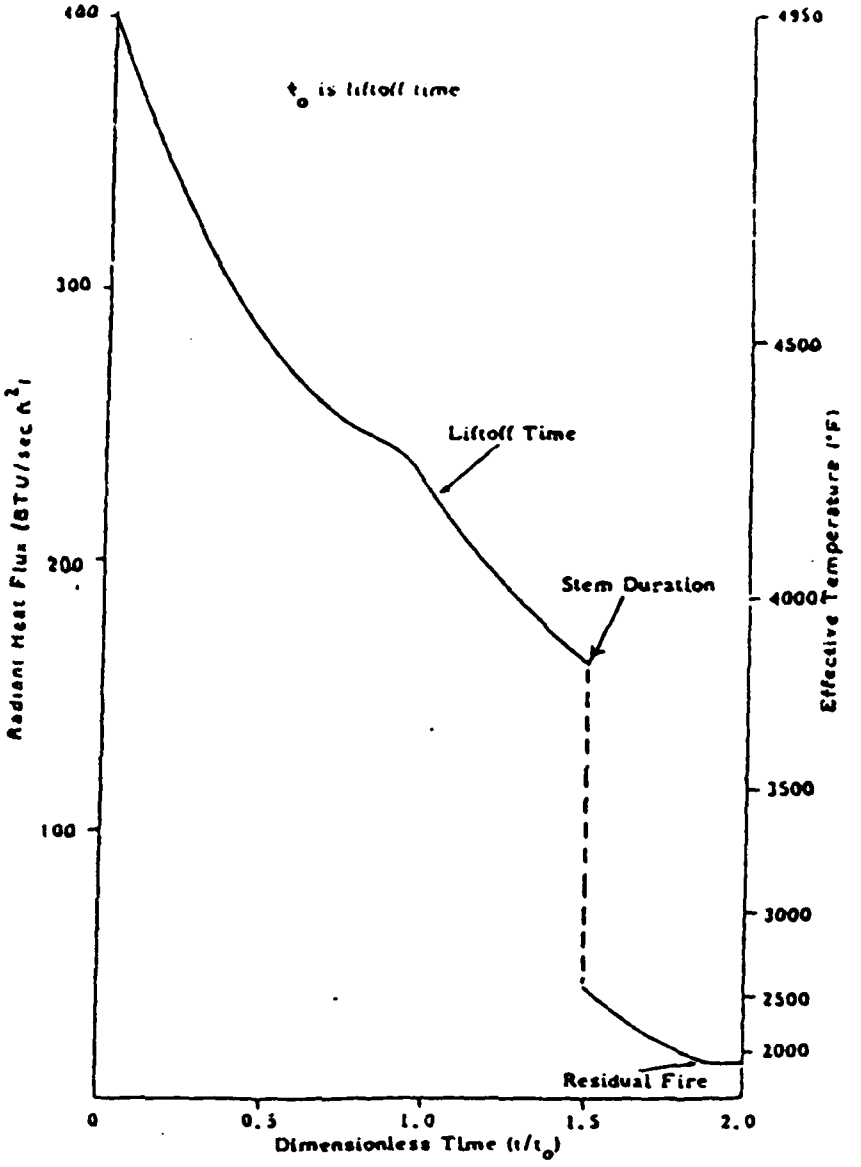


Figure 5-52 Heat flux and Temperature vs dimensionless time for LO2/RP-1

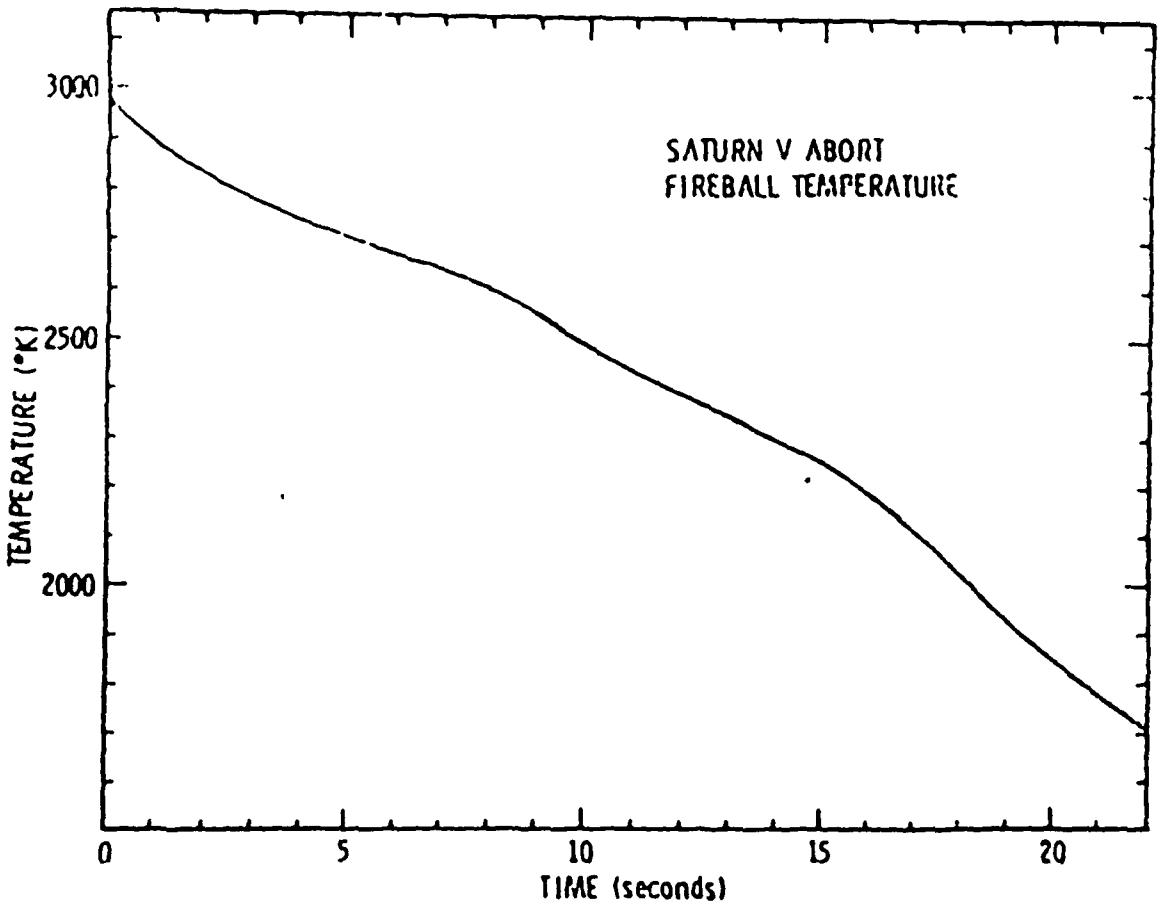


Figure 5-53 Fireball Temperature vs Time for a Saturn V abort (LO2/RP-1)

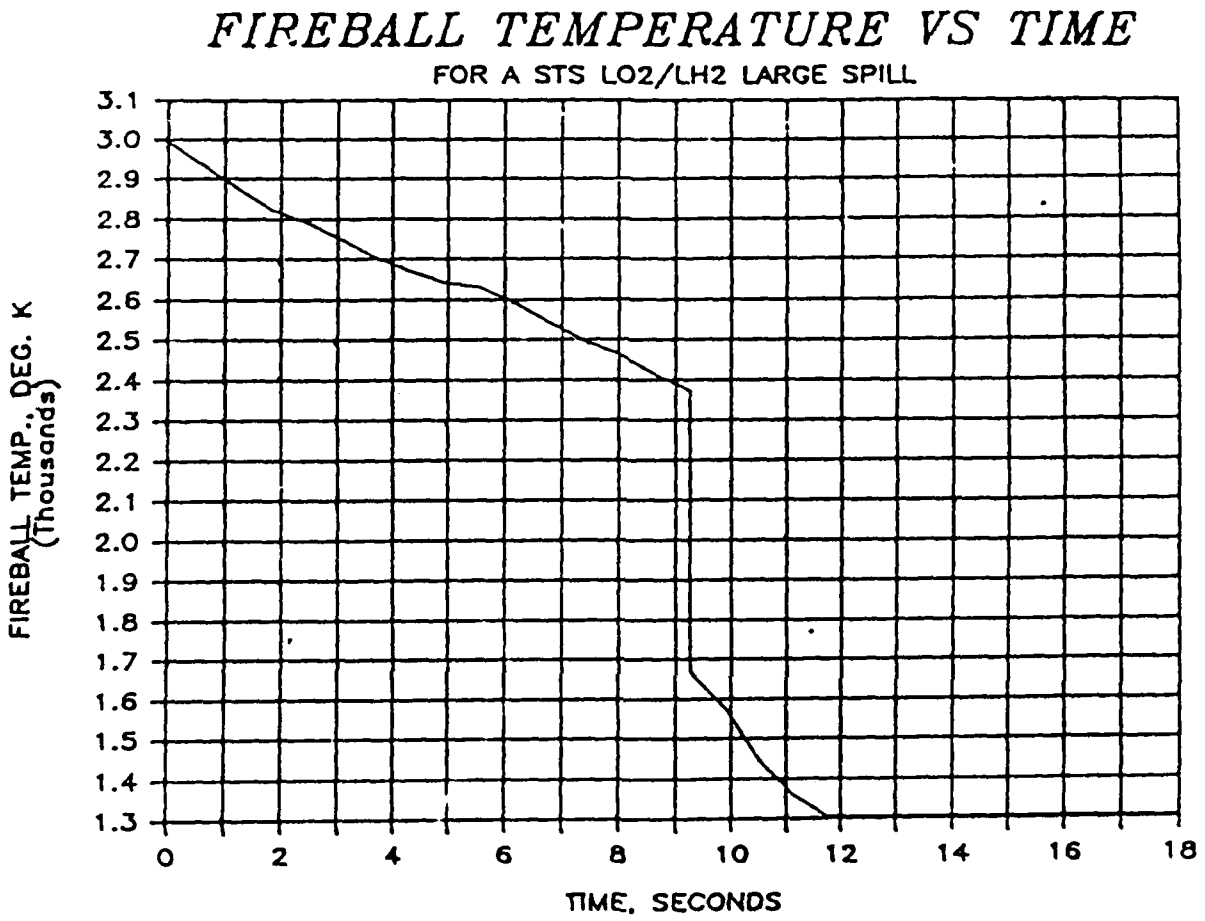


Figure 5-54 Temperature vs Time for LO2/LH2 example problem.

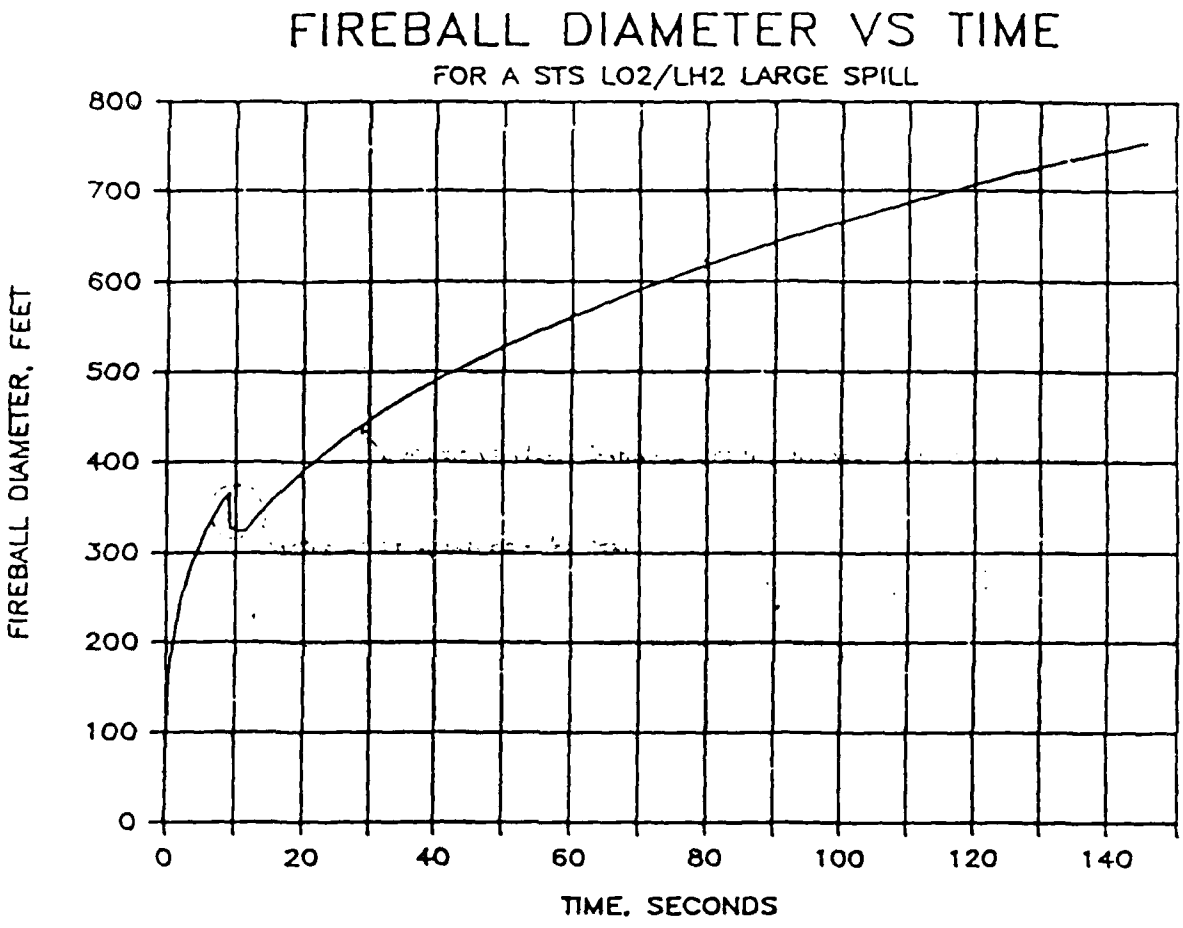


Figure 5-55 Fireball Diameter vs Time for LO2/LH2 Example Problem.

Eq. 5.1.1:

$$P_{over} = \frac{2557.7\ \rho_o Q_o \left(\frac{Q_o}{1000}\right)^{0.25} \left(\frac{\rho_a X}{\rho_o X_o}\right)^{0.223} \left(\frac{\rho_o}{\rho_a}\right)^{-0.9}}{1 + 8\ \left(\frac{Q_o}{1000}\right)^{0.5} \frac{\rho_a X}{\rho_o X_o}}$$

Eq 5.1.2:

$$I_{sp} = \frac{A \rho_o X_o Q_o^{0.5} \left(\frac{\rho_o}{\rho_a}\right)^{-0.45} \left(\frac{Q_o}{1000}\right)^{0.1} \left(\frac{\rho_a X}{\rho_o X_o}\right)^{m}}{1 + 0.2\ \left(\frac{Q_o}{1000}\right)^{-0.3} \frac{\rho_a X}{\rho_o X_o}}$$

Eq 5.1.3:

$$Y = \frac{t}{W^{1/3}} \left(1 + \frac{217}{W}\right) \left(0.59 - 0.092 \frac{L}{D}\right)$$

Eq 5.1.4:

$$V_T(\infty) = \frac{4.64 * 10^4}{r_o * 0.276}$$

Eq 5.1.5:

$$V_T = V_T(\infty) \cdot \left(1 + \frac{0.026}{\left[\frac{L}{D} - \left(\frac{L}{D}\right)_o\right]^{1.46}}\right)$$

Eq 5.1.6:

$$V_T(\theta) = \left[\frac{1.634}{20 - \theta}\right]^{1.64} \cdot V_T\ (\theta = 0)$$

Eq 5.1.7:

$$\lambda = \frac{D}{\left(W_{TNT}\right)^{1/3}}$$

Figure 5-56 Equations in Conventional Notation.

Eq. 5.1.8:

$$Y = \frac{\Delta H_R}{e_{TNT}} \qquad \Delta H_R = \Delta H_{fi}\ (\text{Products}) - \Delta H_{fi}\ (\text{Reactants})$$

Eq. 5.2.1:

$$V_o = 73.96\ Y^{0.43}$$

Eq. 5.2.2:

$$V_{50} = 139\ \lambda^{-1.46}$$

Eq. 5.2.3:

$$V = V_o\ e^{-kx}$$

Eq. 5.3.1:

$$D = 9.56\ W_b^{0.325}$$

Eq. 5.3.2:

$$D = 11.05\ W_b^{0.306}$$

Eq. 5.3.3:

$$D = 8.86\ W_b^{0.328}$$

Eq. 5.3.4:

$$D = (3Rt/4\pi\rho)^{1/3}$$

Eq. 5.3.5:

$$D = (3W_b/4\pi\rho)^{1/3}\ \tau^{1/3}$$

Eq. 5.3.6:

$$D_L = 3.51\ W_b^{1/3}$$

Eq. 5.3.7:

$$\tau = 0.196\ W_b^{0.349}$$

Eq. 5.3.8:

$$\tau_o = 0.572\ W_b^{1/6}$$

Figure 5-56 Equations in Conventional Notation. (Continued)

Eq. 5.3.9:

$$R = \frac{5}{3} (W_b)^{5/6}$$

Eq. 5.3.10:

$$D = 12.4\, W^{1/3}$$

Eq. 5.3.11:

$$D = 6.8\, W^{1/3}$$

Eq. 5.3.12:

$$\Delta H_f(R) - \Delta H_f(P) = \sum_{i=1}^{n} \left(\eta_i A_i T + \frac{\eta_i B_i T^2}{2} + \frac{\eta_i C_i T^3}{3} \right) - \sum_{i=1}^{n} \eta_{xi} \Delta H_{vi}$$

Eq. 5.3.13:

$$\frac{dT}{dt'} = \frac{h_i - h_{fb} - \dfrac{4\pi \varepsilon \sigma}{1.67\, W_b^{1/6}} \left[\dfrac{3t' R}{4\pi P (MW)} \right]^{2/3} T^{14/3}}{t'\, C_p}$$

ε = Emissivity
σ = Boltzmanns Constant
t' = t/t_b = Nondimensional time
C_p = Specific Heat of Products = $A + BT + \dfrac{CT^2}{2} + \dfrac{DT^3}{3}$

Eq. 5.3.14:

$$\frac{dT}{dt'} = \frac{-4\pi \varepsilon \sigma}{1.67\, W_b^{1/6}\, C_p} \left[\frac{3R}{4\pi P (MW)} \right]^{2/3} T^{14/3}$$

Eq. 5.3.15:

$$Rh_i = \varepsilon \sigma A T^4$$

Eq. 5.3.16:

$$\sigma = C (W_b)^{1/3}$$

Figure 5-56 Equations in Conventional Notation. (Continued)

Chapter 6
Hazards Analysis Methods

CHAPTER 6
HAZARDS ANALYSIS METHODS

TABLE OF CONTENTS

Section	Title	Page
6.0	Introduction	6-1
6.1	Analytical Methods	6-1
6.1.1	Qualitative Methods	6-2
6.1.1.1	Change Analysis	6-2
6.1.1.2	Contingency Analysis	6-3
6.1.1.3	Critical Incident Technique	6-4
6.1.1.4	Criticality Analysis	6-5
6.1.1.5	Energy Analysis	6-6
6.1.1.6	Flow Analysis	6-7
6.1.1.7	Interface Analysis/System Hazard Analysis	6-8
6.1.1.8	Job Safety Analysis	6-9
6.1.1.9	Maximum Credible Accident/Worst Case Condition	6-10
6.1.1.10	Naked Man	6-11
6.1.1.11	Operating Hazard Analysis/Procedure Analysis	6-11
6.1.1.12	Preliminary Hazard Analysis	6-12
6.1.1.13	Prototype	6-13
6.1.1.14	Scenario	6-14
6.1.1.15	Software Safety Analysis	6-14
6.1.1.16	Subsystem Hazard Analysis	6-17
6.1.1.17	Systematic Inspection	6-18
6.1.2	*Quantitative* Methods	6-20
6.1.2.1	Cable Failure Matrix Analysis (CFMA)	6-20
6.1.2.2	Event Tree	6-20
6.1.2.3	Failure Modes & Effects Analysis (FMEA)	6-21
6.1.2.4	Fault-Tree Analysis	6-23
6.1.2.5	Management Oversight and Risk Tree Analysis	6-24
6.1.2.6	Network Logic Analysis	6-26
6.1.2.7	Pin Fault/Pin Short Analysis	6-27
6.1.2.8	Sneak Circuit Analysis	6-28
6.1.2.9	Statistical Methods	6-30
6.1.3	Methodology Source Matrix	6-34
6.2	Hazardous Subystem Methods	6-36
6.2.1	MPS - General System Overview	6-36
6.2.2	System (Design) Hazard Analysis	6-39
6.2.3	Integrated Hazard Analysis	6-43
6.2.4	Operating Hazard Analysis	6-51
6.2.5	Interface Hazard Analysis	6-52
6.2.6	Structural Failures	6-53
6.2.7	Mechanism Failures	6-55
6.2.8	Ordnance Failures	6-57
6.2.9	Propulsion Subsystem Failures	6-59
6.2.10	Pressure Subsystem Failures	6-61
6.2.11	Ionizing Radiation Failures	6-63
6.2.12	RF Subsystem Failures	6-65
6.2.13	Electrical Subsystem Failures	6-66

TABLE OF CONTENTS - continued

Section	Title	Page
6.3	Example NSTS Payload Hazards Hazards Analysis, Hazard Reports	6-70
6.3.1	Generic Hazards, Hazard Reports	6-71
6.3.1.1	Generic Hazard Reports	6-72
6.3.1.2	Hazard Report Notes	6-104
6.4	References	6-106

LIST OF FIGURES

Figure No.	Title	Page
6-1	Multipurpose Satellite (MPS)	6-108
6-2	MPS Undeployed	6-109
6-3	MPS - Exploded View	6-110
6-4	Organizing a Design Hazard Analysis	6-111
6-5	Organizing Hazards Analysis of Structure	6-112
6-6	Organizing Hazards Analysis of Mechanisms	6-113
6-7	Organizing Hazards Analysis of Ordnance	6-114
6-8	Organizing Hazards Analysis of Propulsion	6-115
6-9	Organizing Hazards Analysis of Pressure	6-116
6-10	Organizing Hazards Analysis of Ionizing Radiation	6-117
6-11	Organizing Hazards Analysis of RF	6-118
6-12	Organizing Hazards Analysis of Electrical Subsystem	6-119

LIST OF TABLES

Table No.	Title	Page
6-1	Quantitative Hazards Analysis Sources	6-34
6-2	Qualitative Hazards Analysis Sources	6-35
6-3	MPS Hazardous Subsystem Summary	6-38

CHAPTER 6
HAZARDS ANALYSIS METHODS

6.0 INTRODUCTION

This chapter presents, describes, and in certain cases illustrates specific methods to:

(1) Identify hazards, i.e., energy or toxic sources which if uncontrolled or released can lead to accidents;

(2) Identify accidents which may result;

(3) Identify and assess the features, measures and margins which exist in a system or operational design which function to control an identified hazard;

(4) Identify possible events and probable causes which result in loss of control of a hazard;

(5) Identify additional or alternative features, measures and margins which effectively reduce the possibility of loss of control of an identified hazard.

The methods of this chapter have varying utility to hazards analysis. Detailed discussions of each is available in the literature; much of the discussion in this chapter is extracted from that literature. The direct reference associated with each method is a primary reference. Other references to the methods are provided in Section 6.1.3.

The methods of this chapter are organized and described from the viewpoints of

(1) Analytical Methods - Documented qualitative and quantitative techniques or models that are generally useful for hazards analysis of system or operational designs. These are discussed in Section 6.1.

(2) Hazardous Subsystem Methods - Methods which are uniquely suited to analysis of specific categories of energy or toxic sources, i.e., hazardous subsystems. These are discussed in Section 6.2.

(3) Hazards Analysis and Reporting - These are discussed in Section 6.3 for National Space Transportation System (NSTS) Payloads.

6.1 ANALYTICAL METHODS

This section provides a description and evaluation of the documented quantitative and qualitative analytical methods and models used for hazards analysis. Each method is concisely described, and a singular reference to application details is provided. Each method is related to the literature sources of the Annotated Bibliography in Section 6.1.3. The described analytical methods should be viewed as complementary rather than competitive. This compendium concentrates on those classical methods which have most often been employed by the professional system safety community.

6.1.1 Qualitative Analysis

A qualitative analysis is a non-mathematical review of all factors affecting the safety of a system, operation or person. It principally involves examination of the actual design relative to a pre-determined set of acceptability parameters. All possible conditions and events and their consequences are considered to determine whether they could cause or contribute to injury or damage to the environment. Some form and level of qualitative analysis will always precede a quantitative analysis. The objective is to eliminate or reduce hazards and establish effective control over significant hazards, without regard to the mathematical probabilities of specific events. Qualitative methods are used to monitor each safety critical item as the design progresses to assure proper application of safety criteria.

6.1.1.1 Change Analysis - (Reference 1) Change Analysis can be applied to all systems where a system design change is in progress. This method uses a known system as a baseline. It examines the nature of each contemplated change, and analyzes the probable effect of each change, or changes, on system risks. It is used for selection of a preferred change from among several candidate changes. However, baseline risk for the system must have been established as a result of prior analysis. Understanding of the physical principles governing behavior of the system being changed is essential. Difficulty of application is a function of system change and complexity. The chief advantage of the technique lies in its "shortcut" approach, since only the effects of change need be analyzed, rather than the system as a whole.

Application

Change analysis can be used in two ways:

(1) Operational Change Control - A "before-the-fact" analysis of actual or proposed changes in a system or procedure to evaluate safety effects.

(2) Accident/Incident Change and Difference Analysis - An "after-the-fact" analysis to pinpoint changes that may have had potential in causing an accident or near accident.

A structured analytical format should be generated for effective analysis of proposed changes, and to maintain control of each change. The analyses should consider six major elements:

(1) Job Statement - A description of the current method, the change, and why the change is necessary/desired.

(2) Factors - Those items or activities (factors) that could cause problems/accidents/incidents and are affected by the proposed change. Examples of such factors would be: communication, energy, equipment, location, personnel, procedures, protective devices, schedule, subcontractors, time, tools, and weather.

(3) Current Method - A brief description of the current design feature or operational procedure, including its relationship to the factor being evaluated.

(4) Change - Notes the difference between the current method and the proposed change.

(5) Change Assessment - An evaluation of relative merit of the current method and the change.

(6) Action Required - Identifies actions needed to offset the impact of the change where it is less adequate than the current method.

6.1.1.2 Contingency Analysis (Reference 2) - The purpose of Contingency Analysis is to identify the credible mishaps that might occur in a system, and to define emergency measures and protective equipment which will mitigate the effects of the mishap. Contingency Analysis can be used on all systems, subsystems, components, procedures, or interfaces. It is an effective means to evaluate and assess the adequacy of disaster response plans. Contingency Analysis is not a discrete technique. It may require the application of a group of methods to determine the need for contingency features, measures or margins.

Application

A contingency is an emergency caused by an unprogrammed event. The development of contingency measures may ensure control can be reestablished and an accident avoided. Contingency measures should be prepared and adopted before the product is released for general use. The result of contingency analysis may be to alter the operation of a product to increase the time available to act in an emergency, to incorporate monitoring and/or warning preventive devices, or to add automatic devices for rapid corrective or suppressive action.

There are five basic steps to be considered in contingency analysis:

(1) Select the contingency to be accomplished. The selection might be made from a Preliminary Hazard Analysis, a procedure analysis, or the top event of a fault tree.

(2) Sketch the sequence or chain of events which might take place in a contingency situation.

(3) Analyze the chain of events to determine whether or not there is a possible action that could forestall an event.

(4) Identify the corrective actions which would be most effective in minimizing adverse effects at minimum cost. Consider also the end effect of the contingency.

(5) Ensure by analysis and test that the corrective actions selected will be effective and reliable.

Contingencies that may occur during system processing or operations should be considered during system, equipment and operations design. Items of consideration may include:

(1) Product vulnerability - The conditions and time when the product is vulnerable to an unplanned event and loss of control.

(2) Detection and warning methods - The means by which an error, malfunction, or outside condition or its effects, can be detected and whether or not the detection methods will be adequate, or the warnings easily understood.

(3) Points of no return - In some contingencies a point may be reached when recovery should be abandoned and efforts directed to safeguarding personnel. At other points efforts should be diverted from saving the equipment to preventing the adverse condition from affecting the environment of the system. Procedures should be provided for these abandonment points so that personnel will know beforehand exactly when and what escape action is necessary.

(4) Emergency equipment - Select, test for adequacy, and install at readily available locations.

(6) Safety zones and evacuation routes - Identify and input to operational plans.

6.1.1.3 Critical Incident Technique (Reference 2) - The purpose of the Critical Incident Technique is to identify historically significant safety events which may pertain to the system under development. It requires the review of related historical incident reports and/or interviewing operationally experienced experts to collect information on past mistakes, hazards, and near misses. The Critical Incident Technique may be applied to any system for which a reasonable background of historical operational experience has been accumulated. Application is straightforward and uncomplicated.

Application

The Critical Incident Technique should be initiated by interviewing experienced personnel about their involvements in accidents or near-accidents (near-misses), and about hazardous conditions that could result in mishaps. Then form a survey group of experienced personnel. The range of experiences should be as wide as possible. Maintenance and repair personnel are excellent participants, but operators and supervisors should also be included.

The participants are informed of the study and its objectives. They are asked to describe all near-misses or mishaps they can recall. Stimulate their recall by giving each participant a list of similar incidents developed by interview. (People are generally more willing to talk about near-misses and accidents in which others were involved than serious mishaps in which they themselves were involved. When the interviewees who knew of near-misses or mishaps but were not participants are added to those who were participants, a considerable amount of information on problem causes, unsafe conditions, and other pertinent facts becomes available.) Questioning is carried on as long as the participant can recall any human error or its causes, unsafe condition, or incident. Even isolated items reported by only one participant can be used advantageously to alert the analyst to a potential hazard or accident risk that might exist with his proposed product. When a number of persons interviewed report similar problems and accidents, they can be accepted as indicators of deficiencies that will require action in the design or manufacture of the new product.

6.1.1.4 Criticality Analysis (Reference 2) - The damage potential of each system element can be ranked according to its failure effect. This technique can be applied to all systems, processes, procedures, and their elements. Identification of the specific failure modes to which the critically analysis is to be applied, however, must be accomplished by an adjunct technique, usually a failure modes and effects analysis. A variety of criticality indices exist in the literature for use in coding the loss potential of failures. Application of these indices is relatively easy, once the failure modes are identified.

Application

Criticality can be ranked in more than one way and for more than one purpose. The Society of Automotive Engineers (SAE) in Aerospace Recommended Practice 926 (Reference 3) categorizes criticality of failure modes as:

Category 1: Failure resulting in potential loss of life.
Category 2: Failure resulting in potential mission failure.
Category 3: Failure resulting in delay or loss of operational availability.
Category 4: Failure resulting in excessive unscheduled maintenance.

The method of SAE ARP 926 is an extension of failure modes and effects analysis (FMEA), failure modes, effects, and criticality analysis (FMECA). In the SAE procedure for criticality rank determination, the criticality for any component is multiplied by the number of failures of a specific type expected during each one million operations occurring in a critical mode.

Another method of ranking uses the formula:

$$CR = (PL) \times Q \times (FR)$$

where CR = criticality ranking,
PL = probable damage resulting from a specific failure mode,
Q = probability of component failure (1 - reliability), and
FR = ratio of occurrence of a specific failure mode.

A specific component can have more than one mode of failure, with only certain ones possibly causing damage or injury. FR is the ratio of those failures that could generate a specific damage level to the total number of possible failures. These failure ratios can be determined for new systems from manufacturers' data on failure modes, network analyses, tests, or combinations of these sources.

Criticality ranking may be used to determine which items require more intensive study for hazard elimination, special attention during production, special specification requirements, more intensive testing, or special procedures or safeguards. Ranking does not complete a critical component analysis. Evaluations must also be made to establish the preventive and corrective measures that should be taken, and the safeguards to be incorporated if the potential critical hazard could result in loss of control. A number of specialized types of criticality analyses can be used, depending on the system. Fault-free analysis, circuit analysis, or FMEA can be used to determine items that would be critical, or designs in which single-point failures could occur.

6.1.1.5 Energy Analysis (References 4 and 5) - Energy Analysis can be used to identify all sources of energy within a system, and to assess control of energy release. It applies to all systems which include energy in any form (e.g., potential or kinetic mechanical energy, electrical energy, ionizing radiation, or chemical or thermal energy). Oversight in identifying system vulnerability to external sources of energy can be very significant. Combined energy effects are sometimes overlooked (e.g., a vessel whose walls are simultaneously exposed to a pressure differential and a thermal gradient). This method is of special value as a "first-look" technique, but it requires considerable skill in energy analysis.

Application

Energy Analysis is based on the idea that energy flow is a fundamental cause of accidents where energy is transferred or released in an uncontrolled manner. The safety of a system is evaluated and improved by evaluating:

(1) Sources of available energy existing in a system or subsystem, (or in its environment), and the methods to eliminate unnecessary sources of energy.

(2) Means to reduce and control the level of energy by controlling factors such as pressure, temperature, voltage, velocity, or radiation.

(3) Means to control the flow of energy, such as isolating energy sources from regions where they could initiate damage.

(4) Methods of absorbing or reducing free energy to prevent or minimize damage should loss of control occur.

A generalized procedure for an energy analysis includes determining:

(1) Sources and reservoirs of energy and the magnitudes present and available to generate damage or injury. The magnitude of energy present depends on the level of energy per unit (pressure) and the number of units present (volume).

(2) Whether the energy requirements of the product or system could be reduced so that a lesser hazard exists.

(3) Whether a less hazardous type of energy source could be substituted.

(4) Primary hazards, such as ignition sources, that could initiate sudden, inadvertent release of stored energy.

(5) Factors that could contribute to primary hazards, such as corrosion, penetration, or other weakening.

(6) The extent of damage or injury that could result from release of stored energy.

(7) Safeguards, such as relief valves, thermostatic controls, or circuit breakers, to maintain stored energy in its controlled state.

(8) Isolation or shielding measures to prevent increase in energy level from outside sources.

(9) Measures to contain outputs from the energy source or reservoir that could cause injury or damage.

Another methodology which incorporates energy analysis is Management Oversight and Risk Tree (MORT). Within the MORT system, an incident is defined as barrier-control inadequate or failure without consequence. An accident is defined as unwanted flow of energy, or environmental condition, that results in adverse consequences. MORT is an investigative tool that focuses on the many factors contributing to an incident/accident by means of a meticulous trace of unwanted energy sources, along with consideration of the adequacy of the barriers provided. One of the basic MORT concepts, then, is the evaluation of the adequacy of energy barriers relative to persons or objects in the energy channel.

6.1.1.6 Flow Analysis (Reference 4) - Flow Analysis is used to evaluate the confined or unconfined flow of fluids or energy, intentional or unintentional, from one component/subsystem/system to another. Minimal preparation is required to evaluate intentional flows within a system. However, considerable expertise is required to evaluate unintentional flows, combined unintentional flows, and their controls. The adequacy of static barriers can be evaluated by comparison of the physical and functional characteristics of the system with control requirements levied by codes, regulations and standards. Where process controls regulate flow, application becomes more difficult. Automatic or manned controls are not amenable to straightforward flow analysis and so adjunct methods must be used for support. External sources of flow, from adjacent systems or forces of nature, should be included.

Application

Flow analysis investigates flow of fluid, energy, or both, to identify hazardous conditions. Flow may be confined and involve a fluid (water, fuel, oil or steam), or energy (electrical, electromagnetic, hydraulic or thermal). It may also be unconfined (heat radiation from one body to another). The most frequent and severe problems in any system are generally with the fluids and energy that must flow from one unit to another through confined passages.

A procedure for flow analysis may include:

(1) Review the fluid under consideration for inherent hazards, such as flammability, toxicity, odor, corrosiveness, moisture and water lubricity, contamination, loss of material, and loss of pressure.

(2) Determine whether the fluid could affect the surroundings or other equipment with which it might come in contact if uncontrolled. Determine whether any incompatibility would exist.

(3) Review the proximity and relationship between lines, containers, and equipment containing incompatible fluids. Establish that they have been separated adequately or that protection and means to isolate them have been provided.

(4) Establish the level of leakage that would constitute a problem. If only a small amount could produce serious effects, ensure that piping specifications stipulate maximum leakage permissible.

(5) Check potential effects of faulty or failed interconnections between two units. Determine the type of connection best suited for minimizing leakage. Conduct tests to ensure leakage does not exceed established levels.

(6) Indicate requirements in engineering specifications and drawings.

6.1.1.7 Interface Analysis/System Hazard Analysis (Reference 6 and 7) - The purpose of Interface/System Hazard Analysis is to identify physical and functional imcompatibilities between adjacent/interconnected/interacting elements of a system which could generate hazards and result in mishaps. Understanding the behavior of the elements is essential. Use of adjunct techniques to support the analysis may be beneficial - e.g., application of Failure Modes and Effects Analysis at each of the system interfaces.

Subsystems may induce hazards resulting from their integration into the system. Since integrated conditions are not generally considered during subsystem analysis, these hazards may not be identified except at the system level using a System Hazard Analysis (SHA). When performing the SHA, the analyst must consider the interfaces created by the integration of subsystems and the possible independent, dependent, and simultaneous failures that could create a hazardous condition. During a development program the analyst will normally be working from a preliminary operating procedure.

Utilizing the SHA format will require an understanding of the accident sequences which may develop from the exposure of personnel, materials, or property to various potential interface hazards. The following are typical items that should be considered during the SHA:

(1) Identify the operating procedure, step number, or task description number.

(2) Identify the hazardous element or source of energy that may result in an accident.

(3) Identify the event, or actions, which establish the conditions necessary for release of the hazardous energy.

(4) Identify who or what is exposed to the release of the hazardous energy, and which specific hazard exposes man, machine, equipment, materials, or facilities, to hazardous environment, injury, damage or pollutants.

(5) Identify the combination of events which may initiate the accident sequences, such as human error, component failures, fault states, or environmental conditions.

(6) Identify the possible accident event that could result in injury to personnel, equipment or material damage, facility damage, or production interruption.

(7) Identify the worst case possible effects of the occurrence of the accident event.

(8) Identify the hazard category as defined in the particular standard being worked to.

(9) Recommend actions that would eliminate or control the event resulting in a hazardous condition, the triggering event, or the potential effects of the accident event. Consider engineering changes, procedure changes, protective equipment, supervision, and personnel training and selection.

6.1.1.8 Job Safety Analysis (References 8 and 9) - Job Safety Analysis is used to evaluate work processes to identify hazards associated with each element. Job Safety Analysis is a useful technique with which to identify hazards associated with human operations. The method is especially applicable to manual functions during ground operation of hazardous systems/elements. Such functions must be controlled by procedures which provide assurance that they will not vary in significant ways, or anticipated variations must be accounted for in the analysis.

Application

Job Safety Analysis (JSA) is used to review job methods, identify hazards, and stress safe practices. It is one of the first steps in safety training and in hazard/accident analysis where there is a possibility of injury or health hazard to the worker. There are four basic steps in developing a JSA:

(1) Select the job to be analyzed. Give priority to those jobs with the highest frequency of accidents, those which have the potential for or have produced severe injury, and new jobs created by changes in equipment or processes where accident potential may not be fully understood.

(2) Break the job down. A job should be broken down into a sequence of basic steps, each describing what is being done. This technique involves selecting the right operator to observe, briefing him on the purpose, observing the job being performed, and checking the recorded breakdown steps with the operator.

(3) Identify hazards and potential accidents. For each job step the analyst should determine potential accidents that could happen to the operator by observing the job, discussing it with the operator, or recalling past accidents. The analyst should also consider safety/health hazards that could be produced by the environment, such as toxic gas, vapor, mist, dust, heat or radiation. The objective is to fully understand the hazards and potential accidents.

(4) Develop solutions. The final step in a JSA is to develop a recommended safe job procedure to prevent occurrence of the accidents. The principal solutions are: to find a new way to do a hazardous job; change or minimize the physical conditions that create potential hazards; change the work procedure to eliminate hazards still present; and try to reduce the necessity or frequency of performing a hazardous job.

6.1.1.9 Maximum Credible Accident/Worst Case Condition - (Reference 4) Using this technique, the analyst postulates the most severe mishap that might reasonably be considered for a system. He then considers all potential contributors to the mishap in their worst-case states, and examines the possibility that the mishap may occur as a result. This technique can be applied to systems and subsystems of all kinds, whether manned or unmanned. The analyst must be knowledgeable of the system and its use environment. He should guard against needless study of conceivable but improbable worst case conditions.

Application

A system or product will be exposed to extremes of environments, processes, conditions, and loads and stress during its life cycle. All of these should be analyzed to determine the worst case conditions that could exist. The analyst should consider the following:

(1) Design strengths of materials may have been derived from lab test data under specific conditions or normal room temperature and pressure at sea level. Operational conditions, however, can differ drastically from this norm producing greatly increased stresses, reduced strengths, or both. Thus each variable should be analyzed to determine whether operational requirements will be met. Prescribe limits to potential hazards to ensure that a worst case condition does not occur.

(2) The point in time at which a failure occurs may generate a worse effect than at other times. Failure of a first-stage motor igniter just prior to launch of a missile would leave it sitting on the launch pad. Losing control of a missile from the same failure immediately after lift-off would result in a fallback and much more damage as compared to a loss of control far down range. Each operation and hazard must be investigated for the point in time when loss of control could generate the maximal adverse effect.

(3) The most damaging accident can have an extremely low probability of occurrence. Conversely, the greatest danger of a mishap may be at a time when minimal damage is likely. Both factors, probability and severity, must be analyzed to determine the worst-case conditions involved in system operation over an extended period.

In analysis of possible mishaps in which a nuclear device could be involved, the term "Maximum Credible Accident" is used. In such cases the worst-case that can reasonably be expected to occur may have an extremely low probability, but not so low that it would be impracticable to incorporate suitable safeguards in the system.

There are three broad categories of hazards: inherent properties or characteristics of the equipment; material or human failures; and environmental stresses. The various configurations in which a piece of equipment might be operated, and the use to which it will be subjected by personnel of differing competency, must be considered. In most cases suitable safeguards can be provided, especially where material failure constitutes the hazard, since such failure will only occur in a limited number of ways. Where

failure is due to human error, safeguards are more difficult to provide because of the large number of ways in which personnel can cause unsafe conditions.

6.1.1.10 Naked Man (Reference 10) - This method is applied to a basic system, with all existing safety features and mishap controls removed. The inherent hazads of the system are examined as existing controls are restored or new ones applied. The technique is applicable to all types of systems and subsystems, whether manned or unmanned. It is especially useful in analyzing confined-space entry safeguards and procedures. The technique can be exhaustively thorough. It is readily mastered and requires a minimum of instruction. A detailed logging and documentation system is required, which can make analysis very time consuming. Of all the techniques presented here, Network Logic Analysis, Event-Tree Analysis and use of the Naked Man principle are the most exhaustive. Their use, therefore, is well reserved for systems in which risks are thought to be high and well concealed.

Application

This method was outlined for descriptive purposes only. It is now seldom employed by the system safety community.

6.1.1.11 Operating Hazard Analysis/Procedure Analysis (Reference 11) - The approach used for this method is to review, step-by-step, the mission tasks that must be performed, the equipment that must be operated, and the personnel environment to identify possibilities of mishaps. These include mishaps which may harm the operators as well as operator error which can damage the system to cause an unsafe condition. The procedures that result must be sufficiently documented so that safety requirements can assure the step-by step sequence will not be violated. Thoroughness is determined by the degree to which procedural steps are explored, and by the degree to which steps can optionally be performed out of sequence or omitted. More complex procedures require formal documentation and greater analyst experience.

Application

The Operating Hazard Analysis (OHA) focuses on hazards resulting from personnel tasks or activities, and system functions that occur when a system is stored, transported, or exercised. The OHA effort must be initiated early enough in the system development cycle to impact the operating procedures for system testing. It is an effective closed-loop, iterative process of evaluating proposed operations prior to system design completion.

To perform the OHA the analyst should gather engineering descriptions of the system and support facilities. Requirements and procedures should also be a part of the information base. The approach to the analysis is similar to that of the Preliminary Hazard Analysis (PHA) except that operational events are of primary interest. The OHA analysis form should include the following: operational event description, hazard description, hazard effects, hazard control requirements, and disposition. The OHA will yield the following:

(1) Design changes to eliminate hazards or provide safety devices and safeguards.

(2) Special procedures for servicing, training, handling, storing, and transporting the system.

(3) Inclusion of warnings, cautions, special considerations, or emergency criteria in operating procedures.

(4) Identification of the timing of operations or system functions that will relate to hazardous occurrences.

6.1.1.12 Preliminary Hazard Analysis (PHA) (Reference 11) - The PHA is an initial study to identify apparent hazards and methods to control them. Checklists are often used. Various analytical techniques may be applied, singly or in combination. It is not a discrete technique.

Application

A Preliminary Hazard Analysis (PHA) will identify and address each of the significant hazards of a system. The PHA effort must commence during the initial phases of system development. It is used to develop initial system safety requirements, performance and design specifications, and it establishes the framework for the later, more detailed analyses. During the PHA, the analyst should examine the following areas of system design for hazard identification:

(1) Hazardous components that are energy sources.

(2) Interface safety-related problems.

(3) Environmental constraints, including both normal and possible abnormal environmental problems.

(4) Operating, test, maintenance, or other procedural problems.

(5) Facilities and support equipment with commensurate personnel training for proper use.

A checklist of hazard control methods is useful for the PHA. Examples are:

- Redundant devices or procedures
- Interlocks
- Fail safe design
- Fire suppression
- Personnel protective equipment, such as hard hats or breathing equipment
- Vented relief devices
- Electrical safeguards, such as explosion proofing
- Written procedures
- Limits monitors
- Human redundancy
- Energy containment vessels
- Time-phased hazardous functions
- Toxic substance controls, such as breathing equipment, sensors, or alarms

The PHA format may vary, but should include the following:

(1) The formal name of the part or subsystem which is the hazard source.

(2) The operating mode during which this hazard exists.

(3) The failure mode, or modes, of the hardware or procedure that allows loss of control of the hazard.

(4) Estimated probability. It may be qualitative, such as "highly probable" or "improbable," or it may be quantitative. Qualitative measures must be defined.

(5) A description of the mishap, which is the result of malfunction or failure that causes personnel injury or equipment damage.

(6) The effects of the mishap on personnel and equipment.

(7) Classification of the severity of the mishap.

(8) Definition of a feature, measure or margin that will effectively control the hazard and reduce the likelihood of occurrence or the severity of mishap.

(9) Amplifying remarks pertaining to hazard severity, hazard acceptability, or items that will influence the hazard.

6.1.1.13 Prototype (Reference 4) - Prototyping is a method to construct and operate a system or subsystem model, and test for failure under varied conditions. The technique is applicable to systems, subystems, and components, whether electrical/electronic or mechanical. The analysis tends to be costly in resources and time. For that reason, it is reserved for high-severity cases which are not amenable to adequate treatment by other techniques. Vehicle stage destruct testing would be a good example of this type of analysis.

Application

Few new products or systems are fault-free when their first items are produced. Therefore, prototypes are built before production begins, in order to ensure that (1) the item meets performance requirements, (2) that no unforeseen hazards or incompatibilities exist in the system, and (3) that production deficiencies are detected and eliminated.

The safety analysis of a prototype system requires establishing the objective to be achieved, evaluation of equipment, run-through of tasks, and review of designs and test procedures (with checklists). The safety analyst should consider the following detailed steps:

(1) Establish the limits of tests in duration or in results to be achieved.

(2) Establish the significant parameters to be instrumented and monitored.

(3) Select the types of transducers best suited to sense the selected parameters.

(4) Select sensor locations to ensure that readings actually represent existing conditions and are not affected by unrelated stresses. Also ensure that all transducers are properly installed and calibrated.

(5) Select the means by which the transducer signal is to be transmitted to the readout device. The means will depend on the use to be made of the information, whether it is to be an indicative signal, a parameter level, or recorded data for later use.

(6) Determine the proficiency of test personnel to perform as operators, directors, monitors, analysts, or emergency crews.

(7) Prepare test sequences, and provide checklists and suitable forms for each operator. Monitor for the tasks that each one will undertake, such as the characteristics to be observed, the measurements to be taken, and the information to be noted.

(8) Pre-establish the procedures to follow should critical parametric values not be met. Especially indicate the conditions under which a test will be aborted.

(9) Review hazards that might be encountered during the tests. Ensure that protective safeguards are provided.

(10) Evaluate the results of the tests to establish whether any hazards or safety problems exist, whether changes in design or procedures are necessary, or if additional safeguards should be provided.

6.1.1.14 Scenario (Reference 12) - Members of a knowledgeable operational/safety group amass spontaneous ideas (brainstorming) describing conceivable accidents and their contributors. Those ideas deemed wholly unreasonable are discarded, and the remainder are concentrated on by refining descriptions of causes and consequences, and making judgments as to their likelihood. This technique is of special value for manned and unmanned systems where features are novel and, as a result, may have no historical data base for guidance. The technique is limited only by the ability of the individuals to conceive of mishaps and of combinations of events and conditions that might induce them. An active imagination and freedom of thought processes enhances the ease of application. Since the method relies on spontaneity it has the weakness of a lack of methodical discipline.

Application

This method was outlined for descriptive purposes only. It is not a well-disciplined hazard identification and evaluation technique, and is seldom employed by the system safety community.

6.1.1.15 Software Safety Analysis (Reference 13 and 14) - Software Safety Analysis is used to identify hazardous conditions related to software safety critical command and control functions to prevent an erroneous command or

control signal from causing inadvertent activation or to prevent it from functioning at an inappropriate time. Within the system, introduction of such commands or functions may be controlled by inhibits or interlocks which positively prevent the hazardous event from taking place. Tasks and acceptability parameters, such as those specified by MIL-STD-1574A, are intended to provide traceability of safety critical commands generated by software. The objective of the analysis is to ensure that system interlocks and functional controls are incorporated into the software design to prevent the software system from initiating conditions that can result in catastrophic events.

The analysis approach includes a review of the computer program development specifications, and concentrates on program verification of the software system, requirements, design, logic, coding, input/output devices, and maintenance.

Application

The software safety analysis effort is started as soon as the system function allocation process has defined the hardware and software functions. The preliminary software hazard analysis is a direct offshoot of the system preliminary hazard analysis (PHA). The system PHA, when integrated with the requirements levied upon the software, will identify those programs, routines, tables, modules, or software tools that are critical to system safety and must be examined in depth. The preliminary software analysis is accomplished by analyzing the following:

(1) System and subsystem PHAs.

(2) System and subsystem specifications.

(3) System function allocation and interface documents.

(4) Functional flow diagrams, flow charts, and related data.

(5) Storage allocation and program structure documents.

(6) Background information related to safety requirements associated with the contemplated testing, manufacturing, storage, repair, and use.

(7) System energy, toxic and hazardous event sources which are controlled or influenced by software.

A detailed software hazards analysis must consider the particular software routine, the critical command/monitor functions which impact safety, and the system hazards that could occur from improper operation/failure to operate modes of such functions. After overall hazard categories are assigned, and the potential hazards of non-normal operations are defined, recommendations for safety requirements are made to eliminate or control of the hazards within the software system.

The follow-on software hazard analysis is a continuation of the preliminary software hazard analysis, and begins when coding of the software begins. Those software elements that have been previously identified as being safety critical should be analyzed at the source/machine executable code

level. The level of effort required depends on the perceived risks. In certain instances, if the source code is written in a high order language and there is a high level of system risk, the run time object code should be analyzed to insure that the compilation or interpretation process has not introduced any hazards or negated any safety design efforts. Additional activities that occur during the follow-on analysis include:

(1) A review of all hardware/software, software/software, and software/operator interfaces, and of critical data (e.g., files, etc.).

(2) Accomplishment of analysis on all algorithms, and calculations for correctness, and input/output/timing sensitivity. Those elements affecting safety critical items must be reviewed by system safety.

(3) System safety monitoring of the design and coding effort, with special attention to design/program changes.

(4) Placement of a program under in-house configuration control, when it is submitted for analysis, so that the analysis report will reflect a known program version.

The following specialized methodologies are examples of what can be used to help provide a thorough software hazard analysis:

(1) Software Fault Tree (Soft Tree). A soft tree describes a fault tree which includes software interfacing with hardware. The software fault tree proceeds in a manner similar to hardware fault tree analysis and uses a subset of the symbols currently in use for the hardware counterparts. Thus, hardware and software trees can be linked together at their interfaces to allow the entire system to be analyzed. This is extremely important since software safety procedures cannot be developed in a vacuum but must be considered as part of the overall system safety. The goal of software fault tree analysis is to show that the logic contained in the software design will not produce system safety failures, and to determine environmental conditions which could lead to these software induced failures.

(2) Software Sneak Circuit Analysis. Sneak analysis identifies system conditions that could degree or adversely impact mission success or basic equipment reliability. The purpose of software sneak analysis is to define logic control paths which cause unwanted operations to occur, or which bypass desired operations without regard to failures of the hardware system to respond as programmed. After a sneak circuit analysis and a software sneak analysis have been performed on a system, the interactions of the hardware with the system software can readily be determined. Data used for software sneak analysis should reflect the program as it is actually written. This includes system requirements, system description, coding specifications, detailed and complete source code, a compilation listing, and operating system documentation. The analysis technique involves reduction of the program source code to topological network tree representations of the program logic.

(3) Nuclear Safety Cross-Check Analysis (NSCCA). NSCCA is a rigorous methodology developed exclusively to satisfy the requirements of AFR 122-9 and should be accomplished by an agency which is independent of the program developer. NSCCA, to a great degree, is an adversarial approach to software analysis in that its basic objective is to show, with a high degree of confidence, that the software will not contribute to an undesirable event. The technical component of the NSCCA process evaluates the software by criticality analysis and test to assure that it satisfies the system's nuclear safety objectives. The procedural component of the NSCCA implements security and control measures to protect against sabotage, collusion, compromise, or alteration of critical software components. Nuclear weapons system software subjected to NSCCA ascends to the Air Force Critical Components List and, as such, comes under the provisions of AFR 122-4, Nuclear Safety: The Two-Man Concept.

(4) Safety Analysis Using Petri Nets. A Petri net is a mathematical model of a system. The user describes the system using a graphical notation and thus need not be concerned with the mathematical underpinnings of Petri nets. They can be used early in the development cycle when system design changes are relatively inexpensive. A system approach is possible with Petri nets since hardware, software, and human behavior can be modeled using the same language. The modeling language can be used for both formal analysis and simulation at various levels of abstraction. Timing and probabilistic information can be incorporated into the basic Petri net analysis. Unlike the fault tree, the safety analysis can be accomplished by a computer without human guidance because the design is first represented as a mathematical system.

6.1.1.16 Subsystem Hazard Analysis (SSHA) (Reference 4 and 6) - Subsystem hazard analysis is directed to system elements and components at less-than-system level. It can be performed only for subsystems involving functionally discrete groupings of elements/components. Beyond this restriction, application is unlimited. The Subsystem Hazard Analysis may utilize any number of analytical methods singularly or in combination.

Application

Initial SSHA may be conducted systematically by correlating hardware, hazards, personnel, and other factors. Missile and space systems, for example, are categorized according to functional subsystems and major components that each might contain. The analyst can correlate hardware, hazards, and operational time segments during which the hazards could exist. The hazards associated with a major component are related to the subsystem of which it forms a part. After subsystems are analyzed, operational time periods can be reviewed to determine how critical the effects of any hazard might be at any time in the life cycle of the system. Subsystem review sheets should contain space for notes regarding periods during which a specific hazard might be critical to the system. A broad breakdown of operations for a missile or space system should include:

- Transportation to a launch facility
- Loading or unloading on the launcher
- Missile storage
- Assembly and test
- Maintenance and checkout
- Launch (ignition, liftoff, escape, abort)
- Flight (boost, staging, maneuver, flight termination, landing, recovery)

An SSHA is reiterated as more and more information becomes available. In its initial stages it is similar to a Preliminary Hazard Analysis. As the hardware is developed, more intensive analyses, such as Failure Modes and Effects Analysis (FMEA), or network logic analysis can be used. The SSHA may be accomplished by preparing or reviewing applicable portions of the following:

(1) The mission analysis to determine performance requirements and environmental conditions.

(2) A functional flow diagram indicating the various subsystems.

(3) A brief description of each subsystem, including proposed functions and operations, input and output levels, and characteristics.

(4) A checklist of a wide variety of possible primary, initiating, and contributory hazards that could affect each subsystem, and the potential damages that could be generated. Make a determination of whether the subsystem would either be affected by the hazard or would generate the hazard.

(5) Detailed descriptions of the findings to explain problem areas. Entries should be coded in a matrix to relate the alphabetical designation of the hazard and the numerical designation of the subsystem hardware.

(6) Use of an FMEA to establish affecting conditions and environments and to determine modes of failure.

(7) A checklist of injury types to review the possibilities of personal injury by subsystem or operation.

(8) Descriptions of materials to determine the problems that might be involved in acceptance of new materials or applications of known materials for new users.

Each of the above prepared steps should also indicate a possible preventive or corrective measure.

6.1.1.17 Systematic Inspection (Reference 6, 8 and 9) - This method uses checklists, codes, regulations, industry standards and guidelines, prior mishap experience, reports, and similar experience, to methodically examine a design/system/process, in order to identify hazards. Systematic inspection is perhaps the most widely practiced of all hazard analysis methods. Many system safety personnel regard Systematic Inspection as an essential step prior to the application of any other technique.

Application

Systematic inspection is a means of facilitating safety integration. Systematic inspection requires the development of a checklist, after coordination of requirements with Human Factors, Design Engineering, Maintainability, Reliability, or any discipline cognizant of a unique hazardous substance or design feature. This inspection checklist is utilized initially as a reference for preparing the conceptual planning documents, and later for evaluation of a program safety data such as the program plan, hazard reports, design review presentations, and test plans. The safety design checklist provides a controlled means of ensuring that applicable standards and specification requirements imposed on the system are adhered to. A general checklist of considerable detail will be found in AFSC Design Handbook 1-X.

The early examination of a design/system/process requires a safety analyst with a background capable of developing:

(1) A thorough knowledge of the proposed system.

(2) Comprehensive system safety criteria.

(3) A detailed system safety program plan.

The analyst may structure a checklist by major equipments, by system functions, or by types of hazards (explosive - mechanical - electrical - chemical). The checklist is begun by entering the potential hazards, such as those identified during the initial PHA, and relating those hazards to the major equipment level. The related system operational or function is identified and then a recommended hazard control method is recorded. For each major assembly or subassembly a matrix can be developed to show the extent to which the design complies with the checklist. When the list shows the existence of unacceptable hazards, corrective action requests should be prepared to obtain immediate action.

6.1.2 Quantitative Methods

Quantitative methods generally yield results that are quantitative in terms of frequency of occurrence or magnitude of consequence. The methods described in this section are those that can yield quantitative results, even though much of the analysis is qualitative in nature. The user of quantitative methods should understand that where the data used in the analysis is not based on and traceable to experimental or operational data, the results should be suspect as an absolute measure. They may be used, however, as a relative measure such as in comparison of alternative designs. The user of the methods of this section should refer to Chapter 4, System Failure Probabilities.

6.1.2.1 Cable Failure Matrix Analysis (CFMA) (Reference 14 and 15) - This technique is a shorthand method used to concisely represent many of the possible combinations of failures which can occur within cable assemblies. CFMA analysis elements consist of: (a) a cross reference index of cable numbers and connectors; (b) cable assembly diagrams to represent physical configuration; (c) a connector matrix and pin location drawing for each different connector; (d) a cable wire table for each cable. The CFMA provides data to support a Failure Modes and Effects Analysis (FMEA). The FMEA function is to be responsible for all failure rate data associated with failures identified by CFMA. Major connector failure mode identification consists of credible faults that can occur from bent pins, such as pin-to-pin shorts and pin-to-case shorts. Major cable failure modes are wire-to-wire shorts, wire-to-shield shorts and open wire faults.

Application

A pin fault, or pinshort analysis is one of the application programs accessible to support the CFMA, or computerized sort and retrieval network. Reference paragraph 6.1.2.7 for the application example.

6.1.2.2 Event Tree (Reference 16 and 17) - This technique is related to Fault Tree Analysis and Network Logic Analysis. It involves the selection of initiating events, both wanted and unwanted, and develops their consequences through consideration of system/component failure-and-success alternatives. It then continues through all alternate paths, considering each consequence as a new initiating event. This technique is universally applicable to systems of all kinds. However, undesired events (as well as desired events) must be anticipated to produce meaningful analytical results. The technique can be exhaustively thorough. Thoroughness has only two theoretical limits: the presumptions that (1) all system events have been anticipated, and that (2) all consequences of those events have been explored. Successful application to complex systems cannot be undertaken without extended formal study combined with some practical experience. It is enormously time and resource consuming. The exploration of all wanted and unwanted events and their consequences increases the effort substantially beyond that required for Fault Tree Analysis or for Failure Modes and Effects Analysis. Network Logic Analysis, Event Tree Analysis and use of the Naked Man principle are the most exhaustive of these studied techniques. Their use, therefore, is well reserved for systems where risks are thought to be high and well concealed.

Application

The event tree complements the fault tree technique. Whereas a fault tree starts from a particular final event such as an explosion and works from the top down, an event tree begins with a particular initial event such as a power failure and works from the bottom up. The analyst must recognize that event trees are used to define accident sequences that involve the complex interrelationships among engineered safety systems. They are constructed by using forward (deductive) logic: he asks the question, "What happens if the pipe breaks?"

The analyst begins event tree construction by defining a primary event and then defining the consequence events and paths which flow from this. The main elements in the tree are therefore event definitions and logic vertices. The event tree, like a fault tree, lends itself well to quantification, since expected frequencies of failure can be estimated. The emphasis is on the initial cause event and the analysis works from the bottom up to the final effect event. Each of the secondary events has a path for success and a path for failure. By convention the success path is on the left. The initial event is expressed as a frequency (events/y) and the secondary events as probabilities (failure/demand). An event tree shows the effects of a failure. This is particularly important where one failure may have many effects, as with the failure of a utility, such as electrical power or cooling water. It indicates whether the system considered is contributing disproportionately to the totality of the hazards, or putting it another way, it shows which branches in the fault tree of the hazards may be influenced by acting to reduce the particular failure.

The analyst also has the quantitative option of constructing a decision tree, which is a special case of an event tree model. In event trees, working states are not considered, so the sum of all probabilities do not add up to one. In decision trees, the system outcomes are expressed in terms of component states, so the outcomes must be coherent; i.e., they must add up to one. Decision trees can be used if the probabilities of component states are independent or if there are multiple component states or unilateral (one-way) dependencies. They cannot be used in the case of two-way dependencies, and provide no logical method for choosing the initiating event.

6.1.2.3 Failure Modes and Effects Analysis (FMEA) (Reference 2) - This analysis examines a system element by element and identifies modes in which each element can fail and then determines effects on the system of each failure mode. This technique is enormously time consuming as the failure modes which will, and which will not, result in great damage must be reviewed to fully develop the analysis. The advantage of this technique is that no undesirable event need be predetermined to enable its use, as with Fault-Tree Analysis (FTA). Since the end effects of failures are frequently established, FMEAs are often used for safety purposes. Limitations: FMEAs don't usually take into account human error and hazardous conditions; they take into consideration, to a limited extent, the effects of environment; they usually do not consider the effects that result from multiple failures. Used with an FTA, the two can be powerful analytical tools. The FTA is used to pinpoint where an FMEA should be carried out and it provides the additional data the FMEA lacks.

Application

To conduct an FMEA, the analyst must basically know and understand the mission of the equipment, the constraints within which it is to operate, and the limits delineating success and failure. There are numerous variations of forms on which information and data are recorded. Each organization undertaking an FMEA prepares its own format. The analysis proceeds with the following steps:

(1) The product is divided into assemblies that can be handled effectively.

(2) After reviewing functional diagrams, schematics, and assembly drawings, block diagrams are prepared with assigned reference numbers to permit coordination with the items or functional breakdown tables.

(3) A complete component list is prepared for each assembly as it is to be analyzed. The specific function of each component is entered at the same time.

(4) Operational and environmental stresses affecting the product are then established. These stresses are viewed in order to determine the adverse effect that they could generate on the system or its constituent assemblies and components.

(5) The significant failure mechanisms that could affect components are determined from analysis of the engineering drawings and functional diagrams. Effects of assembly failure are then considered.

(6) The failure modes of all components are identified, tabulated, and the effects produced by each listed. Since a component may have more than one failure mode, each mode must be analyzed for the effect on the assembly and then on the product.

(7) Each condition which affects a component should be listed to indicate whether or not there are special periods of operation, stress, personnel action, or events that would increase the possibilities of failure or damage.

(8) For risk assessment the hazard category may be indicated, or a real hazard index calculated.

(9) Preventive or corrective measures to eliminate or control the hazard are then listed.

(10) Probabilities of the occurrence of each component failure may be entered. Initially they may be estimated generic rates that have been developed from experience, from documents such as MIL-HDBK-217B, from reliability data sources that collect and collate such information, or from suppliers required to furnish data on contracted items.

(11) Probabilities of failure of subassemblies, assemblies, and products can then be computed.

(12) Some analyses proceed to determine the criticality of components and the effects that failure will have on the mission. This analysis is called an FMECA (failure modes, effects and criticality analysis).

6.1.2.4 Fault-Tree Analysis (Reference 18 and 19) - Identifies an undesirable event and the contributing faults/conditions that would precipitate it. The contributors and the undesirable events are interconnected using network paths through Boolean logic gates. This technique is applicable to systems of all types. The limitations are: (1) the presumption that the relevant undesirable events have been identified, and (2) the presumption that contributing factors have been identified and explored in sufficient depth. However, this is regarded as among the most thorough of the techniques for general system application. Prior knowledge of Boolean algebra and the use of logic gates is necessary. Computer aids are increasingly used. This method is capable of producing numerical statements of the probability of occurrence of undesirable events, given probabilities of contributing factors. The method does identify minimum sets of contributing factors which could precipitate the central undesirable event.

Application

It is important for the analyst to understand that a fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event which corresponds to some particular system failure mode. The fault tree thus includes only the most credible faults that contribute to this top event. A fault tree is a qualitative model that can be evaluated quantitatively and often is. A fault tree is a complex of entities known as "gates" which serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a "higher" event. The "higher" event is the "output" of the gate; the "lower" events are the "inputs" to the gate. The gate symbol denotes the type of relationship of the input events required for the output event, somewhat analogous to switches in an electrical circuit. The primary events of a fault tree are those events for which probabilities will have to be provided if the fault tree is to be used for computing the probability of the top events.

The concepts which the analyst must consider for the construction of a fault tree are as follows:

(1) Faults vs Failure - First the distinction must be made between the specific word "failure" and the more general word "fault." An item may operate at the wrong time due to the improper functioning of some upstream component. This is clearly not a failure of the item; however, its untimely operation may well cause the entire subsystem to enter an unsatisfactory state. An occurrence like this is called a "fault." "Failures" are basic abnormal occurrence, whereas faults are higher order events. The proper event description of a fault, which is to be entered into the fault tree, must specify not only "what" the undesirable component state is, but also "when" it occurs.

(2) Passive vs Active Components - A passive component, such as a wire or steam line, contributes in a more or less static manner to the functioning of the system. It acts as a transmitter of energy, or loads, from place to place. To assess the operation of a passive component, such tests as stress analysis, or heat transfer studies, are performed. An active component, such as a valve or switch, contributes in a more dynamic manner to the functioning of its parent system by modifying system behavior. To assess the operation of an active component, parametric studies of operating characteristics and studies of functional interrelationships are performed. A passive component can be considered as the transmitter of a "signal," and component failure will result in the non-transmission of its "signal." In contrast, an active component originates or modifies a "signal," and component failure will result in no output "signal," or an incorrect output "signal." From a numerical reliability standpoint the failure rate value of an active component is generally above 1×10^{-4} per demand, and passive component failure rates are two to three orders of magnitude below that value.

(3) Component Fault Categories - The fault tree analyst classifies faults into three categories:

(a) Primary - any fault of a component that occurs in an environment for which the component is qualified; e.g., pressure tank rupture because of a defective weld.

(b) Secondary - any fault of a component that occurs in an environment for which it has not been qualified; e.g., pressure tank rupture above design pressure.

(c) Command fault - involves the proper operation of a component but at the wrong time or in the wrong place; e.g., an arming device closes too soon because of a premature external signal.

(4) The "Immediate Cause" Concept - Failure mechanisms produce failure modes which, in turn, have effects on system operation. The analyst defines the system and then selects a particular system failure mode for further analysis. The latter constitutes the top event of the fault tree. Next the analyst determines the immediate, necessary, and sufficient causes for the occurrence of this top event. These causes of the top event are now treated as sub-top events and then the analyst determines their causes. In this way he proceeds down the tree continually, transferring the point of view from mechanism to mode, until the limit of resolution of the tree is reached.

6.1.2.5 Management Oversight and Risk Tree Analysis (MORT) (Reference 4 and 20) - The method here is to apply a pre-designed, systemized logic tree to the identification of total system risks with the inherent physical equipment, processes, and operational/management inadequacies. As a comparison tool, this tree describes all phases of the safety program and is applicable to various kinds of systems and processes. This technique is of particular value in accident/incident investigation as a means of discovering system or program weaknesses conducive to mishaps. Utility of the technique for this

application is increasing. Thoroughness is limited only by the degree to which comparison evaluations explore the existing system against the model tree. Although tedious and time consuming, the technique is not difficult to apply once a limited formal instruction is achieved.

Application

MORT is a "universal tree" developed for an entire safety system discipline. It can be used as a kind of a "master checklist" to analyze causes and contributing factors of major accidents, or to evaluate the quality of an existing system. Certain sections are, or are not, applicable to the particular situation being analyzed, and some sections may be further developed so as to better isolate an devaluate an important aspect of the situation. The MORT diagram visually shows the elements present and calls the analyst's attention to any missing elements.

The analyst constructs a MORT logic diagram in the form of a "work sheet." While similar in many respects to fault tree analysis, MORT is more generalized and presents over 1500 specific elements of an ideal management program for optimizing occupational safety. Fault tree construction is the logical development of the TOP event, using the technique of deductive reasoning to progressively isolate the contributing factors to the fault event being considered. Each fault event is developed until a system component is identified for which a failure is considered primary or basic. A "fault event" is the result of the logical interaction of other contributing factors or events. The graphical construction, which shows that fault event and its more basic factors, is termed a "branch" of the fault tree. Going from top to bottom on the diagram the analysis proceeds from general to specific, consisting of sequences of events that lead to the TOP system failure or accident. The sequences of events are built by AND gates and OR gates. The sequences finally lead to the primary causes for which there is failure primary causes for which there is failure rate data available. Graphic symbols used in fault tree construction are of two general categories: logic symbols and event symbols. For the most part, MORT uses the logic symbols, event symbols, and tree construction techniques that have been developed by the Fault Tree Analysis technology.

The careful application of MORT by a fault tree analyst to a specific hardware-oriented system insures the resulting tree (logic diagram) will be orderly, properly time-sequenced, logically correct, and suitable for evaluation, using quantitative, probabilistic analytical techniques. The methodology of construction can be stated in the following specific rules:

(1) State the fault event as a fault, including what and when the fault state of that system or component is.

(2) If the fault statement is a state-of-system statement an AND-, OR-, CONDITIONAL- gate may be used. If the fault statement is a state-of-component statement an OR- gate is always used. To continue, look for the primary, secondary, and command failure fault events.

(3) No gate-to-gate relationships.

(4) Expect no miracles; those things that would normally occur as a result of a fault will occur, and only those things.

(5) In an OR- gate, the input does not cause output. If any input exists, the output exists. Fault events under the gate may be restatement of the output events.

(6) An AND- gate defines a casual relationship. If the input events coexist, the output is produced.

(7) A CONDITIONAL- gate describes a casual relationship between one fault and another, but the indicated condition must be present. The fault is the direct and sole cause of the output when that specified condition is present.

When expanding upon the MORT diagram the analyst does not have the same degree of concern with precise time sequencing as does the fault tree analyst. Lower tier expansion of the "universal" generalized MORT logic diagram is directed to obtaining a qualitative (not quantitative) evaluation of the MORT elements as "adequate" or "less than adequate."

6.1.2.6 Network Logic Analysis (Reference 4) - Describes system operation as a network of logic events, and develops Boolean expressions for proper system functions. The network/expressions are then analyzed to identify elements of system vulnerability to mishap. This technique applies to all systems, manned or unmanned having components or operations which can be represented in mi-modal elemental form. Although the technique is exhaustively thorough, a working knowledge of Boolean algebra is essential to master the representation of the system in network form. It explores all wanted as well as unwanted system performance eventualities. It requires much more effort than does Fault Tree analysis or Failure Modes and Effects Analysis. Its use, therefore, should be reserved for systems wherein risks are though to be high and well concealed.

Application

When a safety analyst requires dependable probability estimates of safety levels, network logic analysis can permit the necessary determinations of probabilities of failure or of inadvertent operation of products and subsystems. The symbology for hydraulic, fluidic, and pneumatic systems makes them adaptable to logic analyses. The effects of various failure modes and design inadequacies can be determined when suitable constraints are applied to modulating and multiposition components. Network analysis by application of Boolean logic technique has been best employed in the design and evaluation of complex electrical and electronic circuitry. Its use is increasing as systems grow more complex, as the consequences of failures increase, and as new applications are found. It can not only determine how safety of a system is affected by component failures in a circuit but also whether the circuit can generate damaging outputs or failure modes. It can provide the means to establish the quantitative safety level of a system.

To apply network analysis, the system operation is described in terms of interacting electronic circuits and mechanical devices, which open or close to permit flow of energy from one point to another. These circuit devices are then represented by logic elements. Logic diagrams are developed from wiring diagrams which, in turn, are developed from functional block diagrams. A logic evaluation can be developed to express the condition (on or off, open or closed, successful or failed) of each element required to produce an output event. Each network element is identified by a symbol. Starting with the end event, a Boolean equation is written expressing the conditions that could

cause it to occur. The equation represents each element involved in causing or permitting such an event, and the input and output conditions to that element. The same symbols can also designate the probability that the operation being considered will take place. A separate equation is written for each gate. These equations are then combined in chains of events leading to investigation of the ultimate event. The final equation indicates those factors whose condition will affect operation of the system to produce the end event being investigated. Quantitative analyses can be made by inserting a probability value for each factor in a Boolean equation, taking care that the value actually represents the mathematical expression and all affecting states; e.g., if an expression is based on a relay failing to open, the probability value must correspond, and not include all modes of relay failure. Analyses made in this way can establish probability of success or failure of an entire network or system; the probability of failure of each blocking element; and where improvements in design can best be made to benefit the safety of the system.

Some of the applications of logic analysis to electrical and electronic systems, with safety implications, include:

(1) Investigation of the possibilities of inadvertent activation of ordnance devices, missile destruct systems, or solid-propellant motors by electrical or electromechanical means.

(2) Failure analysis of such devices as fuel quantity indicators, malfunction detection systems, monitoring systems, and warning systems.

(3) Investigation of interlocks to ensure orderly operation of timed or load-sensitive devices that must be activated sequentially.

(4) Analysis of electrical connectors to determine effects that could be generated from mechanical deficiencies, contamination, or circuits grounded due to a damaged connector. Connectors have generated problems in almost every aerospace system. This method of analysis permits concentrated effort on the most critical connector items.

(5) Determination of fail-safe designs that will produce minimal damage in event of a malfunction of electrical equipment.

6.1.2.7 Pin Fault/Pin Short Analysis (Reference 15) - This technique in complex launch systems involves a computer program for identification of cable connector pin shorting possibilities, in support of a Cable Failure Matrix Analysis (CFMA) Basically, for each connector pin geometry, the application program determines the pin-to-pin and pin-to-shell single event shorting possibilities, based on worst case analysis. The organizational structure of the pinshort program is one of modular development according to functional task. The main program serves as a task manager controlling the calls to computational routines.

Application

The first requirement for implementing a pinshort program is to have a data file describing the connector pin layout. With MIL-C-38999 connectors, for example, the required information can be found in MIL-STD-1560A. The matrix of shoring possibilities is generic with respect to the connector insert arrangement. The analyst determines the proper pattern of pin/function alignments based on the identified shorting possibilities. The pin short program accesses the data filed and produces a printout containing the matrix of pin shorting possibilities.

When the shorting possibility criteria has been met, the spatial geometry of surrounding pins is examined for potential obstructions (closer pins) which can prevent the bent pin from touching the pin in question. These pins are examined by factoring in the worst case positions of the blocking and touched pins based on their specified tolerances. The computations are performed primarily by three routines:

(1) Main Routine - Manage the program tasks for the option (analysis, plot, both) specified by the user.

(2) Subroutine - Compute all shorting possibilities for the object pins.

(3) Subroutine - Determine whether there is an obstructing pin which can prevent the short from occurring. This is accomplished by computing the worst case position of the candidate touched pin relative to the bent pin. Repeat until all pins have been examined as potential blocking candidates or until a block occurs.

Depending on the path taken in the computer data flow the user can obtain a printed output and/or a calcomp plot of the results.

6.1.2.8 Sneak Circuit Analysis (Reference 21 and 22) - Sneak circuit analysis is a system analysis tool which is used to identify and evaluate problems in the design and operation of control systems software. It reports sneak conditions which could affect safety and the reliability of a space, airborne, or ground-based system. Software sneaks are defined as latent conditions, inadvertently designed into the system, which either cause an unwanted function to occur or inhibit a desired function. These conditions occur without regard to system or component failure in the surrounding hardware. The analysis and computer aids are highly systematized and have direct application to verification and validation task efforts. In conjunction with a hardware sneak circuit analysis, cause and effect relationships can be analyzed in the context of the combined hardware-software control system.

The analysis is complete because of the thorough, systematic methodology. The process for a large-scale program involves computer-aided sorting of the data, identifying all current and logic paths, providing accountability for the sequence of elements in these paths, and editing functional errors that may have been generated by personnel error. Next, topological network trees are generated which provide functionally oriented circuits and logic paths which can be easily analyzed for sneak conditions.

This type of analysis is costly in resources and time. For that reason its application should be reserved for suspected high-severity cases which are not amenable to adequate treatment by other techniques. A staff of trained analysts, including experienced instructors to maintain a training program, is required to keep current with new technology and improved analysis methods. Also, this unique technique is proprietary and can only be performed by the Boeing Company. Although the analysis is costly, major benefits may result from the saving of overall project dollars; increased confidence in system safety reliability and operability through independent hardware-software design verification; and fewer development delays from the impact of numerous system modifications. Other types of analysis which require component failure identification or which normally examine only critical functions, do not reveal sneak conditions.

Application

Data used for software sneak analysis includes system requirements, system description, coding specifications, detailed and complete source code, a compilation listing, and operating system documentation. The purpose of the software sneak analyst is to discover program logic which causes undesired program outputs, or inhibits a desired output. The first task is to convert the program source code into a form usable for analysis. This step requires that the code be converted, with reference to an input language description file, into topological network trees.

Once the trees have been drawn, the analyst identifies the basic topoligical patterns that appear in the trees. Six basic patterns exist: the single line, the return dome, the iteration/loop circuit, the parallel line, the entry dome, and the trap circuit. In a system level analysis, code is modeled in terms of impedances, powers, grounds, switches, nodes, and relay coils and switches. Trees are constructed hierarchally, so that program control analysis proceeds from the top down. Although at first glance a given software tree may appear to be more complex than these basic patterns, closer inspection will reveal that the code is actually composed of these basic structures in combination. As each mode in the tree is examined, the analyst must identify which pattern or patterns include that mode. The analyst then applies the topograph specific clues that have been found to typify the sneaks involved with that particular structure. These clues are in the form of questions that the analyst must answer about the use and interrelationships of the instructions that are elements of the structure. These questions are designed to aid in the identification of the sneak conditions in the instruction set which could produce undesired program outputs.

Software sneaks are classified into four basic types:

(1) Sneak output - the occurrence of an undesired output.

(2) Sneak inhibit - the undesired inhibition of an output.

(3) Sneak timing - the occurrence of an undesired output by virtue of its timing or mismatched input timing.

(4) Sneak message - the program message does not adequately reflect the condition.

When potential sneak is identified, the analyst must verify that it is valid. The code is checked against the latest listing. Compiler information may be reviewed concerning the language in question. If the sneak is verified, a software sneak report is written which includes an explanation, system-level impact, and a recommendation for elimination of the sneak.

Following are some analytic methods used in sneak analysis:

(1) Desk checking - verifies compliance of program logic and data flow, and output value correctness.

(2) Code walk-through - a process by which a team of programming personnel do an in-depth logic flow review of a program by inspection.

(3) Structural analysis - an automated tool that seeks and records errors in the structural makeup of a computer program undergoing analysis.

(4) Proof of correctness - the process of using mathematical theorem - providing concepts on a computer program or its design to show it is consistent with its specification.

The sneak analysis specifications are currently listed in MIL-STD-785B, Reliability Program for Systems and Equipment Development and Production.

6.1.2.9 Statistical Methods (Reference 11 and 23) - Such methods are useful tools in accomplishing the quantification of risk in various hazard analyses. Examples would include probability theory, binomial distribution, hypergeometric distribution, Poisson distribution, confidence limits, and math models.

Applications for these probability-type tools can be of great use in the areas of statistical quality control, maintainability, and system effectiveness. The increased use of computer technology for evaluations of safety levels has generated an increase in the use of probabilities for this purpose. Statistical analysis can only augment the reasoning process by introducing some confidence that the reasoning process is accurate. Used improperly statistical analysis can add unnecessary cost; used effectively it can indicate where costs can be avoided through safe design.

Application

The quantitative approach to risk assessment is coming into wider use as the practitioners of the methods become educated, management demands a justification for the resources devoted to risk control, and the methods grow in their sophistication. The use of computers for system analysis requires a rigorous logic and invites quantification as an aid to assessment of hazard. Statistical methods allow one to account for the uncertainty in making predictions of future losses in accidents. A synopsis of a few of the most useful concepts for the system analyst is as follows:

(1) Probability Theory - Probability is the principal predictive descriptor for the analyst. A probability value is defined as the ratio of the number of ways an event may occur in a specified

manner to the total number of ways the event may occur. The larger the sample size, the more likely it is that the probabilities computed approximate the true values that may be obtained with an infinite sample.

There are three laws that are most useful in calculations involving probability values:

(a) The addition law - you may add the probabilities of events if any one of the events will satisfy the specification of the outcome of system function, if the events are mutually exclusive. Even if the events may not be mutually exclusive, in safety situations, the probability found is a conservative bound on the true value.

(b) The multiplication law - this law can be applied whenever the probability space describing a situation can be divided into two parts that encompass every possible outcome of the system function. Thus, in an accident system, we may talk of some number of accidents occurring or not occurring. The complementary law may be used to compute the more difficult probability of any accidents occurring through the complement of the probability of no accidents.

(2) Statistical Measures - In gathering descriptive data about the state of safety of a system, certain characteristics of the data help to describe the nature of the data sets, assist in the decision-making process, and allow one to describe this state more readily to others.

(a) Measure of central tendency - these single-valued descriptors are frequently used when it is desirous to represent an entire data set with a single value. Useful measures are the mode, median, arithmetic mean, and geometric mean.

(b) Measures of dispersion - these describe how widely the data are separated from some measure of central tendency. Such measures indicate the fundamental variability of the data originating from a system, and evaluate how representative the measure of central tendency is. Measures of dispersion are vital in statistical inference calculations. Typical measures are range, average deviation, and standard deviation.

(3) Binomial Distribution - In safety, systems or situations that behave in accordance with the Bernoulli process are frequently encountered - that is, they have the two characteristics of such a process. These are:

(a) The events or outcomes of system function may occur in only two ways.

(b) The probability of a particular outcome of one trial or function is stationary, or the probability remains constant from trial to trial.

In examining gross accident statistics, the Bernoulli process is the one that may govern the generation of statistical data; the accident either occurs or it doesn't.

(4) Normal Distribution - The normal (Gaussian) distribution is a continuous distribution, although it can be used to describe phenomena which are discrete (outcomes associated with foxed values). The normal distribution takes the form of a bell-shaped curve with the ordinate describing the frequency of real-world values, which are plotted along the abscissa. Since the normal distribution is continuous, and the height of the curve is frequency, the height can be considered the probability density of any point or value along the abscissa. An area beneath the curve therefore represents probability of the occurrence of the real-world values that bracket the area. A good application would be calculation of the probability that a pressure switch will function at a given pressure value, or at a pressure between two values.

(5) Poisson Distribution - The binomial distribution dealt with a finite number of opportunities or exposures for an event to occur. The distribution was discrete. The Poisson distribution enables the analyst to compute the number of events that may occur in a case of infinite exposure or infinite opportunity for the occurrence. The distribution remains discrete. A good application would involve aircraft accidents. How many accidents may occur in 1000 hours of flight, given an accident rate for the aircraft to be flown? The binomial distribution could provide probabilities for no more than 1000 accidents, since it assumes that only one accident may occur in an hour. The Poisson will allow the computation of the probabilities of as many accidents as we please, because it assumes infinite exposure for the event to occur. The Poisson series has an infinite number of terms while the binomial has a finite number of terms. However, the Poisson probability law may be applied only to a process that is dichotomous, stationary, and independent, just as with the binomial.

(6) Confidence Limits - When a complex system is allowed to function a large number of times, the outcome will not be the same for each function, as there are different mean times to failure under the same operating stress. The accident propensity of this system will yield different accident results, both in terms of differing severities as well as different rates of occurrence. Chance cause system events occur with differing frequency and thus interactions differ somewhat from operation to operation to vary the output. We cannot predict with exactitude the true mean system accident rate. Given the rate that does manifest itself, the probability of some number of future event occurrences, given the future exposure, can be predicted. The solution to this problem is to use statistical methods to allow us to estimate a range in which we wish the true system parameter to lie, or to specify a confidence that the range does include some computed value. The larger the risk we are willing to accept in making an estimate of the range of certain values, the smaller this range

needs to be. However, if we demand a small risk, or large confidence, the range must be quite large, given the same basic estimated data. Thus, as the confidence requirement is increased, the range must also increase with the same sample of system performance. Safety analysts are more concerned with making the conservative prediction about future performance than they are with showing how good things may possibly be. The conservative estimate in safety is thus the pessimistic bound on the parameter in question, and one that would be more acceptable to management.

6.1.3 Methodology Source Matrix

Table 6-1 and Table 6-2 summarize the Annotated Bibliography sources for the quantitative and qualitative methods respectively. Each document in the tables is identified by its Annotated Bibliography reference number. The tables distinguish between documents which pertain to the theory or concept of a particular analysis technique, and those documents that pertain to the practical application of that technique.

Table 6-1 Quantitative Hazard Analysis Sources

Quantitative Technique	Conceptual*	Vehicle Usage*
Cable Failure Matrix Analysis	454	
Event Tree	199-439-	051-318-
Failure Modes and Effects Analysis	022-064-065-308-199 200-430-456-457-021	039-050-076-077-281 305-318-334-457
Fault-Tree Analysis	022-044-064-065-308 097-430-440-021	044-
Management Oversight and Risk Tree	063-064-065-308-100 199-429-439-	
Network Logic Analysis	022-044-440-021-430	
Pin Fault Analysis	454-	
Sneak Circuit Analysis	308-429-455	
Statistical Methods	044-065-184-190-199 200-210-211-221-232 280-400-429-202-453 457	030-051-076-077-082 004-171-172-281-302 303-304-305-318-321 327-342-357-358-402

*Numbers refer to items in annotated bibliography.

Table 6-2 Qualitative Hazard Analysis Sources

Qualitative Technique	Conceptual*	Vehicle Usage*
Change Analysis	439-	015-071
Contingency Analysis	022-184-190-197-439-021	024-170-171-172-244
Critical Incident Technique	022-	023-170-171-172-340-342
Energy Analysis	022-065	
Flow Analysis	022-065-199	
Interface Analysis/System Hazard Analysis	022-044-064-065-308 4390453	015-016-023-045-049 288-312-342-356-440
Job Safety Analysis	065-308-199-333-439 440-	
Maximum Credible Accident/Worst Case Condition (Fault)	064-065-308-430-021 022	024-
Naked Man	439-	
Operating Hazard Analysis/ Procedure Analysis	022-044-064-065-308 199-439-440-453-021	015-016-023-045-161 312-342-356-431
Preliminary Hazard Analysis	044-064-065-308-430-439-440-453-021	045-342
Prototype	184-190-199-200-202-221-022	039-082-292-294-302-303-304-305-318-321-358-431
Scenario	194-199-202	043-049-050-051-281 292-342-358-305
Software Safety Analysis	439-430-202-439-455	281-292-454
Subsystem Hazard Analysis	022-064-308-440-453	015-016-023-045-048 049-288-312-342-356-357-402-431
No Identifiable Technique	042-204-206-242-243 216-275-361	
Low Application for SPHAM	053-062-203-205-207 284	

6.2 HAZARDOUS SUBSYSTEM METHODS

This section discusses hazards analysis from the viewpoint of hazardous subsystems. A hazardous subsystem is a collection of the energy and toxic sources by type, e.g., propellants, pressure, RF, etc. A complete discussion of hazards analysis methods for hazardous subsystems would include:

(1) methods to determine energy and toxicity level at the source and probable release resulting from loss of control,

(2) methods to establish human, hardware and environmental susceptibility to the hazard and limits to the release

(3) methods to identify or synthesize and evaluate control of the hazard within a hazardous subsystem.

Methods fully meeting these requirements were not available for this edition of SPHAM. The data included in this section was extracted from the Accident Risk Assessment Report (ARAR) Handbook, Chapter IV (February, 1987). This Handbook is being developed by the USAF to aid contractors in preparing accident risk assessment reports (ARAR) to Data Item Description (DID) DI-S-30565 for payloads flying on NSTS. This DID requires the development of data and analysis by hazardous subsystem. Properly formatted and detailed ARARs generally satisfy the pre-launch safety package data requirements of ESMC and WSMC. The Chapter IV data is included here to partially illustrate the approach and guidelines for the conduct of hazards analysis by hazardous subsystem, specifically on the Multipurpose Satellite System (MPS). NOTE: The ARAR Handbook is not release as of September 1, 1987. Interested inquiries can be made to the System Safety Office, Space Division, USAF.

6.2.1 MPS General System Overview

Multipurpose Satellite (MPS) System consists of the Multipurpose (GSE) satellite, its airborne support equipment (ASE), and ground support equipment. The MPS satellite utilizes the Space Transportation System (STS) and requires no upper stage. MPS is a retrievable, geosynchronous satellite that uses a laser to calibrate ground-based optical sensing devices. These ground-based optical sensing devices are not within the scope of this document. Figures 6-1, 6-2, and 6-3 illustrate the undeployed and deployed MPS.

The following is a synopsis of the MPS subsystems and their basic function:

(1) Structure. The S/C structure provides the load paths for environmental forces and serves as the supporting member for attaching S/C hardware.

(2) Attitude Control System (ACS). The ACS is a combination of momentum wheels and a monopropellant propulsion system that positions and stabilizes the S/C on orbit.

(3) Apogee Thrust System (ATS). The ATS is a solid rocket motor which transfers the S/C from an elliptical orbit to a circular orbit.

(4) Bipropellant Motor System (BMS). The BMS is a bipropellant liquid propulsion system which puts the S/C into its elliptical orbit and also provides capability to change orbital parameters. It is the means by which the MPS can return to low earth orbit for retrieval or servicing.

(5) Space Communications System (SCS). The SCS is the RF data link for the S/C.

(6) Command and Decoder System (CDS). The CDS receives and decodes commands and transmits signals to perform the required functions.

(7) Electrical Distribution System (EDS). The EDS takes power from the batteries and solar arrays and distributes it throughout the S/C.

(8) Deployment System. The deployment system consists of S/C and solar array and equipment deployment mechanisms.

(9) Table 6-3 is a listing of hazardous subsystems onboard the S/C.

The following is a summary of S/C operations:

(1) Ground Operations (ELS):

(a) Skid Strip: S/C and GSE arrival

(b) SPIF Integration Cell: Assembly, checkout and fueling

(c) Pad 39: Final checkout and launch

(d) Solid Propellant Storage Area: Ordnance storage (solid motor is shipped in by truck)

(e) Propellant Servicing Facility: Propellant Carts Loading

(2) Flight Operations:

(a) T = 0. All S/C power off

(b) T +20 min. S/C heaters are powered through ASE

(c) T +12 hrs, 30 min. ASE mechanism releases

(d) T +12 hrs, 50 min. Cargo Element is deployed

(e) T +13 hrs. Safe distance from the Orbiter is achieved

(f) T +13 hrs, 35 min. S/C times run out; S/C gets power

Table 6-3 MPS Hazardous Subsystem Summary

Structure: Primarily aluminum with some beryllium and composite material

Mechanisms: Equipment wing release and deploy mechanism
Laser gimbal mount release and deploy mechanism
Antenna release and deploy mechanism
Momentum wheels (2)
S/C separation system
ASE release mechanism

Ordnance: 2000# solid rocket motor (Apogee Thrust System)
TBD EEDs for appendage and S/C release

Propulsion: 5600# MMH, 7200# NTO (Bipropellant Motor System)
800# N2H4 (Attitude Control System)
(See also ordnance)

Pressure: 400 psi for BMS launch pressure (helium/bipropellants)
4000 psi for BMS on-orbit repressurization (helium)
300 psi for ACS (nitrogen/hydrazine)
1000 psi for Nickel Hydrogen Battery Cells (40)
100 psi for heat pipes (ammonia)
50 psi for laser cooling (liquid methane, cryogen)

Sealed Containers: Nickel Cadmium battery
Momentum wheels housing

RF: 15 GHz, 100W, 30 dB
12 GHz, 10W, 20 dB

Iodizing Radiation: Atomic Clock (TBD millicuries, cesium)
Laser Voltage X-rays

Electrical: Nickel Hydrogen Batteries (S/C power)
Nickel Cadmium Batteries (laser power)
Solar Arrays (2)

6.2.2 System (Design) Hazard Analysis

We use the term system (design) hazard analysis to mean an analysis to identify subsystem hardware design hazards, that is to say, identifying hazards which are inherent in the design of the subsystem as opposed to how they are used (operating hazard analysis) or with what they are used (integrated or interface hazard analysis). The Multipurpose Satellite is used here as an example.

(1) The first step in performing a system (design) hazard analysis is to divide the system into manageable entities, e.g., divide a satellite into its functional subsystems. Refer to the list generated for the System Overview.

(2) Identify toxic material and energy sources, identify the hazardous subsystems which relate to the functional subsystem, e.g., The Attitude Control Subsystem: hydrazine, mechanisms, spring force, Deployment Subsystem: ordnance, spring force.

(3) Organize the hazard analysis. The hazardous subsystems can be analyzed with the following approach:

(a) Structure: Primarily aluminum with some beryllium and composite material

(b) Mechanisms: Equipment wing release and deploy mechanism
Laser gimbal mount release and deploy mechanism
Antenna release and deploy mechanism
Momentum wheels (2)
S/C separation system
ASE release mechanism

(c) Ordnance: 2000# solid rocket motor (Apogee Thrust System)
TBD EEDs for appendage and S/C release

(d) Propulsion: 5600# MMH, 7200# NTO (Bipropellant Motor System)
800# N_2H_4 (Attitude Control System)
(See also ordnance)

(e) Pressure: 400 psi for BMS launch pressure (helium/bipropellants)
4000 psi for BMS on-orbit repressurization (helium)
300 psi for ACS (nitrogen/hydrazine)
1000 psi for Nickel Hydrogen Battery Cells (40)
100 psi for heat pipes (ammonia)
50 psi for laser cooling (liquid methane, cryogen)

(f) Sealed Containers: Nickel Cadmium battery
Momentum wheels housing

(g) RF: 15 GHz, 100W, 30 dB
12 GHz, 10W, 20 dB

(h) Ionizing Radiation: Atomic Clock (TBD millicuries, cesium)
Laser Voltage X-rays

(i) Electrical: Nickel Hydrogen Batteries (S/C power)
Nickel Cadmium Batteries (laser power)
Solar Arrays (2)

(4) Set up hazard analysis worksheets as necessary. These worksheets would identify the functional subsystem and the specific hardware being assessed. For example: Attitude Control Subsystem (functional), propulsion subsystem (hazardous), and valves (specific hardware). The worksheets should identify any undesired event (hazard), the effect (end event), contributing factors (causes), controls and verifications.

The following procedure can be employed to identify hazards and their possible causes. The essential ingredient is imagination. "Brainstorming" is a healthy approach to identification of hazards and hazard causes. See Figure 6-4.

Level 1. Determine the specified operating parameters/interfaces including environments. The hazard analysis will only be valid for what is defined as "spec conditions". It is therefore essential to identify expected operating parameters/interfaces, including environments, which exceed specifications. For example, if the subsystem is designed for 3Gs, but it can expect to see 5Gs during an emergency landing in Spain, it is essential to identify the risk involved. A decision is necessary to redesign or preclude an emergency landing in Spain. Other considerations include:

(a) High temperature (e.g. direct sun)

(b) Low temperature (e.g. deep space)

(c) Electromagnetic (e.g. RF susceptibility)

(d) Chemical (e.g. reactivity, flammability, or viscosity)

(e) Electrical (e.g. 110 or 220 volts)

(f) Service life (e.g. one shot or reusable)

(g) Shelf life (e.g. perishable)

(h) Cycle life

(i) Handling (e.g. manually or mechanically)

Level 2. Determine how the subsystem works and then analyze how it fails. Safety-type failures involve events that must not happen or high safety factors are necessary. Reliability type failures involve events that should not happen so provide redundancy or involve strict quality control to avoid failure.

Note: If the PHA identifies a hazard of inadvertent valve opening, the subsequent hazard analyses may want to establish a level 2.5 which addresses inadvertent opening of specific valves.

Level 3. Determine when in the program life cycle failure modes can be built-in to the subsystem and then assess how. For example, during design, there are several ways to "build-in" a failure into a subsystem:

(a) Bad input. Design analysis has to be based on the correct operating parameters/ interfaces and environments in order for it to be valid.

(b) Bad analysis. Design analysis has to be based on the proper assumptions and equations in order for it to be valid. The mate has to be right too!

(c) Bad Design. The designer has to select the right components and arrange them in such a way that the subsystem will work safely. For example:

(d) Materials: Don't select materials which are susceptible to *stress corrosion*, flame propagation, static build-up, etc.

(e) Safety factors: Derate the strength of your materials, the correct capacity of your wires, etc.

(f) Sneak circuits: Control the energy paths in your subsystem.

(g) Other: Comply with safety related design requirements!

(h) Bad Communication. The designer has to communicate with the supplies, builders, users, so that a safe system on the drawing board becomes a safe system. Proof reading specifications drawings and procedures for typo's is also not a bad idea.

(i) Manufacturing/Assembly. During manufacturing/assembly, there are several ways to "build-in" a failure into a subsystem.

(j) Bad parts/materials. This gets into the issue of high reliability parts and quality control to include acceptance testing and inspection.

(k) Bad process/method. Examples of bad processing (fabrication) would be insufficient bake-out of plated parts to prevent hydrogen embrittlement or curing time for adhesives or concrete. Bad methods (assembly) would be when hardware is damaged even though procedures are followed, for examples a test fixture which applies unintentional stresses on a pressure vessel.

(l) Unplanned events. This includes human errors such as failing to seal a component during manufacturing or dropping the component during assembly. It would also include mismated connectors, damaged O-rings and bent pins.

(m) Other. There are a lot of ways for a subsystem to be doomed to failure between the time it leaves the designer to the time it is actually used. Of the above list concentrate on the obvious.

(n) Random failures. Random failures mean that the subsystem fails regardless of safety precautions. The standard way of protecting against random failures is to add extra inhibits or provide redundancy.

(o) Functioning. If a subsystem is properly designed and properly built, the only way it can fail when used is by experiencing a random failure or out of spec operating condition. The most common out of spec operating condition is human error, e.g., throw the switch at the wrong time. Revisit our level 1 discussion.

(p) Other. Depending on the system, other elements in the program life cycle such as maintenance, demolition, retrieval, refurbishment or emergencies must be considered.

(5) Extract the relevant information out of the worksheets and factor them into the subsystem descriptions and hazard reports.

6.2.3 Integrated Hazard Analysis

An integrated hazard analysis looks at the hazards of integrating a particular subsystem with the remaining subsystems on the system (e.g., satellite). For example, all of the designs for an Attitude Control System can be examined without identifying all of its associated hazards. Integration of the ACS into the overall satellite must be examined to recognize possible problems. The most common problem is accessibility, e.g., fill and drain valves look fine on a mechanical schematic, but when the fully assembled satellite is examined, it is noted that somebody placed a solar panel in the way.

In order to take a rigorous approach to integrated hazard analysis, address hazards by hazard "source" rather than hazard "result", e.g., the RF initiation of ordnance is identified when assessing the RF subsystem rather than the ordnance subsystem. In other words, assess the specific subsystem effects on the other subsystem.

A. Integrated Hazard Analysis (General)

If the system (e.g., satellite) contains a particular hazardous subsystem, there are some basic hazards which should be anticipated when doing the integrated hazard analysis. An integrated hazard analysis should be performed as follows:

(1) Structural Subsystem. Look at the problems which the structural subsystem may cause other subsystems.

(a) Accessibility. Satellite structure can create accessibility problems for all of the other subsystems, e.g., access to arm plugs or fill and drain valves.

(b) Structure. Problems which structural items have when integrating with each other is really a system (design) hazard analysis problem, but it is mentioned here. The problems can be:

- o Transmission of unsafe loads whether they be static or dynamic
- o Inadequate attachment whether it be by design or procedural error
- o TBD

(c) Mechanisms. Same integration hazards as structure, but also:

- o Inadequate clearances between mechanism and structure

(d) Ordnance. Same integration hazards as structure, but also:

- o Inadequate ground plane, e.g., poor bonding

(e) Propellants/Propulsion. Same integration hazards as structure, but also:

(f) Pressure. Same integration hazards as structure, but also:

(g) RF Radiation. Same integration hazards as structure, but also:

- o RF interference affecting transmission or reception
- o RF focusing creating increased EMI on other circuits

(h) Optical Radiation. Same integration hazards as structure, but also:

(i) Electrical. Same integration hazards as structure, but also:

- o Inadequate ground plane, e.g., poor bonding
- o Abrasion/shorting hazard to cable harness
- o Increased EMI caused by cable harness proximity to ground plan of satellite structure
- o TBD

(j) Ionizing Radiation. Same integration hazards as structure, but also:

(k) Hazardous Materials.

- o Material compatibility

(2) Ordnance Subsystem.

(a) Accessibility. The location of the satellite ordnance subsystem can create accessibility problems for other subsystems.

(b) Structure.

- o Pyro shock concerns
- o Unsafe loads, e.g., the kick motor is too heavy

(c) Ordnance. Problems which ordnance items have when integrating with other elements of the ordnance subsystem is really a system (design) hazard analysis problem. The problem may be:

- o Mismated connectors or other connector problems
- o Improper grounding and bonding
- o Failure to maintain shielding continuity
- o Pyro shock concerns when one ordnance item is fired and it effects either the circuitry or ordnance items elsewhere in the satellite
- o EMI between circuits
- o Miswired circuits
- o Failure to maintain inhibit independence

(d) Propellants/Propulsion

- o Pyro shock
- o Structural/accessibility concerns which require propellants to be loaded prior to solid motor mating
- o Inadvertent firing of a squib valve
- o Failure of a squib valve to properly activate
- o TBD

(e) Pressure.

- o See propellants/propulsion

(f) RF Radiation

- o Pyro shock

(g) Optical Radiation

- o Pyro shock

(h) Ionizing Radiation

- o Pyro shock

(i) Electrical

- o Pyro shock
- o Pin-to-case shorting
- o Solid motor offgassing (coupled with electrical subsystem ignition source)

(j) Hazardous Materials

- o Material compatibility

(3) Propellants/Propulsion Subsystem.

(a) Accessibility. The location of the satellite propulsion subsystem can create accessibility problems for other subsystems.

(b) Structure.

- o Unsafe loads

(c) Ordnance.

- o (Internal subsystem for flight hardware not ground hardware)

(d) Propellants/Propulsion. Problems which propulsion items have when integrating with other elements of the propulsion subsystem is really a system (design) hazard analysis problem, but to play it safe we will mention it here. The problems you can have are:

- o Mismated connectors or other connector problems
- o Improper ground and bonding
- o Inadequate mechanical connections (e.g., welds)
- o Miswired circuits
- o Misrouted plumbing
- o Failure to maintain inhibit independence

(e) Pressure.

- o (See propellants/propulsion)

(f) Electrical.

- o Leak/ignition source hazard

(g) Hazardous Materials.

- o Material compatibility

(4) Pressure Subsystem.

(a) Accessibility. The location of the satellite pressure subsystem can create accessibility problems for other subsystems.

(b) Structure.

- o Unsafe loads

(c) Ordnance.

- o (Internal subsystem for flight hardware not ground hardware)

(d) Propellants/Propulsion. Problems which involve pressurized components of a propulsion subsystem are really a system (design) hazard analysis concern, but it will be mentioned here. The problems can be:

- o Inadvertent pressurization
- o Inadvertent pressure loss (for a pressure supported structure)
- o Failure to pressurize properly

(e) Pressure. Problems caused by integrating pressurized components of a pressure system are really a system (design) hazard analysis problem, but it will be mentioned here. The problems can be:

- o Same problems mentioned above for propulsion
- o Inadequate mechanical connections

(f) Hazardous Material.

- o Material compatibility
- o TBD

(5) RF Radiation Subsystem.

(a) Accessibility. The location of the RF radiation subsystem can create accessibility problems for other subsystems.

(b) Structure.

- o Unsafe loads

(c) Ordnance.

- o RF initiation of EEDs
- o DC initiation of EEDs caused by RF activation of inhibits
- o RF/electrostatics coupled with solid motor offgassing
- o RF dudding
- o RF damage to circuits

(d) Propulsion/Propellant.

- o RF/electrostatics and vapor leaks
- o RF initiation of inhibits

(e) Pressure.

- o RF initiation of inhibits

(f) RF Radiation. Problems caused by integrating the RF subsystem with itself are really a system (design) hazard analysis problem, but it also will be mentioned here. The problems can be:

- o EMI between circuits which can either damage these circuits, inhibit these circuits or cause inadvertent RF radiation
- o Inadequate wave guide connection (leakage)

(g) Optical Radiation.

- o EMI which can damage circuits, inhibit circuits or cause inadvertent optical radiation

(h) Ionizing Radiation.

- o EMI which can damage circuits, inhibit circuits or cause inadvertent ionizing radiation.

(i) Electrical.

- o EMI which can damage circuits, inhibit circuits or cause inadvertent activation of circuits

(j) Hazardous Materials.

- o Material compatibility
- o RF/electrostatics and vapor leakage concerns

(6) Optical Radiation Subsystem.

(a) Accessibility. The location of the satellite optical radiation subsystem can create accessibility problems for other subsystems.

(b) Structure.

- o Unsafe loads

(c) Ordnance.

(d) Propulsion/Propellants.

- o Heating or laser penetration

(e) Pressure.

(f) Ionizing Radiation.

(g) Electrical.

(h) Hazardous Materials.

- o Material compatibility
- o TBD

(7) Ionizing Radiation Subsystem.

(a) Accessibility. The location of the satellite ionizing radiation subsystem can create accessibility problems for other subsystems.

(b) Structure.

- o Unsafe loads

(c) Ordnance.

- o Inadvertent activation of EEDs

(d) Propellants/Propulsion.

(e) Pressure.

(f) RF Radiation.

(g) Optical Radiation.

(h) Ionizing Radiation. Problems which the ionizing radiation subsystem has when integrating with itself are really a system (design) hazard analysis concern, but will be mentioned here.

- o Inadequate shielding caused by poor design or procedure

(i) Electrical.

(j) Hazardous Material.

- o Material compatibility

(8) Electrical Subsystem.

(a) Accessibility. The location of the satellite electrical subsystem can create accessibility problems for other subsystems.

(b) Structure.

(c) Ordnance.

- o Power failure.
- o Sneak circuits or EMI

(d) Propellants/Propulsion.

- o Power failure.
- o Sneak circuits or EMI
- o Ignition source/leakage

(e) Pressure.

- o Power failure.
- o Sneak circuits or EMI

(f) RF Radiation.

- o Power failure.
- o Sneak circuits or EMI

(g) Optical Radiation.

- o Power failure
- o Sneak circuits or EMI

(h) Ionizing Radiation.

- o Power failure
- o Sneak circuits or EMI

(i) Electrical.

(j) Hazardous Materials.

- o Material compatibility
- o Ignition source/leaks or flammable materials

(9) Hazardous Materials. Address as above.

(10) Thermal Subsystem. Address as above.

(11) Command & Decoder

B. Integrated Hazard Analysis (Specific)

(1) Read through the generalized integrated hazard analysis and see what can be added to it. The examples presented above are to encourage thinking of possible hazards.

(2) For each item that has a system (design) hazard analysis worksheet, perform an integrated hazard analysis. Determine specific hazards, causes and controls.

Note: Remember if an analysis of a subsystem (e.g., propulsion) by its major components (e.g., valves, lines, etc.) is performed, the hazards when those items are integrated must also be assessed. The obvious integration hazard for a valve is when its nonhazardous failure couples with another valve's nonhazardous failure to cause a hazardous event such as thruster firing.

(3) Incorporate integrated hazards into the hazard reports as appropriate.

6.2.4 Operating Hazard Analysis

The first step in an operating hazard analysis is identification of the operations involved. This is an iterative process. Using an Attitude Control System as an example.

(1) Phase 0. At Phase 0, the following ACS operations should be recognized:

(a) Pressure demo and leak test
(b) Load S/C

(2) Phase 1. The list expands.

(a) Pressure demo and leak test
(b) Load S/C
(c) Pressurize S/C
(d) Depressure S/C (contingency)
(e) Offload S/C (" ")
(f) Flush S/C (" ")
(g) Purge and vacuum S/C (" ")

(3) Phase 2. A functional test may be added to the list.

(4) Phase 3. The ACS procedures should be assessed. The list can become very large recognizing the number of tasks involved with a small number of procedures. For example, in order to perform a pressure demo and leak check, a flex hose must be attached from the GSE to the S/C. At some point in time it will be necessary to determine if there is a concern over that particular task. If the leak test is with radioisotope tracer gas, there is an obvious leakage concern. If the leak test pressure is greater than 150 psi, there is a concern regarding flex hose restraint. What is the result if the flex hose is damaged or broken?

The second step in an operating hazard analysis is to analyze the operation:

(1) Preliminary OHA. The term OHA is used to address the identification of operationally unique hazards created by the types of operations that will be performed. Please note that type of operation means something specific like "S/C loading" and not something as generic as "propellant operations". The results of the preliminary OHA should be reflected in the hazard reports or in the procedures section of the ARAR as appropriate.

(2) Detailed OHA. The term "detailed OHA" means the identification of operationally unique hazards created by specific tasks performed within a particular procedure. In industrial engineering terms it would be called a "task analysis". The

brunt of the matter is that some level of subtasks for each procedure, short of assessing each individual step of each procedure, must be assessed. Ultimately this will be accomplished by the review and approval of each procedure. A prime purpose of the OHA is to be a tool to ensure that the right controls are in a procedure before it reaches its final revisions.

(3) Integrated OHA. Besides having a better idea of what the ACS condition will be during prelaunch operations, a better idea of what other subsystems or systems are doing and how it may affect the ACS should be known. For example, when is installation of the satellite kick motor planned with respect to ACS loading? When will the upper stage be fueled? When will the STS be fueled? This will affect planning and may create a hazard. If a lot of testing after propellant loading is necessary, an obvious hazard exists. It's not really a new hazard, but it constitutes increased risk. The integrated OHA identifies increased risks as individual subsystems and other systems conduct operations. These increased risks may require documentation in hazard reports, but as a minimum they should be discussed in the ARAR procedures section.

6.2.5 Interface Hazard Analysis

Whereas an integrated hazard analysis looks at interfaces between subsystems, an interface hazard analysis looks at interfaces between the system (e.g., satellite) and other systems.

The following satellite interfaces must be identified and assessed:

(1) GSE
(2) Upper Stage
(3) Orbiter
(4) Facility
(5) ASE
(6) Other cargo elements

The following GSE interfaces must be identified and assessed:

(1) Satellite
(2) Upper Stage
(3) Orbiter
(4) Facility
(5) ASE
(6) Other cargo elements

Note: Satellite-GSE interfaces are normally discussed in the GSE section of an ARAR.

An illustration of an interface hazard analysis:

Suppose a piece of propulsion GSE has completed a thorough design analysis to ensure that all the right safety factors exists and adequate relief valves are included. Is there confidence that no hazards exists? The answer should be no if an interface hazard analysis (in conjunction with an operating hazard analysis) has not been performed. Is it known if the GSE would be pressurized by a 6000 psi facility nitrogen source instead of a 2000 psi k-bottle? Or if there are relief valves in the circuit which pressures the S/C? Are there relief valves in the circuit which purges the S/C?

6.2.6 Structural Failures

We'll use the design hazard analysis methodology we provided to analyze the MPS structural subsystem.

Refer to Figure 6-5 outlining the hazard analysis applicable to most structures. It is suggested you apply brainstorming techniques to add to the "other" entries and examples.

Let's apply the analysis to the MPS. We know that blocks 1, 2, 3, and 4 need to be addressed. We also know that in presenting these "hazards" to the safety review team, we ned to consolidate the information that is scattered throughout our hazard analysis worksheets. This is done in the hazard reports. Let's discuss on the topics for our MPS hazard reports:

Block 1: Failures involving out of spec operating conditions. We don't need a hazard report dedicated for this situation, but we do need to recognize these situations as potential hazard causes. For example, one way for a piece of structure to yield/fracture is for it to see 5 Gs when it was only designed to 3 Gs. If 5 Gs is an expected environment, then it needs to be addressed as a hazard cause.

Block 2: Yield/Fracture.

(a) The first question to ask is whether or not to address all structure in a single hazard report. In general, the answer is yes because of common concerns.

(b) The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and operations. In general, the answer is no because a single hazard report is usually manageable.

(c) The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard cause, e.g., stress corrosion is a special interest item. In general, the answer is no. As it happens stress corrosion is enough of an issue in the STS arena that Material Usage Agreements are required.

(d) The fourth question to ask is whether or not to combine this hazard report with another. In this case the answer is no, but the structural failure hazard report will be referenced in many other hazard reports.

Block 3: Separation bolt failures. The separation bolt is the only reliability-type structural failure element on the MPS. Failure of separation bolts becomes a safety concern when the failure of a bolt would put the orbiter into a catastrophic hazard situation, e.g., the S/C has 8 separation bolts; failure of any one would "hang up" the S/C prevent deployment and STS return to earth. At this point, instead of making this a single hazard report, it was decided to include the concern in hazard report entitled "Deployment Hazards".

Block 4: Other. Never say that these are all the hazards that need to be addressed. Remember, that integrated, operating, and interface hazard analyses must be performed. In performing an OHA on the deployment activity the above mentioned design failures plus other potential problems such as deployment dynamics and clearances will be assessed.

The causes of structural failure may be:

(1) Out of spec conditions (which have been discussed).

(2) Designed-in failures such as inadequate safety factors or materials susceptible to stress corrosion.

(3) Manufactured-in failures such as hydrogen embrittlement or undetected damage during test or assembly.

(4) Random failures, or single point failures, may be considered non-credible given proper design, manufacture and assembly, but it is better to provide redundant load paths and multiple welds.

(5) Other. The above list is not all inclusive.

Conclusion: A single hazard report called "Structural Failure".

6.2.7 Mechanism Failures

Use the design hazard analysis methodology provided in this chapter to analyze the MPS mechanisms.

On the previous page is a hazard analysis applicable to most mechanisms. It is suggested that you apply brainstorming techniques to add to the "other" entries and examples. For further discussion on Design Hazard Analysis see Section 6.2.2.

Let's apply the analysis to the MPS. Blocks 1, 2, 3, and 4 (Figure 6-6) need to be addressed. It is also known that in presenting these "hazards" to the safety review team, it is necessary to consolidate the information that is scattered throughout the hazard analysis worksheets. This is done in the hazard reports. Let's discuss topics for the MPS hazard reports:

Block 1: Failures involving out of spec conditions. A hazard report dedicated for this situation is not needed, but we do need to recognize these situations as potential hazard causes. For example, a mechanism may be designed to only operate in 0 G as opposed to 1G.

Block 2: Inadvertent Equipment Wing Movement. The first question is whether or not to address all mechanisms in a single hazard report. Even before we started our flow chart we knew that each mechanism needed to be addressed separately

(a) The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and functioning. In general, the answer is no because a single hazard report is usually manageable.

(b) The third question is whether or not separate hazard reports are needed for any special failure mode or hazard cause, e.g., pinpuller failure vs drive motor failures. In general, the answer is no. The mechanism hazard report will be shortened by cross-referencing to the "structural failure" and "inadvertent EED firing" hazard reports.

(c) The fourth question is whether or not the inadvertent equipment wing deployment hazard report can be combined with another hazard report. Since we're already using the "structural failure" and "inadvertent EED actuation" hazard reports, the only issue left is inadvertently activating the drive motor. If we assume this is not a problem for our MPS, we do not need a hazard report.

Block 3: Failure of ASE Mechanism. We would use the same rationale as with inadvertently activating the equipment wing. When it comes down to see if we can combine this with another hazard report, we would select our "Deployment Hazards" hazard report.

Block 4: Other. Keep asking questions until you are convinced you've identified all the hazards.

Conclusion: A separate hazard report for inadvertent equipment wing deployment hazard report is not required. The same rationale can be applied to the other mechanisms. Therefore, one hazard report entitled "Mechanism Failure" will suffice.

6.2.8 Ordnance Failures

The design hazard analysis methodology provided is used to analyze the MPS ordnance subsystem.

On the following page is a hazard analysis applicable to most ordnance subsystems. Suggest applying brainstorming techniques to add to the "other" entries and examples. For further discussion on Design Hazard Analysis, see Section 6.2.2.

Applying the analysis to the MPS, blocks 1, 2, 3, and 4 (Figure 6-7) need to be addressed. Also recognized is that in presenting these "hazards" to the safety review team, there is a need to consolidate the information that is scattered throughout the hazard analysis worksheets. This is done in hazard reports. Discussed below are the topics for our MPS hazard reports:

Block 1: Failures involving out of spec operating parameter interfaces, including environments. A hazard report is not selected for this dedicated situation, but recognize these situations as potential hazard causes. For example, one way for an ordnance item to inadvertently function is for it to see 400°F when it was designed never to see more than 300°F.

Conclusion: Address out of spec conditions as hazard causes.

Block 2: Inadvertent functioning.

(a) The first question to ask is whether or not to address all ordnance in a single hazard report. In general, all EEDs are addressed in a single hazard report because of common concerns. In addition, the MPS also has a solid rocket motor which has some unique concerns, e.g. electrostatic ignition of propellant grain. Rather than try to force this into an EED hazard report or have a separate SRM hazard just for this one concern, address it in the ARAR ordnance subsystem description, subject to safety review team concurrence.

(b) The second question to ask is whether or not separated hazard reports are needed for design, manufacturing and functioning. In general, the answer is no because a single hazard report is usually manageable.

(c) The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard cause, e.g., electrostatic discharge is a special interest item. In general, the answer is no.

(d) The fourth question is whether or not to combine this hazard report with another hazard report. In general, the answer is no because it would have to be combined with several hazard reports which involve inadvertent ordnance firing. It is difficult to get a full understanding of ordnance concerns and controls with this approach.

Conclusion: A single hazard report called "Inadvertent firing of EEDS" is required.

Block 3: Failure to Function.

(a) The first question to ask is whether or not to address all EEDs in a single hazard report. For the MPS, the answer is easy because the separation bolts are the only EEDs with a failure to function concern. (Regardless the answer would be one hazard report.)

(b) The second question is whether or not separate hazard reports are needed for design, manufacturing and functioning. In general, the answer is no because a single hazard report is usually manageable.

(c) The third question is whether or not separate hazard reports are needed for any specific failure node or hazard cause. In general, the answer is no because that would lead to a proliferation of hazard reports.

(d) The fourth question is whether or not to combine this hazard report with another hazard report. Since the effect of the separation bolt failing to function is failure to deploy, which is the effect of other subsystem failures, we may want to combine them all into one hazard report. If there were other EEDs besides the separation bolt which had a failure to function hazard, a separate hazard report would probably be maintained.

Conclusion: There is not a failure to function hazard report, but incorporate this failure analysis into the "Deployment Hazards".

Block 4: Other. For example, solid rocket motors have an offgassing concern. The failure of the separation bolt to function is not the only reliability concern, e.g., the EED must both function and do its job, also the safe and arm device must be able to rotate to safe if rotated to arm within the cargo bay.

Conclusion: No additional hazard reports are needed, but further analysis and documentation is required.

Some common causes of ordnance failures are:

(1) Inadvertent EED firing.

(2) Out of spec conditions: Excessive RF, electrostatic potential temperature, shelf life, shock/vibration, inadvertent commanding, etc.

(3) Designed in failures: Sneak circuits, etc.

(4) Manufactured-in failures: There are countless ways to make a bad EED which is why acceptance tests are required. Other concerns are solder-balls inside relays, damaged wires and connectors, mismated connectors, etc.

(5) Random failures: For STS, the requirement is 3 inhibits for catastrophic events in order to protect against random failures.

(6) Failure to function: Similar concerns as inadvertent EED firing.

6.2.9 Propulsion Subsystem Failure

The design hazard analysis methodology provided is used to analyze the MPS propulsion subsystem.

Above is a hazard analysis applicable to most propulsions subsystems. Suggest applying brainstorming techniques to add to the "other" entries and examples. For further discussion on design hazard analysis, see Section 6.2.2.

Applying the analysis to the MPS, blocks 1, 2, 3, 4, 5 and 6 (Figure 6-8) need to be addressed. Also known is in presenting these "hazards" to the safety review team, we need to consolidate the information that is scattered throughout the hazard analysis worksheets. Discussed below are topics for our MPS hazard reports:

Block 1: Failures involving out of spec operating parameters/interfaces including environments. A hazard report is not merely dedicated for this situation, but recognize these situations as potential hazard causes. For example:

(a) Service fluid (e.g. a system designed for hydramine may not be suitable for oxidizer)
(b) Service pressure (e.g. a system designed to operation at 400 psi may not be suitable for operation at 500 psi even though the factor of safety is greater than 2:1)
(c) Cycle life (e.g. a system designed for 5 cycles may not be suitable for 12 cycles)

(d) Shelf life (e.g. a system designed for a shelf life of 2 years may not be suitable for 5 years, particularly if the system is stored in a fueled condition)
(e) Service life (similar concerns as shelf life and cycle life)
(f) Operating temperature (both hot and cold)

Note: The above list is by no means complete. There is a lot of analysis associated with determining out of spec conditions. Still to be performed are integrated, operating and interface hazard analysis. There is one interface hazard associated with the propulsion subsystem which must be addressed, that being constant current to a latch valve. Because failures on the propulsion subsystem side of the interface can also cause this hazard we will include it on our design hazard analysis as well.

Block 2: Rupture. The first question to ask is whether or not to address all propulsion subsystem ruptures in a single hazard report. This system probably requires the use of two hazard reports: one for our bipropellant system and one for our monopropellant system. Later a decision to create separate hazard reports for the fuel, oxidizer and helium portions of our propellant system can be made.

The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and operations. In general, the answer is no because a single hazards report is usually manageable.

The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard cause. Two leading candidates are a diabatic detonation and latch valve overheat. In trying to control the number of hazard reports these items are maintained in the rupture hazard report.

The fourth question to ask is whether or not to combine hazard reports. The obvious candidate is to combine rupture and leakage. Since the rupture hazard report is expected to be lengthy, leakage is addressed separately. Besides leakage involves some unique concerns.

Conclusion: We will have two hazard reports: "Rupture of BMS" and "Rupture of ACS".

Block 3: Leakage. The same questions asked for rupture should be asked and would come to the same conclusions. Note that in the discussion of pressure systems (other than propulsion systems) is in a better position to combine rupture and leakage should it be chosen to do so.

Conclusion: Two hazard reports: "Leakage of BMS" and "Leakage of ACS".

Block 4: Inadvertent valve opening. The first thing to be done is to determine the effects of inadvertent valve opening. (The effects of rupture and leakage were obvious). If a valve inadvertently opened, can overpressurization of the propellant tanks, adiabetic detonation, inadvertent thruster firing occur or just a loss of an inhibit? Since inadvertent thruster firing is a separate hazard, a separate hazard report is created (actually two, one for our bipropellant system, one for our monopropellant system.) All of the other valve opening concerns can be addressed in the rupture hazard reports.

Conclusion: Two hazard reports: "Inadvertent BMS Thruster Firing" and "Inadvertent ACS Thruster Firing".

Block 5: Other. Remember that performing integrated, operating and interface hazard analyses might identify hazards and therefore the "other" section should not be deleted until after Phase 3. In performing the DHA on the deployment activity discovered the above mentioned design failures plus other potential problems such as propellant slosh. Note that this hazard had to be identified early because the control (baffles) is integral to the design of the propellant tanks.

Block 6: Reliability-type failures. Not planning on activating the propulsion subsystem until a safe distance from the orbiter is achieved, could easily dismiss this discussion; however, further analysis is warranted. The first question to ask is whether or not any part of the propulsion subsystem is or could be activated. Depending on where the interface is defined, there could be several such as telemetry, heaters, etc. Even latch valve activation can be a reliability issue in an offload scenario.

Here are some additional suggestions on analyzing a propulsion subsystem. For example:

(1) Look at both internal and external rupture/leakage situation.
(2) When look at external rupture/leakage paths, consider thrusters, parts, joints, barriers, etc.
(3) When identifying hazard courses, consider electrical, mechanical, chemical, thermal concerns, etc.

6.2.10 Pressure Subsystem Failures

We'll use the design hazard analysis methodology we provided earlier to analyze the MPS pressure subsystem.

The previous page is a hazard analysis applicable to most propulsions subsystems. Suggest applying brainstorming techniques to add to the "other" entries and examples. For further discussion on design hazard analysis, see Section 6.2.2 to this chapter.

Applying the analysis to the MPS. Blocks 1, 2, 3, 4, 5 and 6 (Figure 6-9) need to be addressed. Also known is that in presenting these "hazards" to the safety review team, we need to consolidate the information that is scattered throughout the hazard analysis worksheets. Discussed below are the topics for our MPS hazard reports:

Block 1: Failures involving out of spec operating conditions. A hazard report is not needed, dedicated for this situation, but recognize these situations as potential hazard causes. For example, one way for a pressure subsystem to rupture is for it to see 400°F when it was designed to see no more than 120°F.

Conclusion: Address out of spec conditions as hazard causes.

Block 2: Rupture. The first question to ask is whether or not to address all major pressure elements (e.g., battery and heat pipes) in a single hazard report. Most pressure elements are independently designed and built so it can get confusing combining all of them into a separate hazard reports. Since the MPS has many pressure elements they are not combined. However, our stated containers are combined into one hazard report because there are only two. The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and functioning concerns. In general, the answer is no because a single hazards report is usually manageable. The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard cause, e.g., fracture control is a special interest item. In general, the answer is no because that would lead to a proliferation of hazards reports. The fourth question to ask is whether or not to combine hazard reports with another hazard reports. Rupture and leakage concerns are often addressed in the same hazard report. Expect to form the propulsion subsystem, pressure subsystem rupture hazard reports are usually simple enough that including leakage won't cause too much confusion.

Conclusion: We will have the following pressure subsystem rupture hazard reports:

- "Rupture/Leakage of Nickel Hydrogen Battery Cells"
- "Rupture/Leakage of Heat Pipes"
- "Rupture/Leakage of Laser Coding Reservolin"
- "Rupture of Sealed Containers"

Block 3: Leakage. Following the rationale provided under rupture.

Block 4: Inadvertent valve opening. Other than the propulsion subsystem, no pressure subsystem on the MPS uses valves.

Block 5: Other. We never want to say that these are all the hazards you need to look at. For example, the batteries could be a hot surface concern when in an overheat mode.

Block 6: Reliability-type failures. The heat pipes are a pressure system that has to work, however they do not warrant a hazard report for this concern. Their inability to transfer heat would be a hazard cause for other hazard reports as an integration hazard concern.

Taking it one step further and identify common causes of pressure system failures, addressing rupture and leakage collectively. It is suggested having a thermal subsystem section in your ARAR such that all thermal constraints on the system can be addressed. Shock and vibration constraints can be consolidated in the structural/mechanical section. Cross reference to these sections.

(1) Out of spec conditions: Ambient temperature, heater failures, heat pipe failures, incompatible fluids, shock and vibration, etc.

(2) Designed-in failures: Inadequate safety factors, inadequate materials (stress corrosion/compatibility), etc.

(3) Manufactured-in failures: Hydrogen embrittlement, residual weld stress, bad welds, damaged O-rings, cross-threading, improper torquing, test fixture stresses, etc.

(4) Random failures: Controlled by safety factors, quality control and testing.

6.2.11 Ionizing Radiation Failures

We'll use the design hazard analysis methodology we provided in this chapter to analyze the MPS propulsion subsystem.

The previous page is a summon picture of a hazard analysis applicable to most ionizing radiation subsystems. Suggest apply brainstorming techniques to add to the "other" entries and examples. For further discussion on design hazard analysis, refer to Section 6.2.2.

Apply the analysis to the MPS. Blocks 1, 2, 3, 4, 5 and 5 (Figure 6-10) need to be addressed. Also known is that in presenting these "hazards" to the safety review team, a need to consolidate the information that is scattered throughout the hazard analysis worksheets is required. Discussed below are the topics for our MPS hazard reports:

Block 1: Failures involving out of spec conditions. A hazard report dedicated for this situation is not needed, but recognize these situations as potential hazard causes. For example, one way for an ionizing radiation source to experience leakage and contamination is for it to be involved in an explosion.

Conclusion: Address out of spec conditions as hazard causes.

Block 2: Leakage. The first question to ask is whether or not to address all ionizing radiation sources/machines in a single hazard report. It is recommended to separate sources from machines, but otherwise combination can be acceptable. In the MPS case, it is only one of each. The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and functioning concerns. In general, the answer is no because a single hazards report is usually manageable. The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard cause. In general, the answer is no because that would lead to a proliferation of hazard reports. The fourth question to ask is whether or not to combine hazard reports. The radiation source leakage hazard report should be combinable with the radiation contamination hazard report. The radiation machine leakage hazard report should combine with a laser hazard report.

Conclusion: One ionizing radiation hazard report called "Atomic Clock Leakage/Contamination". Laser x-rays will be discussed in a hazard report tentatively called, "Laser hazards".

Block 3: Contamination. Follow the same rationale as leakage.

Block 4: Other. The hazard of inadvertent x-ray production will be discussed in the laser hazard report. Another potential hazard will be the effect of biologically safe radiation leakage on electronic components.

6.2.12 RF Subsystem Failures

The design hazard analysis methodology provided earlier to analyze the MPS propulsion subsystem.

Above is a hazard analysis applicable to most RF subsystems. Suggest applying brainstorming techniques to add to the "other" entries and examples. For further discussion on design hazard analysis, see Section 6.2.2.

Apply the above analysis to the MPS. Blocks 1, 2, 3, 4, and 5 (Figure 6-11) need to be addressed. Also known is that in presenting these "hazards" to the safety review team, a need to consolidate the information that is scattered throughout the hazard analysis worksheets is required. Discussed below are the topics for our MPS hazard reports:

Block 1: Failures involving out of spec conditions. A hazard report dedicated for this situation is not needed, but recognize these situations as potential hazard causes. For example, one way for an RF subsystem to produce excessive radiation is for a control circuit to see 5G's when it was designed to see no more than 3G's.

Conclusion: Address out of spec conditions as hazard causes.

Block 2: Inadvertent radiation. The first question to ask is whether or not to address all major RF elements (emmitters) in a single hazard report. Since RF emitters share common concerns and/or circuits and since the MPS has only two emitters, a single hazard report is used. The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and functioning concerns. In general, the answer is no because a single hazards report is usually manageable. The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard cause, e.g. exposure to personnel during ground operations. In general, the answer is no because that could lead to a proliferation of hazards reports. The fourth question to ask is whether or not to combine this hazard report with another hazard report. The obvious candidate is the RF radiation hazard report. If properly presented, these hazard reports should be combinable. Suggest that the primary emitter is activated within the orbiter bay, then assume that primary emitter is already operating on low power with the doors closed.

Conclusion: We will have a single hazard report called: "RF Radiation", subject to safety review team approval.

Block 3: Excessive radiation. Follow the same rationale as inadvertent activation.

Block 4: Other. For example, RF emitters can also present hazards of hot surfaces, electric shock, air sealed/pressurized containers and ionizing radiation.

Block 5: Reliability-type failures. A reliability type failure should be addressed if radiation is planned within doors open which would violate closed doors criteria. This situation could probably be added to the RF radiation hazard report. There could be other reliability-type failures depending on what has to be powered.

Taking it one step further and identifying causes of RF radiation failures:

(1) Out of spec conditions: Shock and vibration inadvertent commanding, etc.

(2) Designed in failures: Sneak circuits, inadequate overling, etc.

(3) Manufactured-in failures: Bad parts (e.g., solder balls in relays), damaged shields, damaged connectors, etc.

(4) Reinforce failures: Controlled by the proper number of inhibits.

6.2.13 Electrical Subsystem Failures

The following page is a summary picture of a hazard analysis applicable to most electrical subsystems. Suggest applying brainstorming techniques to add to the "other" entries and examples. For further discussion on Design Hazard Analysis, see Section 6.2.2.

Apply the above analysis to the MPS. Blocks 1, 2, 3 and 4 (Figure 6-12) need to be addressed. Also known is that in presenting these "hazards" to the safety review team, a need to consolidate the information that is scattered throughout the hazard analysis worksheets is required. Discussed below are the topics for our MPS hazard reports:

Block 1: Failures involving out of spec conditions. A hazard report dedicated for this situation is not needed, but recognize those situations as potential hazard causes. For example, one way for an electrical subsystem to inadvertently activate a hazardous function is for it to see shock and vibration levels above spec.

Conclusion: Address out of spec conditions as hazard causes.

Block 2: Inadvertent Activation. The first question to ask is whether or not to address all major electrical elements in a single hazard report. Let's look at all of the electrically activated hazardous subsystem:

- o Equipment release and deploy mechanism
- o Laser gimbal mount release and motor drive system
- o Antenna release and deploy mechanism
- o Momentum wheels
- o ASE release mechanism
- o EED activated functions
- o Bipropellant motor system valve activation
- o Altitude control system valve activation
- o RF radiation
- o Laser activation
- o Battery charging
- o Battery discharging
- o Heater activation

As can be seen right away, most of these subsystems are addressed in other hazard reports. The list used for the MPS since the others are addressed elsewhere are as follows: 1) Battery charging; 2) Battery discharging; 3) Heater activation; and 4) Momentum wheels. The second question to ask is whether or not separate hazard reports are needed for design, manufacturing and functioning concerns. In general, the answer is no because a single hazard report is usually manageable. The third question to ask is whether or not separate hazard reports are needed for any specific failure mode or hazard course e.g. software related failures. In general, the answer is no because that would lead to a proliferation of hazard reports. The "fail-safe" nature of software is generally described in the electrical subsystem description where it can be referred to in hazard reports as needed. The fourth question to ask is whether or not to combine these hazard reports with each other or another hazard report. Since the basic battery concern is rupture/leakage we can incorporate in our charge/discharge discussion in our "Nickel Hydrogen Rupture/Leakage Hazard Report" and our

"Seal Container" (nickel camdium battery) hazard report. The inadvertent heater activation is not worth a hot surface hazard report and otherwise is a potential hazard cause to any hazard report with thermal concerns. Heaters will be discussed in the thermal section and referred to in hazard reports as needed, subject to safety review team approval. For the MPS there is no reaction wheel breakup hazard, but inadvertent spin up is a deployment hazard concern. This concern will be discussed in the deployment hazards report.

Conclusion: No hazard report called inadvertent activation.

Block 3: Electric Shock. Electric shock is a generic concern which can be addressed in the electrical subsystem description without the need for a hazard report.

Block 4: Ignition Source. The first question to ask is whether or not to address all major electrical elements in a single hazard report. Since this is a generic issue, use a single hazard report. The second question to ask is whether or not separate hazard reports are required for design, manufacturing and functioning concerns. In general, the answer is no because a single hazard report is usually manageable. The third question to answer is whether or not separated hazard reports are needed for any specific failure mode or hazard cause, e.g. separate hazard reports for ignition of flammable material and ignition of flammable atmospheres, the latter concern being a special interest item for Orbiter contingency situations. If it can be successfully distinguished between the two situations, a single hazard report will suffice, subject to safety review team concurrence. The fourth question to ask is whether or not to combine this hazard report with another hazard report, e.g., a fire hazard report.

Conclusion: We will have a single hazard report called, "Ignition of Flammable Atmospheres/Materials".

Block 5: Fail to Activate. Look at all the electrical elements planned on activating in various scenarios and determine which ones present a hazard if they failed to activate. One example is the heaters which have already been addressed. There may be others.

Conclusion: No fail to activate hazard report.

Block 6: Fail to Deactivate. Look at all the electrical elements planned on activating in various scenarios and determine which ones present a hazard if they failed to deactivate. Again use the heaters as an example. Again there may be others particularly as it affects the ignition of flammable atmospheres hazard report.

Conclusion: No fail to deactivate hazard report.

Block 7: Other. Other safety-type failures could include hot surfaces, hazardous materials, pressured/sealed/vented containers, etc. Could have electrical irregularities which would get into the battery overcharging and over discharging issues as well as a multitude of computer hardware problems associated with electrical irregularities. Other reliability-type failures could include also electrical irregularities.

6.3 EXAMPLE NSTS PAYLOAD HAZARDS, HAZARDS ANALYSIS, AND HAZARD REPORTS

The generic hazard reports and guidelines in this section were extracted from the Accident Risk Assessment Report (ARAR) Handbook, discussed in section 6.2. These generic hazard reports were developed specifically to aid the development of hazards analysis for DOD payloads aboard the NSTS. For this reason, they must not be used as the basis for hazards analysis or hazards reporting for any other type of system, since the hazards, control requirements and scenarios will all be different. They do provide considerable data and guidelines to support the analysis methods, particulary as they relate to hazardous subsystems. The user should view them as a source of methods data only.

Both the Department of Defense and the National Aeronautics and Space Administration require the reporting of STS payload hazards and their controls in the form of hazard reports. The purpose of the hazard report is to identify hazards resident in the payload system, demonstrate control of the hazard and specifically address and show compliance with STS safety requirements (References 24 and 25). The hazard report forms the basis of safety compliance documentation that must be submitted in mandatory payload safety reviews (References 24 and 26) which are held by NASA/JSC, KSC/ESMC, KSC/WSMC, and Air Force Space Division.

Although tailored specifically for DOD STS programs, the hazard report guidelines included here are equally applicable to NASA reviewed programs, as the required essential technical contents for NASA and DOD hazard reports are similar. Two differences exist between DOD and NASA report forms. Both NASA and DOD reports require closed loop tracking of implementation of hazard controls and verification methods. Only DOD, however, requires documentation of implementation verification (Reference 25). This results in the need to add references for all controls and verification methods. It should be noted that although hazard report content is mandatory, several different formats have been accepted.

NASA conducts separate reviews for flight design/operations (JSC) and ground design/operations (KSC/ESMC or WSMC). To support these reviews, separate "stand alone" packages are required (Reference 24). The DOD has one set of reviews that require the same data but are contained in a single package to cover both areas. The enclosed hazard reports are structured to support a DOD-type safety review/certification process. Adapting these reports to the NASA process will cause some of the reports to be segregated into separate packages to support the separate reviews.

6.3.1 Generic Hazards, Hazard Reports

The selected generic hazards and hazard reports most generally applicable to propulsion systems during flight and/or ground operations include:

Subsystem	Hazard	Generic Hazard Report (GHR) No.
Propulsion/ Propellants	Premature/inadvertent liquid engine or attitude control system firing	PROP-1
	Premature/inadvertent SRM firing	PROP-2
	Recontact after planned deployment or during planned retrieval	PROP-3
Pressurized	Pressure system leak or rupture	PRES-1
Electrical/	Ignition of flammable atmospheres	ELEC-5
Electronics	Battery leakage/rupture	ELEC-7
Materials	Release of hazardous materials (for failure paths not covered in PROP-1 or PRES-1)	MAT-2

The selected generic hazards and hazard reports that are most applicable to Ground Support Equipment or flight hardware hazards unique to ground operational phases include:

Subsystem	Hazard	No.
Pressure/ Vacuum	Rupture and/or failure of GSE pressure system vessels and components	GO-2
Propellants/ Cryogenics	Inadvertent release of corrosive, toxic, flammable or cryogenic fluids	GO-3
	Loss of habitable/breathable atmosphere	GO-4
Ordnance	Inadvertent activation of ordnance devices	GO-5
Electrical	Ignition of flammable atmosphere and/or materials	GO-6

The following comments apply to all the generic hazard reports:

(1) The hazard potential listed on the individual hazard reports is the typical worst case.

(2) Flight and ground crew interfaces must be considered when the cause. "operator errors" is listed.

(3) Corresponding hazard controls must be provided for each cause. Controls are design or operational features that specifically address the control of the applicable hazard cause and provide compliance with requirements. Sufficient specific information must be provided on the HR to demonstrate compliance. The listing of controls should numerically correspond to the causes.

(4) Corresponding verification must be provided for each control. Verification methods are tests, analyses or inspections. The listing of verification methods should numerically correspond to the controls.

(5) Certain minimum supporting data must be attached to the hazard report to complete the presentation of hazard control and to completely demonstrate compliance with requirements. Suggested minimum data will be listed. The numerical listing will correspond to the hazard controls. Absence of a listing for a particular area indicates that there is no suggested minimum data. Additional system details needed for a complete understanding of the system will be included in the system description section of the safety compliance data package (ARAR).

(6) The words "discuss" or "summarize" in the HR text sections indicate the need to provide 1-2 sentences only. In effect, these words mean "provide the bottom-line". More detail is needed if these words are used in the HR support data suggestions.

6.3.1.1 Generic Hazard Reports - The generic hazards applicable to flight hardware during flight and/or ground operations are provided in this section. Notes referenced in the Hazard Reports are explained in Section 6.3.1.2.

Generic Hazard Report - No. PROP - 1

Subsystem: Propulsion/Propellants

Hazard Group: Fire/Collision Hazard Potential: Catastrophic

Hazard: PREMATURE/INADVERTENT LIQUID ENGINE OR ATTITUDE CONTROL SYSTEM FIRING

This GHR is to address inadvertent operation of all payload liquid (or gaseous) propellant delivery systems that could damage the launch vehicle, or facilities, resulting in injury to the flight or ground crew by engine plume effects, thrust (collision) effects or release of hazardous propellants through the engines. It applies to all phases from propellant loading through the payload reaching a safe distance and/or through deservicing upon return. Requirements for this GHR are given in Paragraphs 202.2b, 201.2, 203, and possibly 210 and 214 of NHB 1700.7A and 4.1.1 of SAMTO HB S-100/KHB 1700.7.

Hazard Causes:

1. Mechanical component failures
2. Electrical component failures (flight hardware, GSE interfaces)
3. Operator errors
4. Software (flight, GSE) programming errors (if software has control of more than 1 inhibit)

Hazard Controls:

1. Specify and list the devices that interrupt (inhibit) the propellant flow path to the engine. Specify when these devices are to be opened/closed, nominally including ground system test and in-flight operations. State how these devices can fail upon loss of control signal (e.g., open, closed, as-is). Reference the applicable released drawings.
2. Specify the total number of electrical inhibits that control the mechanical inhibits. The electrical inhibits are the interrupts in the power train from the electrical source to the electrically operated flow control device. List the inhibits (related to the applicable flow control device) and indicate if and how each is monitored. Indicate those inhibits that are operated by RF command and if their RF links are encrypted. Reference the applicable drawings and the flight procedures that specify the applicable monitoring. Specify the fault tolerance of the system controlling the electrical inhibits including the total launch vehicle and GSE interfaces. For pyrotechnically activated flow control devices, refer to the discussion on pyrotechnic circuitry safety in GHR PROP-2, Controls 3 and 6, or address or repeat here.

3. See Note 2

4. See Note 3

Safety Verification Methods:

1a. Specify how it was verified that the flow control devices can withstand the expected launch environments. Reference applicable qualification reports.

1b. Specify what procedure/monitoring will be used to verify that the flow control devices are in the proper position prior to launch. Reference the procedure.

1c. For retrieval, describe the safing sequence and specify how the proper failure tolerance is verified.

2a. See Note 4

2b. See Note 5

2c. See Note 6

3. See Note 7

4. See Note 8

Minimum GHR Supporting Data:

1a. Schematic of mechanical system components. Circle and number the flow control devices per the listing in Control 1. Indicate portions of the system that are dry.

1b1. Tabulate the flow control devices, when last cycled and how the final closure is verified.

1b2. Schematic of each flow control device.

2a. Integrated electrical/mechanical schematic showing flow control devices, electrical inhibits, controls (including GSE interfaces) and monitors and which shows independency of the inhibits. Circle and number the electrical inhibits per the listing in Control 2.

2b. See Note 11

3. See Note 12

4. See Note 13

Generic Hazard Report - No. PROP-2

Subsystem: Propulsion/Propellants

Hazard Group: Fire/Collision Hazard Potential: Catastrophic

Hazard: PREMATURE/INADVERTENT SOLID ROCKET MOTOR (SRM) FIRING

This GHR is to address inadvertent operation of payload systems containing solid propellant devices that could damage the launch vehicle or facilities resulting in injury to the flight or ground crew by engine plume effects or thrust (collision) effects. It applies to all phases from arrival of the solid-propellant-bearing components at the applicable launch site through achieving a safe distance from the launch vehicle (or de-integration upon contingency return). Requirements for this GHR are given in Paragraphs 202.2a, 201.2, 210 and 214 of NHB 1700.7A and 4.1.1 of SAMTO HB S-100/KHB 1700.7.

Hazard Causes:

1. Electrical component failures
2. Operator errors
3. EMI/EMC (including EMI/EMC caused by rotating the S&A device)
4. Software programming errors (if software has control of more than 1 inhibit)
5. Propellant sensitivity to induced environments
6. Static discharge

Hazard Controls:

1. See Note 1. In addition, indicate the type of Safe and Arm (S&A) device used. Indicate when the S&A device is activated. If the S&A is to be activated prior to the payload reaching a safe distance from the launch vehicle, provide specific timelines and describe specifics of monitoring that will be available just prior to maneuvering for deployment. Reference the applicable released drawings and flight procedures.
2. See Note 2.
3. See Note 17.
4. See Note 3.
5. Identify what environments can cause ignition and show that margins exist.
6. See Note 16.

Safety Verification Methods:

1a. See Note 4.

1b. See Note 5.

1c. See Note 6.

2. See Note 7.

3. Summarize and reference analysis and/or test results (include dB margins).

4. See Note 8.

5. Specify verification approach and results of tests/analyses. Reference applicable documents.

6. Describe how it is verified that firing squibs are free from electro-static effects. Summarize and reference test results.

Minimum GHR Supporting Data:

1a. See Note 10.

1b. See Note 11.

2. See Note 12.

3a. Drawings of EMI/EMC suppression devices (e.g., RF attenuation shields). EMI field strength data (worst case)used in analyses/tests.

3b,6c. Schematic showing ordnance circuit. Show location of static bleed or circuit bleed resistors if used.

4. See Note 13.

6a. Cut away schematic of initiator (if not an NSI).

6b. Table listing flight initiators tested and results (if not NSI's).

6c. See 3b above.

Generic Hazard Report - No. PROP-3

Subsystem: Propulsion/Guidance

Hazard Group: Collision Hazard Potential: Catastrophic

Hazard: RECONTACT AFTER PLANNED DEPLOYMENT OR DURING PLANNED RETRIEVAL

This GHR is to address potential recontact (collision) from payloads that have been safely deployed from the manned launch vehicle or inadvertent collision from payloads that are intended to be retrieved. For deployed payloads, these causes apply after the payload has reached a distance that is safe for payload engine firing. (Reaching this "safe distance" does not necessarily control this hazard.) For retrieval phases, these causes apply during manned vehicle approach and grapple. Collision potential during deployment and after grapple is addressed in GHR S/M-4. Applicable requirements for this GHR are given in Paragraphs 201.? and 214 of NHB 1700.7A.

Hazard Causes:

1. Pointing/guidance errors existing during engine firing
2. Positioning errors
3. Mechanical component failures in propulsion system affecting thrust vector

Hazard Controls:

1. Specify the mission design and orbital maneuvers to prevent collision. Describe payload provisions for ground stations to track and ensure Orbiter and payload trajectories will not intersect, i.e., collide. Show how the identified concerns are incorporated into procedures and designs to prevent collision. Reference applicable documents.
2. Provide TTC and GNC operational descriptions and failure modes and tolerances if functioning is needed to control the hazard. Reference applicable documents.
3. Specify nominal telemetry errors expected (worst case) and subsequent limits on orbital trajectories. Reference applicable documents.
4. Specify components whose failure would affect the desired thrust vector (e.g., engine gimbaling devices, computer/avionics hardware devices, failed on/off attitude control jets, etc.). Address fault tolerance and other controls that assure safe firing.

Safety Verification Methods:

1. Summarize Recontact Analysis and consideration of worst case calibration uncertainties, misalignments and tolerance limits. Reference analysis.
2. See Note 6.

3. Summarize analysis that shows expected errors will not cause a hazard. Reference applicable documents.

4. See Note 6.

Minimum GHR Supporting Data:

1. Summary of Recontact Analysis, mission design and orbital maneuvers.

2. Provide drawings and schematics in sufficient detail to demonstrate compliance.

Generic Hazard Report - No. PRES - 1

Subsystem: Pressurized Structure

Hazard Group: Explosion, Fire Hazard Potential: Catastrophic

Hazard: PRESSURE SYSTEM LEAK OR RUPTURE

This GHR is to address failure of payload pressurized subsystems that could cause damage to the launch vehicle and injure flight or ground crews by explosion effects or by effects of hazardous material leaks. It applies to all launch/operational phases from payload installation through the payload reaching a safe distance and/or through deservicing upon return. All areas of the S/C and/or CE structure that fall under the definition of pressure vessels given in NHB 1700.7A are to be addressed. Also included in this GHR are all other components of the pressurized system such as lines, fittings, valves, regulators, etc. The effects of pressure, temperature and support loads on these components is to be addressed. Supporting structure, bracketry, etc., should be covered in GHR S/M-1. Requirements for this GHR are given in Paragraphs 208.4, 208.5, 208.6, 209.1a and 214 of NHB 1700.7A and Paragraph 4.1.1 of SAMTO HB S-100/KHB 1700.7.

Hazard Causes:

1. Internal (external) pressure, support reactions and temperature exceed the container strength capability. Load, temperature and pressure sources to be considered are nominal flight loading (including landing loads), emergency landing loads, the nominal mission thermal profile, mechanical shock/vibration, and transportation and handling loads.

2. Corrosion

   a. Stress corrosion
   b. Dissimilar metals, propellant, etc.

3. Propagation of crack-like defects ("fracture control")

4. Adiabatic compression/detonation of propellants (e.g., for hydrazine systems with dry lines)

5. Over-pressurization from GSE or other servicing equipment

   a. Mechanical component failures
   b. Electrical component failures
   c. Operator errors
   d. Software programming errors (if software has control of critical components)

6. Potential leak paths

   a. "B-nuts"
   b. Fill/drain valves, quick disconnects
   c. Non-welded parts
   d. Thruster valve chatter
   e. Fill/drain connections/residuals

7. Hydrogen embrittlement or other embrittling processes

8. Failed-on open/close commands to valves causing temperature rise in valve coil and valve

9. Heat soak-back from thruster firing

10. Freeze/thaw expansion effects

11. Failed-on heaters

Hazard Controls:

1a. Specify structural design criteria. Include pertinent design safety factors or levels and the compliance option chosen within NHB 1700.7A or MIL-STD-1522A. Reference the applicable engineering document.

1b. Discuss derivation of design loads, pressures and temperatures. Reference applicable documents.

1c. Describe the analysis and/or tests that determines environments (including shock/vibration effects) on applicable hardware. Specify how hardware design requirements will be developed to withstand these environments. Reference the analysis and design requirements specification.

2. Specify how MSFC-SPEC-522A will be used to identify materials for susceptibility to stress corrosion cracking. Address controls for dissimilar metals corrosion and environmentally induced corrosion (include pressurization medium). Address the propellant compatibility of materials within components that could be exposed after a single barrier failure.

3. Describe the fracture control program (per the requirements of SD-YV-0068 or equivalent). Reference the fracture control plan (if applicable).

4. Specify the electrical inhibits that prevent inadvertent valve functioning. (See Note 1). Alternately, specify test data for flight configuration and safe distance criteria. Specify controls designed to cushion "water hammer" effects (e.g., GN_2 cushion blanket, bypass equalizing valves, throttle valves, etc.). Reference drawings.

5a. Specify and list the devices that interrupt the pressurization path from potentially hazardous GSE sources to the S/C. Specify failure tolerance and how this is obtained. Specify number of pressure relief devices, adequacy of flow capabilities including safety margins, instrumentation, line sizes and hydrostatic test levels. Reference drawings.

5b. See Note 14.

5c. See Note 2.

5d. See Note 3.

6a-e. For each of the components listed in Control 6, specify the number and locations that will be exposed to fluid during mission phases. Within each type of component, identify potential leak paths. Specify the controls that prevent leakage through these paths.

7. Define the process controls required to preclude substandard material mechanical properties.

8. Specify effects of failed-on commands to all valves. Reference analysis. See the first four sentences of Note 1 if controls are needed per the analysis.

9. Describe thermal protection for components exposed to heat soak-back from thruster firing. Reference released drawings/procedures.

10. Specify temperatures that cause hazardous freezing/thawing. Specify constraints to be placed on launch vehicle. Reference document that places these restraints on the launch vehicle.

11. Specify effect of failed-on heaters and required failure tolerance. If failure tolerance is required, see Note 14.

Safety Verification Methods:

1a. Specify structural verification criteria. Include the test factors or levels. Reference Structural Verification Report.

1b. Summarize and reference design loads, pressure and thermal reports.

1c. Summarize and reference strength analysis and test reports.

2. Reference results of MSFC-SPEC-522A review, fluid compatibility and dissimilar metal assessments.

3. Provide the "bottom-line" of the Fracture Mechanics Analysis Report. Reference the analysis.

4. For inhibit approach, see Notes 4, 5 and 6. Address relevant mechanical inhibits in Note 4 also. For the test approach, summarize analysis that shows the test encompasses all expected flight environments, contamination, etc. Reference applicable analysis.

5a. Specify how it was verified that the control devices can withstand the expected pressures. Reference qualification reports. Specify what procedure/monitoring will be used to verify that the control devices are in the proper position prior to operation. Reference the procedure.

5b. See Note 6.

5c. See Note 7.

5d. See Note 8.

6a-e. Summarize and reference the tests/analyses/procedures used to verify the design adequacy and flight hardware integrity.

7. Describe how the adequacy of the process controls were verified. Reference applicable controls.

8. If the analysis discussed in Control 8 concludes that failed-on commands do not present a hazard to the system, no verification is applicable. Otherwise, see Notes 4, 5 and 6

9. Summarize and reference thermal analysis and/or test.

10. Summarize and reference the thermal analyses/tests that verify adequacy of the identified constraints in the expected and potential contingency thermal environments.

11. Summarize and reference results of thermal analysis. If failure tolerance is required, see Note 6.

Minimum GHR Supporting Data:

1a. Summary of stress analysis, such as minimum margins of safety, and summary correlation with test results. Resolve any discrepancies between analysis and test.

1b. Summary listing giving the following data for all components:

a. Component name
b. Design pressure/temperature
c. Proof-pressure. Qualify if established by fracture mechanics *and/or adjusted for testing* at other than design temperatures. Note if proof pressure applies for the component or the system.
d. Burst pressure design/observed. Qualify if adjusted for testing at other than design temperature and whether demonstrated analytically combined with a test or strictly by test.
e. Margins of safety under combined effects of pressure, load and temperature, as applicable.

2. Summary of MSFC-SPEC-522A review and/or analysis as well as references to approved non-compliance reports on safety critical components.

3. Summary of safe-life analysis giving predicted service life, safe-life, etc. Include initial, final and critical flaw size. Provide NDI process and capability to be used in inspection for initial flaws.

4. Summary of tests and see Notes 11 and 12.

5a. Schematic of mechanical system components. Circle and number the control devices. Table listing the control devices and how proper setting is verified. Cut-away schematics of control devices.

5b. See Note 15.

5c. See Note 12

5d. See Note 13.

6a-e. Schematic which indicates location of potential leak paths. "Cut-away" schematics of key components.

7. See Notes 10, 11 and 12.

8. Summary of tests including assumptions, initial conditions and results.

9. Summary of analyses/tests including assumptions, initial conditions and results.

10. If failure tolerance is needed, see Note 15.

Generic Hazard Report - No. ELEC - 5

Subsystem: Electrical/Electronics (Descent and Landing Phase)

Hazard Group: Fire/Explosion Hazard Potential: Catastrophic

Hazard: IGNITION OF FLAMMABLE ATMOSPHERES

This GHR is to address the potential of a payload igniting a flammable atmosphere that is presented by the launch vehicle. NASA has indicated that this is a possibility during Orbiter descent and therefore appropriate payload controls must be implemented to provide an overall protection against the fire/explosion potential. Only nominal (powered) payload operations are to be considered. Consequently, the ignition sources of concern are a subset of those addressed on GHR ELEC-4. This GHR applies to descent and landing phases. Payload ascent configuration is to be considered due to the fact that certain Orbiter scenarios will not allow reconfiguration of the payload for descent. The ground processing phase of this hazard is addressed in GHR GO-6. Applicable requirements are given in Paragraphs 219 and 214 of NHB 1700.7A.

Hazard Causes:

1. Arcing, sparking devices
2. Hot spots
3. Static electricity discharge

Hazard Controls:

1. Discuss what arcing and sparking devices are used and how they are controlled during ascent, descent and landing mission phases. Specify the number of inhibits that interrupt power sources during unscheduled power-on events and indicate their independence.
2. Discuss potential hot spots and how they are controlled during critical mission phases.
3. Describe all controls that preclude opportunities for a static discharge through an uncontrolled path to ground. For high volume resistivity materials specify design criteria that precludes accumulation of electrostatic charge on specified surfaces. If the control is intrinsic to the system, so state and describe. Include hazard controls associated with stray energy paths.

Safety Verification Methods:

1. See Notes 4 and 5 (apply to one inhibit only).
2. Verify by test or analysis that the peak temperature presented by any portion of the system to a worst case atmosphere does not exceed the flash or fire point ignition temperature for the specified condition. Reference applicable test or analysis sources.

3. Verify by test or analysis that the peak magnitude of static discharge does not present an ignition source to a "worst case" atmosphere or material for the specified condition. Reference applicable test or analysis sources.

Minimum GHR Supporting Data

1. Schematic showing electrical inhibit(s) and controls.

2. Drawings/schematics showing heat sources. Heat diffusion/dissipation data. Worst case assumptions or conditions postulated and/or simulated.

3. Path impedance/maximum discharge data. Provide pictorials of designs to avoid/interrupt discharge path continuity to known flammable/explosive materials and devices.

Generic Hazard Report - No. ELEC - 7

Subsystem: Electrical/ELectronics

Hazard Group: Contamination/Explosion/ Corrosion/Flammability

Hazard Potential: Catastrophic

Hazard: BATTERY LEAKAGE/RUPTURE

This GHR is to address battery cell failures that could injure the ground or flight crew by damaging the Orbiter due to explosion or contamination effects. It applies to all phases of ground processing and flight of cargo element airborne and ground support equipment batteries, including storage, handling, activation, installation, operation, removal, and disposal. Applicable requirements are given in Paragraphs 201.2 and 208 of NHB 1700.7A and Paragraphs 4.1.1 and 4.3.9 of SAMTO HB S-100/KHB 1700.7. The causes on this GHR were compiled from many different types of batteries. Select only the causes that apply to the type(s) of batteries to be covered.

Hazard Causes:

1. Internal shorting
2. Overcharging/discharging
3. Cell reversal. Note: This cause addresses individual cell capacity imbalances, discharging through a dead cell, and the subsequent heat generation from the increased internal resistance of the battery.
4. Excessive internal cell/case pressure from thermal effects (excluding thermal runaway) causing pressures to exceed design capability.
5. Thermal runaway (chemical reaction)
6. Freeze/thaw
7. Accumulation and ignition of hazardous gas mixture
8. Operator error
   a. Procedural inadequacy
   b. Training, certification, and/or supervisory inadequacies
9. Computer software/hardware interface deficiencies

Hazard Controls:

1. Identify and describe all controls that preclude internal shorting. Ensure all potential internal short causes are addressed. Reference applicable drawings.

2. For overcharging, specify what devices (e.g., automatic reset thermal trips, circuit breakers, etc.) and procedures are designed to limit the maximum charging current and time so as not to initiate or sustain an excessive outgassing or thermal runaway condition. State which devices are monitored by crew and/or ground personnel. Specify those controls that prevent charging lithium batteries under any condition (e.g., shunt bypass diodes). For overdischarging, specify devices and procedures that are designed to limit the current discharge rate. Specify failure tolerance of these controls. Reference applicable drawings.

3. Specify procedures, monitoring and/or manufacturing/maintenance controls that ensure that the capacity of each cell of a multiple cell battery is within established specifications prior to discharging (e.g., prior to battery conditioning or use).

4. Provide an initial summary stating whether the battery design will be treated as a sealed container or as a pressure vessel and reference or list the criteria used to make the determination. State the minimum safety margin above operating pressures. Specify how the individual cells and case are designed to prevent or control a rupture event (e.g., venting mechanisms, burst discs, pressure relief devices, etc.). Specify effects of failed-on heaters and necessary failure tolerance.

5. Establish an operational condition envelope or similar data format whereby operations within the limits of the envelope will prevent thermal runaway reactions. Describe devices/designs used to keep the system operating within the constraints of the envelope. Reference applicable documents.

6. Specify resultant designs that prevent or minimize abnormal freezing temperatures or prevent physical damage to the cell or case. Reference applicable documents.

7. For byproducts (e.g., gas generated, chemical reaction, etc.) where controls are necessary for safe operation, specify the control system (e.g., control of free volume, ventilation, temperature control) that effectively places their generation and accumulation within a safe envelope of operation during worst case conditions.

8. Specify any procedures or training required to control hazards that could result from operator error. For procedural controls, state how precautions and step by step instructions are validated (e.g., walked through). Include contingency, off-normal and/or emergency procedures/instructions. For marking controls, specify all markings created and the basis for their creation. Describe the human factors engineering designs incorporated into the markings (e.g., color choice, size, wording/phrasing, visibility, etc.). In general, as part of controlling human error, specify how access to hazardous areas should be controlled (e.g., control points). Describe how training as a control will be implemented to educate and develop an understanding by the operator for battery hazards and how to avoid them.

9. See Notes 3 and 14.

Safety Verification Methods:

1. Specify what technique will be used to verify that internal short guards and controls are in place. See Note 9. Summarize and reference qualification program.

2. See Notes 4, 5, 6, 7 and 8.

3. Discuss how the implementation of controls in the event of cell reversal will be verified.

4. Verify by analysis or test (e.g, burst pressure capability test) the safety margin between rupture and operating pressure for worst case conditions. Reference analyses, tests. Summarize and reference thermal analysis that determined operating conditions. If heater failure tolerance is required, (see Notes 4-8).

5. Verify by analysis or demonstration that the required failure tolerance is maintained (i.e., operating envelope limits are not violated). Describe how procedural precautions, if any, are verified. Reference applicable documents.

6. Provide results of freeze/thaw analysis or testing. For temperature control circuits, specify fault tolerance for the heaters fail off condition. Reference applicable drawings and documents of temperature controls and cell/case construction (see Notes 4-8).

7. Reference the design and testing.

8. Describe how it will be assessed that written procedures are understood by operators, and hazardous conditions can be avoided.

9. See Notes 6 and 8.

Minimum GHR Supporting Data:

1. Provide illustrations of each control.

2. Provide summary of test and/or analysis performed to establish maximum charge and discharge ratings. State worst case assumptions used (see Notes 10-13).

3. Schematics of control and monitoring circuits. ICV voltage and capacity relationships data. List of precautions included in procedures.

4. Provide results of tests and/or analysis showing structural performance under abnormal pressure conditions. Provide drawings, schematics of pressure control systems and relief devices. Include all component ratings (e.g. pressure relief valve flow rates, line sizes, setpoints, etc.). See Notes 10-13 and 15.

5. Analysis of how the operational envelope (or limits) is derived. State all worst case assumptions used.

6. Summary of test results, schematics of temperature control circuits showing fault tolerance designs, cell/case construction descriptions and diagrams.

7. Provide data describing burn/explosive concentration and combustible characteristics of gases generated.

8. Illustrations of key markings, etc.

9. See Notes 13 and 15.

Generic Hazard Report - No. MAT - 2

Subsystem: Materials

Hazard Group: Contamination/Corrosion Hazard Potential: Critical/Catastrophic

Hazard: RELEASE OF HAZARDOUS MATERIALS (for failure paths not covered in GHR PROP-1 or GHR PRES-1)

This hazard report addresses control of hazardous functions which could release hazardous materials prematurely or inadvertently in the Orbiter. Previous hazard reports have addressed release of hazardous materials by system rupture or leakage which can be considered a subset of this hazard. Rupture/leakage could be incorporated into this hazard report or this separate report can be used for the causes listed below. This GHR applies to all phases when the hazardous materials are present. Ground support equipment concerns are addressed in GHR GO-3. Applicable requirements are given in Paragraphs 201, 202, 209.1 and 214 of NHB 1700.7A and paragraph 4.1.1 of SAMTO HB S-100/KHB 1700.7.

Hazard Causes:

1. Mechanical component failures.

   a. Vent system
   b. Dump system
   c. Relief system
   d. Flow control valves (engine firing is covered in GHR PROP-1. This cause addresses release of materials through the thrusters that may not necessarily equate to engine firing).

2. Electrical component failures

   a-d. Same as 1.

3. Operator errors

   a-d. Same as 1.

4. Software programming errors (if the software has control of more than 1 inhibit)

   a-d. Same as 1.

Hazard Controls:

1a-d. For each flow path, specify and list the devices that interrupt or control flow. Specify what features of the devices prevent inadvertent opening and show how the required failure tolerance is provided. Reference the applicable released drawings. For systems/components that are designed to release (e.g., vent) hazardous materials for purposes of controlling various physical parameters, specify the design, location and operations of the release endpoint (e.g., waste collection tank).

2a-d. Specify the total number of electrical inhibits that control the mechanical devices in each release path. List the inhibits (related to the applicable flow control device) and indicate if and how each is monitored. Reference the applicable drawings and the flight procedures that specify the applicable monitoring. Specify the fault tolerance of the system controlling the electrical inhibits including GSE interfaces. Discuss fail on/off impacts to vent/dump/relief/FCV components (e.g. fail positions) and discuss how an accidental release is avoided.

3a-d. See Note 2.

4a-d. See Note 3.

Safety Verification Methods:

1a-d. For each flow path:

(1) Specify how it was verified that the flow control devices can withstand the expected STS environments. Reference applicable qualification reports.
(2) Specify what procedure/monitoring will be used to verify that the flow control devices are in the proper status (or structurally adequate) prior to launch. Reference the procedure.
(3) For retrieval, describe the safing sequence and specify how the proper failure tolerance is verified.

2a-d. See Notes 4, 5 and 6.

3a-d. See Note 7.

4a-d. See Note 8.

Minimum GHR Supporting Data:

1a-d. (1) Schematic of mechanical system components.
(2) Table listing the flow control devices, when last cycled and how the final closure is verified.
(3) Schematic of each flow control device.

2a-3. (1) Integrated electrical/mechanical schematic showing flow control devices, electrical inhibits, controls (including GSE interfaces) and monitors and indicators which show independency of inhibits. Circle and number the electrical inhibits. circle and number the electrical inhibits per the listing in Control 2.

3a-d. See Note 12.

4a-d. See Note 13.

Generic Hazard Report - No. GO - 2

Subsystem: Pressure/Vacuum

Hazard Groups: Explosion/Injury or Illness Hazard Potential: Catastrophic

Hazard: RUPTURE AND/OR FAILURE OF GSE PRESSURE SYSTEM VESSELS AND/OR COMPONENTS*

This hazard report should address pressurized ground support equipment and its interfaces with cargo elements, facilities, personnel, and other hazardous fluids or gaseous subsystems. Hazardous effects of concern in this GHR are explosion effects, release of hazardous materials and personnel injury by failures that can cause depletion of a breathable atmosphere. It applies to all ground processing phases when the GSE is pressurized. Applicable section of SAMTO HB S-100/KHB 1700.7 is Paragraphs 4.1.1, 4.1.6 and 4.3.3. (See GHR GO-3).

Hazard Causes:

1. Inadequate strength/design

   a. Load factors exceeded - insufficient safety factors
   b. Corrosion, wear or abuse
   c. Propagation of crack-like defects
   d. Physical damage during manufacturing or handling
   e. Mechanical component failures
   f. Electrical component failures

2. Improper use/operations

   a. Improper installation/assembly
   b. Operator error
      1. Procedural inadequacy
      2. Training, certification, and/or supervisory deficiencies
   c. Computer software/hardware interface deficiencies.

*Overpressurization of flight H/W (hardware) by GSE (ground support equipment) should be covered in GHR PRES - 1

Hazard Controls:

1a. Specify structural design criteria. Include applicable design safety factors. Reference applicable engineering document.

1b. Specify how system hardware is protected from stress, galvanic, general, embrittling or other corrosive/erosive processes. Discuss compatibility of vessels with materials to be contained. Reference applicable implementing document.

1c. Specify controls for metallic and non-metallic parts that minimize chance of failure from undetected flaws. Reference implementing document.

1d. Describe the inspection and approval process that ensures system hardware arrives at its ultimate location in an undamaged condition. Reference manufacturing specifications and recommendations that are included for handling.

1e. For each fluid/gas flow path, specify and list the devices that interrupt or control flow. Specify what features of the devices prevent inadvertent opening and show how the required failure tolerance is provided. Reference the applicable drawings. For systems/components that are designed to release (e.g., vent) hazardous materials for purposes of controlling various physical parameters, specify the design, location and operation of the release endpoint (e.g., waste collection tank). Identify structural components/assemblies that interface with other cargo elements, facility systems or external environments for purposes of locating potential leak points. Specify nominal leak rates if they exist (e.g., valve stem leakage, leakage at flange unions, etc.) For vacuum systems, identify components that provide assurance that the vacuum is maintained.

1f. Specify the total number of electrical inhibits that control the mechanical devices in each release path. (Or, discuss control circuit failure tolerance if "electrical inhibits" are not provided.) List the electrical inhibits (related to the applicable device) and indicate if and how each is monitored. Reference the applicable drawings and the procedures that specify the applicable monitoring. Specify the fault tolerance of the systems controlling the electrical inhibits, including all interfaces. Discuss fail on/off consequences to vent/dump/relief FCV components (e.g., fail positions) and discuss how an accidental release is avoided.

2a. Specify installation and assembly procedures that pertain to structural integrity. Reference applicable documents.

2b1,2. See Control 2b1,2 of GHR GO-1.

2c. See Note 3.

Safety Verification Methods:

1a. Describe how it is verified that the system has adequate strength for its intended operation. Operational lifetime should be considered and include periodic preventive maintenance/testing that ensures system integrity persists. Reference applicable documents.

1b. See Verification 1b in GHR GO-1.

1c. Summarize and reference life cycle analysis or test. Specify inspection and test result recording methods and verification methods. Reference inspection records and test document numbers.

1d. Reference how damaged hardware is identified. Explain how personnel are informed in such a manner as to prevent future operations until proper repairs are made. Reference how this is accomplished. Specify procedure review and validation process.

1e. Reference applicable verification results pertaining to the safe design and operations of GSE pressure/vacuum mechanical components. See Note 6.

1f. See Note 7.

2a. Specify how procedures are verified. Reference the validation procedure.

2b1. Specify procedure review process and validation process. Reference validation procedure.

2b2. Summarize and reference training and certification process. Reference validation procedure.

2c. See Note 8.

Minimum GHR Supporting Data:

1a. See GHR GO-3, Minimum Backup Data 1a.

1b. See GHR GO-3, Minimum Backup Data 1b.

1c. See GHR GO-3, Minimum Backup Data 1c.

1d. See Note 12.

1e. Provide drawings showing locations of component connections that are under pressure/vacuum.

1f. Provide schematics showing number and location of electrically activated inhibits.

2a. Provide drawings and summaries of control designs (e.g., mating connector design, etc.)

2b. Reference personal qualifications.

2c. Reference software test procedures and results.

Generic Hazard Report - No. GO - 3

Subsystem: Propellants/Cryogenics GSE (Ground Support Equipment)

Hazard Groups: Contamination/Fire/Explosion/ Injury or Illness

Hazard Potential: Catastrophic

Hazard: INADVERTENT RELEASE OF CORROSIVE, TOXIC, FLAMMABLE, OR CRYOGENIC FLUIDS

Note: This GHR could reference applicable sections of the flight hazard reports as appropriate.

This hazard report should address propellant/cryogenic ground support equipment and their interfaces with cargo elements, facilities, personnel, and other hazardous fluids or gases subsystems. Separate similar hazard reports should be provided for each distinct fluid unless the systems containing the fluids are of common design. Applicable sections of SAMTO HB S-100/KHB 1700.7 are Paragraphs 4.1.1, 4.1.6, 4.3.7 and 4.3.8. (See also GHR GO-2).

Hazard Causes:

1. Inadequate Strength/Design
   a. Load factors exceeded - insufficient safety factors
   b. Corrosion, wear or abuse
   c. Propagation of crack-like defects
   d. Physical damage during manufacturing or handling
   e. Electrical component failures
   f. Mechanical component failures
   g. Computer software/hardware interface deficiencies

2. Improper Use/Operations

   a. Improper installation/assembly
   b. Operator error
      1. Procedural inadequacy
      2. Training, certification, and/or supervisory deficiencies

Hazard Controls:

1a. Specify design criteria. Include design safety factors. Reference applicable engineering document.

1b. See GHR GO-2, Control 1b.

1c. See GHR GO-2, Control 1c.

1d. Statement to identify manufacturing or handling operations and define procedures to preclude physical damage.

1e. Specify the total number and list the electrically activated inhibits that control the mechanical inhibits and indicate if and how each is mounted. Reference drawings.

1f. Specify and list the devices that interrupt the fluid flow path. Specify when these devices are to be opened/closed nominally during ground operations and state how these devices can fail (e.g., open, closed). Reference drawings. For each flow path, specify and list the devices that interrupt or control flow. Specify what features of the devices prevent inadvertent opening and show how the required failure tolerance is provided. Reference the applicable drawings. For systems/components that are designed to release (e.g., vent) hazardous materials for purposes of controlling various physical parameters, specify the design, location and operation of the release endpoint (e.g., waste collection tank).

1g. Specify how the required fault tolerance has been maintained in the software portion of the control system for GSE operations.

2a. Statement to identify assembly and installation operations and define procedures to preclude physical damage.

2b1. Statement to identify procedural contents and method of verification of accuracy. Specify personnel protective clothing (gloves, coveralls, respirators, etc.) and other equipment required for operations and planned use of toxic vapor checks.

2b2. Statement to identify personnel training and certification policies. Reference training records.

Safety Verification Methods:

1a. Review of design drawings and specifications. Reference drawing numbers.

1b. List documentation verifying material compatibility.

1c. Summarize and reference life cycle analysis or test. Specify inspection and test result recording methods and verification methods. Reference inspection records and test document numbers.

1d. Specify procedure review and validation process.

1e. Specify how it was verified that the electrically activated inhibits will control the mechanical inhibits and specify what procedure/ monitoring will be used to verify that the electrically activated inhibits are in the proper state prior to the operation. Reference the procedure.

1f. Specify how it was verified that the control devices are adequate. Reference qualification reports. Specify what procedure/monitoring will be used to verify that the control devices are in the proper state prior to operation. Reference the procedure.

1g. See Note 8.

2a. Specify how the procedures are verified. Reference the validation procedure.

2b1. Specify procedure review process and validation process.

2b2. Specify training and certification procedures. Reference validation procedures.

Minimum CHR Supporting Data:

1a. Summary of analyses, such as minimum margins of safety and summary correlation with test results. Resolve any discrepancies between analyses and tests. Provide table of components including component name, design pressure/temperature, proof-pressure and design burst pressure/observed.

1b. Summary of specification review and/or analysis as well as references to approved non-compliance reports on safety critical components.

1c. Summary of analysis giving predicted service life, safe-life, etc. Include initial final and critical flaw size. Provide NDI (non-destructive inspection) process and capability to be used in inspection for initial flaws.

1d. See Note 12.

1e. Integrated electrical/mechanical schematic showing control devices, electrical inhibits, controls and monitors. Circle and number the electrical inhibits. Table listing electrical inhibits and how final position is verified.

1f. Schematic of mechanical system components. Circle and number the control devices. Table listing the control devices and how final closure is verified. Schematic of control devices. Specific values should be shown for control reduction and/or relief valves settings, especially any used to protect the flight unit from overpressurization from the GSE.

1g. Summary of software safety analysis, verification/validation.

2b2. Provide training records.

Generic Hazard Report - No. GO - 4

Subsystem: Propellants or Pressure

Hazard Group: Contamination/Injury or Illness

Hazard Potential: Catastrophic

Hazard: LOSS OF HABITABLE/BREATHABLE ATMOSPHERE, TOXIC MATERIAL

This hazard report should address all ground processing activities where the oxygen level of the environment could drop below acceptable levels or toxic/harmful airborne substances could be introduced from nominal operations (including toxic materials used for cleaning, bonding, potting, etc.). Failure to contain harmful substances should be covered in GHR GO-3 and/or the applicable Flight hazard reports. Applicable sections of SAMTO HB S-100/KHB 1700.7 are Paragraphs 4.1.1, 4.3.9 and 4.4.2.2.

Hazard Causes:

1. Normal Venting
2. Improper use/operation
3. Purging with inert gas

Hazard Controls:

1. Specify normal venting rates and rates possible with credible system failures. Identify containment procedures for toxic materials.
2. Specify what procedures will be used to ensure proper use or operation of the equipment. Reference procedures.
3. Specify monitoring methods to identify O_2 deficient areas. Reference procedures.

Safety Verification Methods:

1. Summarize and reference analysis that verifies area ventilation is adequate for maximum concentration of inert gases. Specify method to verify procedure adequacy to control toxic materials. Monitor concentration of potential toxic materials.
2. Specify procedure review and validation processes. Summarize and reference results of the OHA (Operations Hazards Analysis), if performed.
3. Summarize and reference validation process and emergency procedures.

Minimum GHR Back-up Data:

1-3. Lists of toxic/flammable materials and quantities to be used during processing.

Generic Hazard Report - No. GO - 5

Subsystem: Ordnance

Hazard Group: Explosion/Fire/Radiation /Injury or Illness

Hazard Potential: Catastrophic

Hazard: INADVERTENT ACTIVATION OF ORDNANCE DEVICES

Note: This hazard report may be incorporated with the applicable flight hazard report.

This hazard report should address the installation, test and/or checkout of ordnance devices and their interfaces with cargo elements, facilities, personnel, and ordnance test/checkout equipment. Applicable sections of SAMTO HB S-100/KHB 1700.7 are Paragraphs 4.1.1 and 4.3.5.

Hazard Causes:

1. Inadequate design of test/checkout equipment
2. Static discharge
3. Electromagnetic interference
4. Improper installation/handling
5. Operator error*
   a. Procedural inadequacy
   b. Training, certification, and/or supervisory deficiencies
6. Computer software/hardware interface deficiencies*
7. Electrical component failures*

---

*Address only GSE unique aspects of these causes. The Flight Hazard Report should address these causes once the ordnance device is installed and GSE interfaces are terminated.

Hazard Controls:

1. See Notes 1, 2 and 3. Include energy input used in susceptibility analysis.
2. See Note 16.
3. Specify controls required during EMI testing.
4. Statement to identify assembly and handling operations and define procedures to preclude physical damage. Reference applicable documents.

5a. Statement to identify procedural contents and methods of verification of accuracy. Reference applicable documents.

5b. Statement to identify personnel training and certification policies. Reference training records.

6. Specify how the required fault tolerance has been maintained in the software portion of the control system for GSE operations. Reference the software hazards analysis.

7. See Control and Note on previous page.

Safety Verification Methods:

1. See Notes 6 and 7.

2. Describe how it is verified that the firing circuit is free from electro-static effects. Summarize and reference test result.

3. Specify equipment used to limit emission levels. Include analysis and test results (include dB margins).

4. Specify how the procedures are verified. Reference the validation procedure.

5a. Specify procedure review process and validation process. Reference the validation procedure.

5b. Summarize and reference training and certification process. Reference validation procedure.

6. See Note 8.

7. See Verification 1 and the subnote on the first page of this GHR.

Minimum GHR Supporting Data:

1. Provide test equipment specifications (see Note 10).

2. Provide data sheets of material tests.

3. Provide analysis and test reports.

5b. Provide training records.

6. Summary of software safety analysis verification/validation.

7. See item 1.

Generic Hazard Report - No. GO - 6

Subsystem: Electrical

Hazard Groups: Fire/Explosion/Injury or Illness

Hazard Potential: Catastrophic

Hazard: IGNITION OF FLAMMABLE ATMOSPHERE AND/OR MATERIALS

Note: This hazard report may be incorporated with the applicable flight hazard report.

This hazard report should address electrical support equipment and their interfaces with the cargo element, facilities, personnel, and flammable fluids, gases or materials, specifically those addressed in Ground Hazard Report 3. Applicable sections of SAMTO HB S-100/KHB 1700.7 are Paragraphs 4.1.1, 4.3.2 and 4.4.2.

Hazard Causes:

1. Improper design

   a. Hot spots
   b. Arcing/sparking devices
   c. Shorts/faults, etc.
   d. Static discharge

2. Improper use/operations

   a. Improper installation/assembly
   b. Operator error
      1) Procedural inadequacy
      2) Training, certification, and/or supervisory inadequacies
   c. Computer software/hardware interface deficiencies

3. Use of hazardous GSE materials

   a. Flammable materials
   b. Static-producing materials
   c. Non-compatible materials

Hazard Controls:

1a. Discuss potential heat sources and how they are controlled during ground operations. Reference applicable procedures.

1b. Discuss what arcing and sparking devices are used and how they are controlled during ground operations. Reference applicable procedures.

1c. Discuss controls to eliminate or minimize the effects of potential shorts/faults during ground operations. Reference applicable drawings.

1d. Discuss use/control of materials that might produce static electricity during ground operations. Reference applicable drawings/procedures.

2a. Statement to identify installation and assembly operations and define procedures to preclude physical damage. Reference applicable procedures.

2b1. Statement to identify procedural contents and methods of verification of accuracy. Reference applicable documents.

2b2. Statement to identify personnel training and certification policies. Reference training records.

2c. Specify how the required fault tolerance has been maintained in the software portion of the control system for GSE operations. Reference the software hazards analysis.

3a. Specify the conditions (i.e., area, atmosphere, operations, etc.) when flammable materials will be used and list restrictions. Reference applicable drawings/procedures.

3b. Specify the conditions (i.e., area, atmosphere, operations, etc.) when static producing materials will be used and list restrictions. Reference applicable procedures.

3c. Specify the conditions (i.e., area, atmosphere, operations, etc.) when non-compatible materials will be used and list restrictions. Reference applicable procedures.

Safety Verification Methods:

1a-c. Specify method of verification. Reference applicable document.
3a-c.

1d. Specify selection of approved materials for hazardous atmospheres. Reference applicable document.

2a. Specify how the procedures are verified. Reference the validation procedure.

2b1. Specify procedure review process and validation process. Reference validation procedure.

2b2. Summarize and reference training and certification process. Reference validation procedure.

2c. See Note 8.

Minimum GHR Supporting Data:

1c. Provide electrical schematic and a table listing wire sizes and fusing.

2b2. Provide training records.

2c. Summary of software analysis, verification/validation.

3a. Provide a table of major flammable materials giving quantities, where used, and requirement for use.

3b. Provide a table of major static producing materials giving quantities, where used, and requirement for use.

3c. Provide a table of non-compatible materials giving amount, where used, and requirement for use.

6.3.1.2 Hazard Report Notes - The following notes correspond to references within the generic hazard reports. These are guidelines that apply in many locations and are listed here and referenced to avoid repeating data within each report.

(1) Specify the total number of independent electrical inhibits that prevent occurrence of the hazard. List the inhibits and indicate if and how each is monitored. Reference the applicable drawings and flight procedures that specify the applicable monitoring. Specify the fault tolerance of the system controlling the electrical inhibits including Orbiter and GSE interfaces. If the electrical inhibits control pyrotechnically activated devices, discuss susceptibility to EMI/EMC and static discharge or refer to a general discussion in another hazard report.

(2) If the design physically locks out flight or ground crew commanding, so state and describe. Otherwise, describe how the required failure tolerance is maintained considering potential errors by the flight crew, processing personnel and/or ground flight controllers. Reference the applicable released drawing or the operations sequence document, respectively.

(3) Specify how the required fault tolerance has been maintained in the software portion of the control system including launch vehicle and GSE interfaces. Reference the software hazards analysis.

(4) Specify how it was verified that the electrical inhibits and controls can withstand the expected STS environments. Reference applicable qualification reports.

(5) Specify what procedure/monitoring will be used to verify that the electrical inhibits are in the proper status prior to launch. Reference the procedure.

(6) Specify and summarize the FMEA (or other analysis) that verifies fault tolerance of the control system. Specify how the FMEA was performed to the level needed to establish the independency of the inhibits (if applicable). Reference the FMEA (or other analysis).

(7) Specify how the hardware lockout or procedures are verified. Reference the validation procedure.

(8) Specify how the software was verified. Reference the verification report.

(9) If a failure occurs, describe how the design is verified to preclude resultant venting, fire, or explosion. When venting cannot be prevented in the event of a major failure, describe how venting will occur in a manner that is not hazardous to the Orbiter.

(10) Schematic showing electrical inhibits, controls (including Orbiter and GSE interfaces) and monitors and which shows independency of the inhibits. Circle and number the electrical inhibits per the hazard control listing.

(11) Table listing the electrical inhibits, when last cycled and how the final status is verified.

(12) Schematic showing how operator commands are locked-out or a description of the procedural sequence to be used to prevent this hazard.

(13) Summary of software safety analysis, verification/validation, etc.

(14) Specify failure tolerance of the electrical controls. Describe how this failure tolerance is attained. Reference applicable drawings.

(15) Diagram showing redundant (etc.) control paths that effect the required failure tolerance.

(16) Specify whether special initiators are used. List lot acceptance criteria. If NSI's are used, state so and reference. For all other pyrotechnic initiators, reference the design and test document used. Determine if the special test requirements of reference 27 are applicable and if so, document and reference compliance efforts. Describe how the circuits are grounded and list special components used (e.g., static bleed resistors, etc.). Show compliance efforts with reference 28 or reference 29.

(17) Specify shielding configurations for RF/EMI attenuation (e.g., twisted/braided, etc.). List potential shielding gaps. Show compliance efforts with references 27, 28, and 29.

6.3 REFERENCES

(1) DOE 76-45/21, SSDC-21; "Change Control and Analysis," March 1981; EG&G Idaho, Inc., P. O. Box 1625, Idaho Falls, Idaho 83415.

(2) Willie Hammer; "Product Safety Management and Engineering;" 1980; Prentice-Hall, Inc., Englewood, N.J. 07632.

(3) Society of Automotive Engineers (SAE), Aerospace Recommended Practice 926.

(4) Willie Hammer; "Handbook of System and Product Safety," 1972; Prentice-Hall, Inc., Englewood Cliffs, N.J. 07632.

(5) DOD 76-45/4, SSDC-4, Revision 2; "MORT User's Manual," May 1983; EG&G Idaho, Inc.; P. O. Box 1625, Idaho Falls, Idaho 83415.

(6) NAVORD OD 44942, Part III; "Weapon System Safety Guidelines Handbook, System Safety Engineering Guidelines," 1973; Naval Ordnance Systems Command, Washington, D.C. 20360.

(7) NAVORD OD 44942, Part IV, "Weapon System Safety Guidelines Handbook, Hazard Control for Explosive Ordnance Production," 1973; Naval Ordnance Systems Command, Washington, D.C. 20360.

(8) Frank McElroy, Editor; "Accident Prevention Manual for Industrial Operations, Administration and Programs;" National Safety Council; (8th Edition).

(9) "Supervisors Safety Manual," National Safety Council, Chicago, Illinois 60611.

(10) Kije, L. T.; "Residual Risk," Russe Press, 1963. (Out-of-Print)

(11) Harold E. Roland and Brian Moriarty; "System Safety Engineering and Management;" John Wiley & Sons, New York; 1983.

(12) "Systems Safety;" Notes for Course No. 529; The George Washington University; May 1979. (Out-of-Print)

(13) Headquarters Air Force Inspection & Safety Center; "System Safety Handbook, AFISC SSH 1-1, Software System Safety," 5 Sept 1985; Norton Air Force Base, CA 92409-7701.

(14) SAMSO STD 79-1, "Integrated System Safety Program for the MX Weapon System," AFSC Space & Missile Organization, El Segundo, CA; 25 Sept 1979.

(15) SA-0018, Rev. A, "Peacekeeper Weapon System, System Safety Cable Failure Matrix Analysis, Bent Pin Analysis Users Manual," prepared by Martin Marietta Corporation, Denver Aerospace for the Department of the Air Force, Air Force Systems Command, Ballistic Missile Office.

(16) E. J. Henley, University of Houston, and H. Kumamoto, Kyoto University; "Reliability Engineering and Risk Assessment;" Prentice-Hall, Inc., Englewood Cliffs, NJ 07632.

(17) F. P. Lees; Loughborough University of Technology; "Loss Prevention in the Process Industries, Hazard Identification, Assessment and Control," Volume 1 and 2; Butterworths, London, Boston.

(18) Vesely, Goldberg, Roberts, Haasl; "Fault Tree Handbook," NUREG-0492; January 1981; Systems and Reliability Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

(19) DOE 76-45/11, SSDC-11, Rev. 1; "Risk Management Guide;" September 1982; EG&G Idaho, Inc., P. O. Box 1625, Idaho Falls, Idaho 93415.

(20) DOE, SSDC-17; "Applications of MORT to Review of Safety Analysis;" July 1979; EG&G Idaho, Inc., P. O. Box 1625, Idaho Falls, Idaho 83401.

(21) Headquarters Air Force Inspection and Safety Center; "System Safety Handbook, AFISC 55H1-1, Software System Safety;" 5 September 1985; Norton Air Force Bae, CA 92409-7701.

(22) J. P. Rankin, G. J. Engels, and S. G. Gody; "Software Sneak Circuit Analysis;" DTIC, AF WL-TR-75-254; April 1976; Boeing Aerospace co., Houston, TX 77058.

(23) R. Parsons; "Statistical Analysis: A Decision Making Approach;" Harper & Row, New York, 1978.

(24) JSC 13830, "Implementation Procedure for STS Payloads System Safety Requirements," Rev. A, 16 May 1983.

(25) MIL-STD-1574, "System Safety Program for Space and Missile Systems," Rev. A, 15 August 1979.

(26) Space Division Regulations 127-4, "System Safety Certification Procedures and Technical Requirements for Department of Defense (DOD) Space Transportation System Payloads," 1 October 1981.

(27) NHB 1700-7, "Safety Policy and Requirements for Payloads using the Space Transportation System (STS)," Rev. A, 9 December 1980.

(28) MIL-STD-1512, "Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods," 21 March 1972, or MIL-STD-1512 STS Tailoring, 15 April 1983.

(29) MIL-STD-576, "Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems," 31 July 1984.

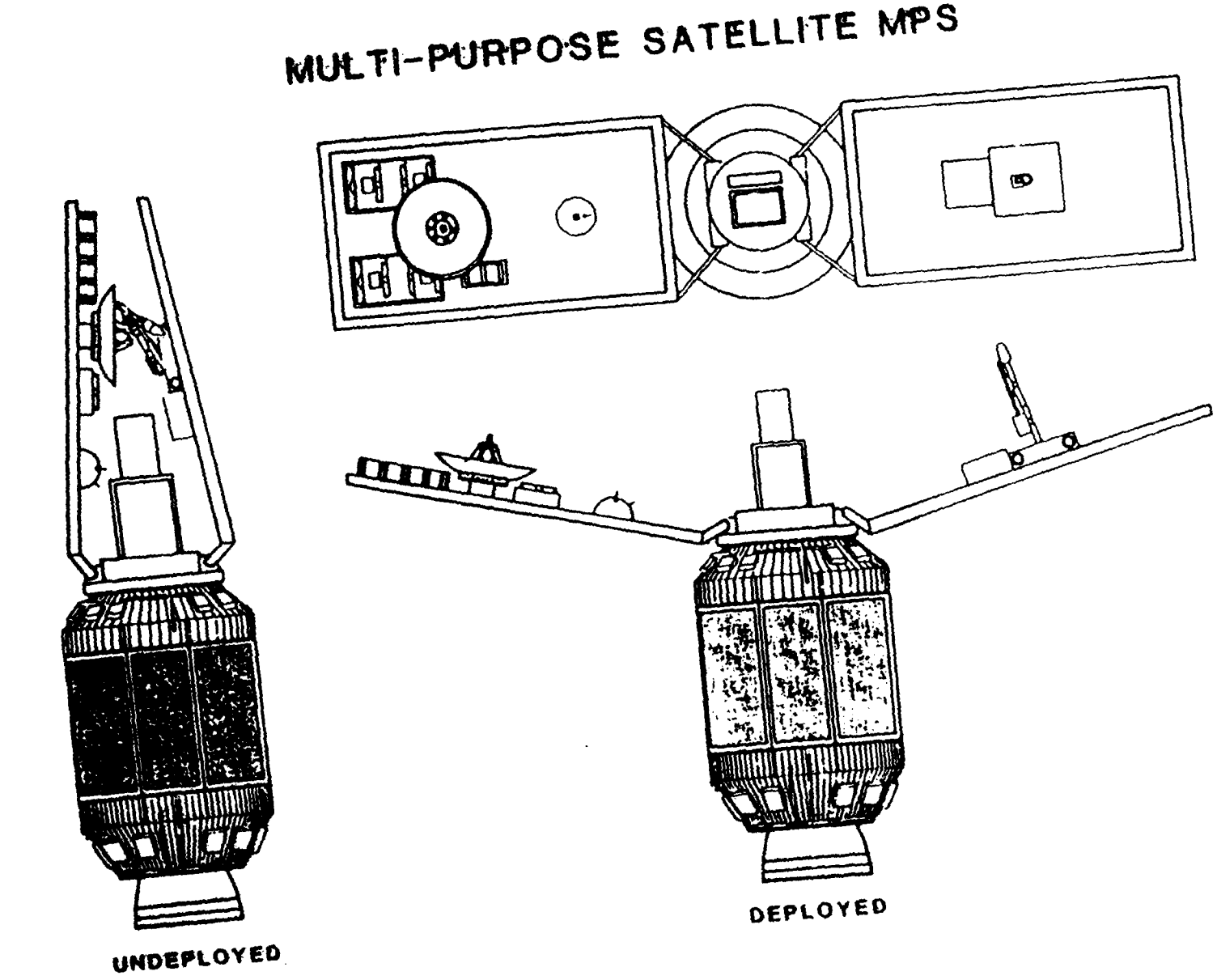
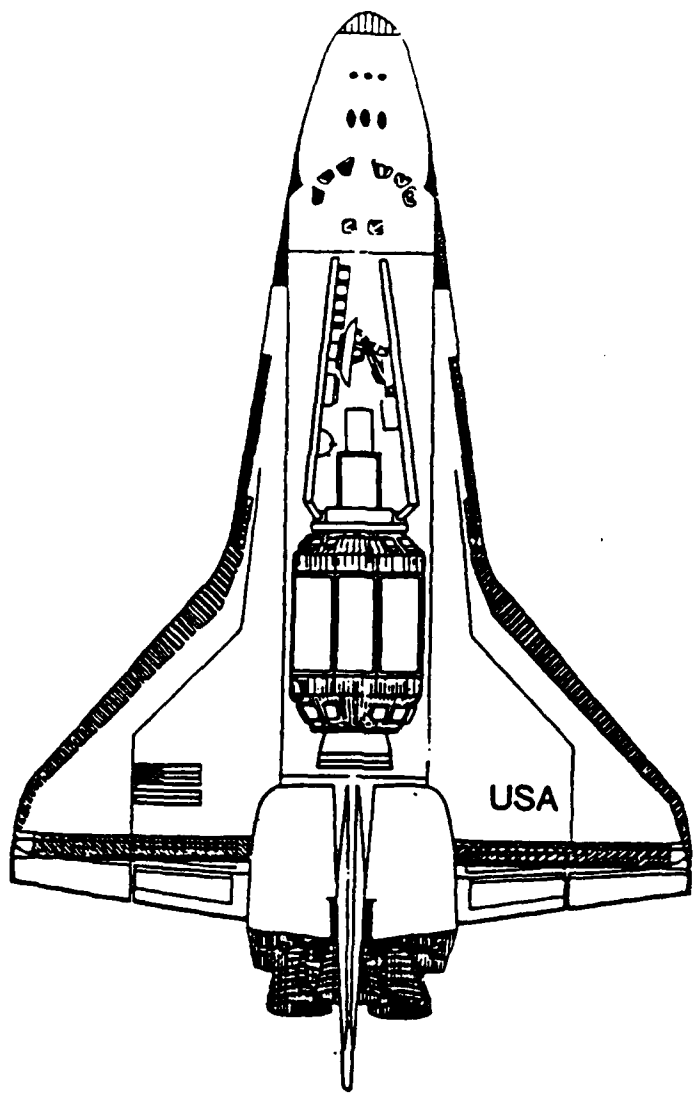


Figure 6-1 Multipurpose Satellite (MPS)

MULTI-PURPOSE SATELLITE MPS



UNDEPLOYED

Figure 6-2 MPS Undeployed

Figure 6-3 MPS - Exploded View

ORGANIZAING A DESIGN HAZARD ANALYSIS

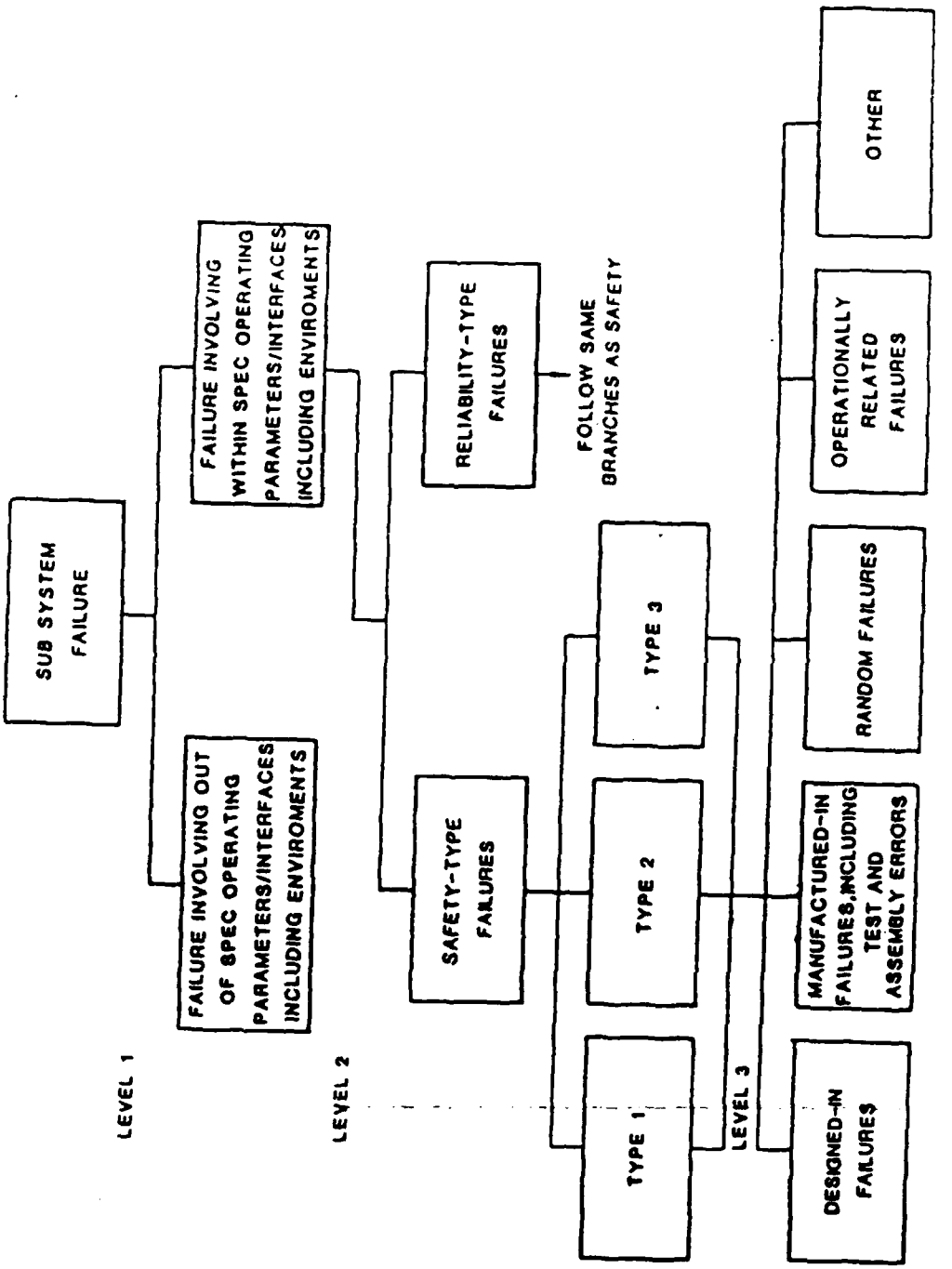


Figure 6-4 Organizing a Design Hazard Analysis

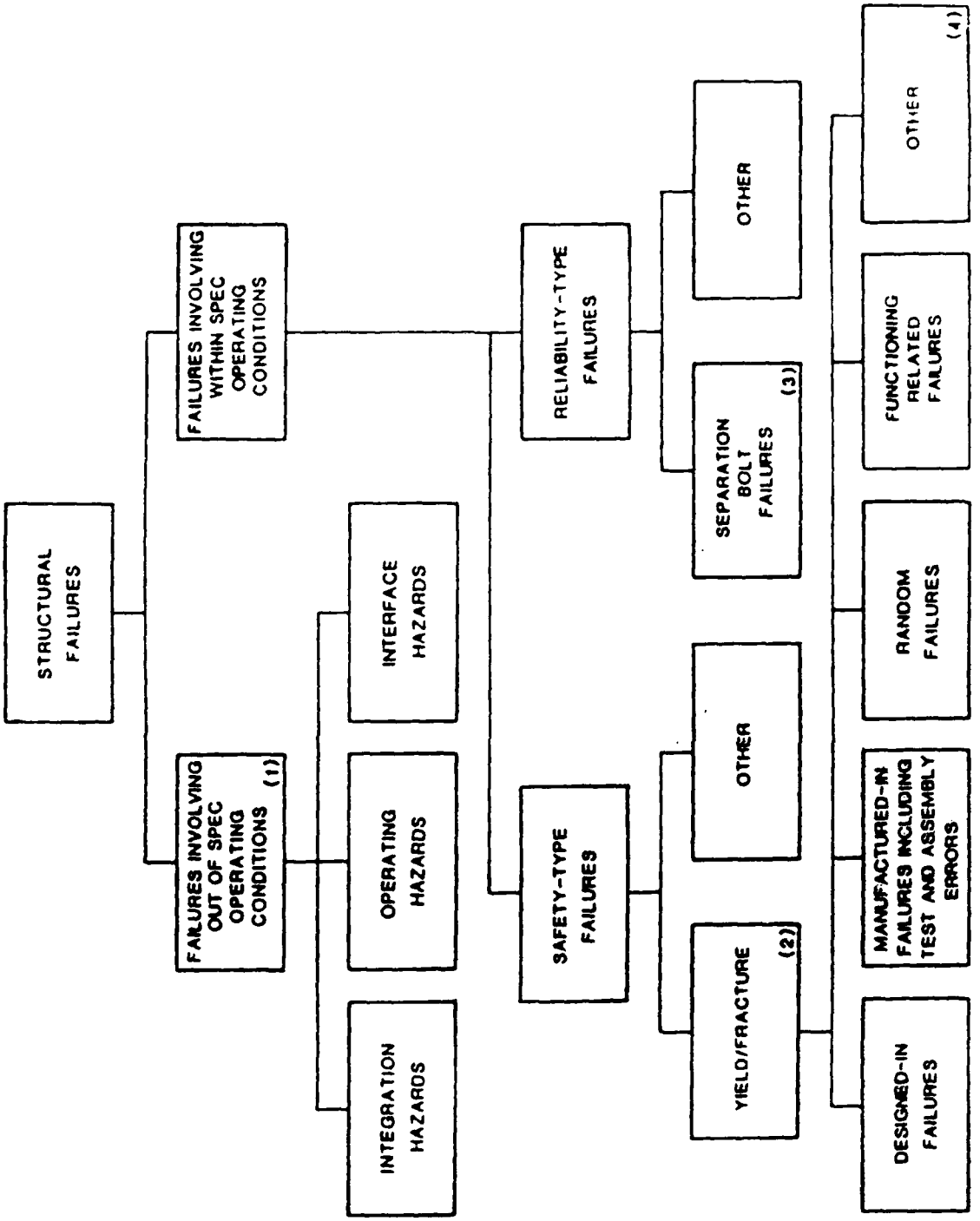


Figure 6-5 Organizing Hazards Analysis of Structure

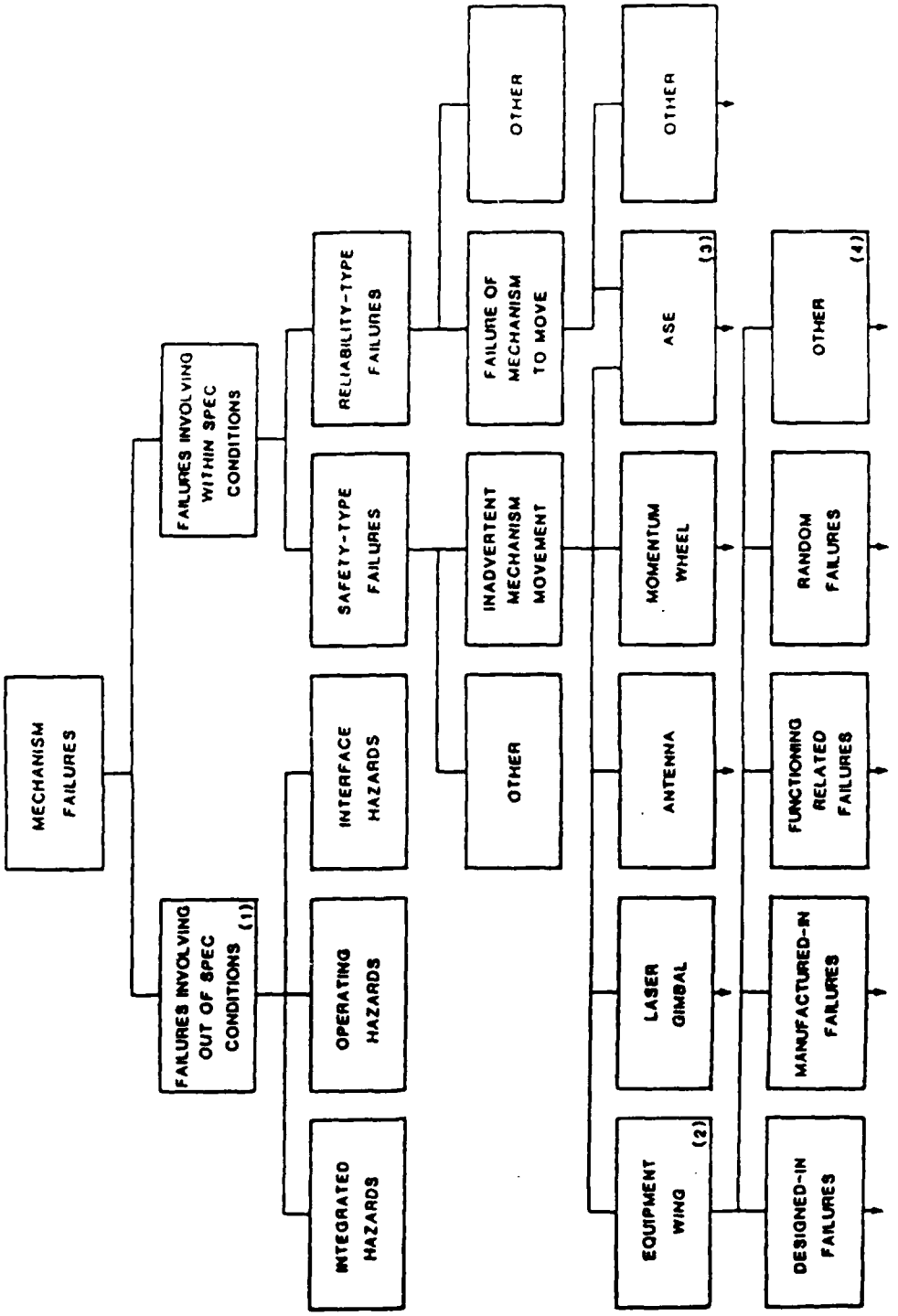


Figure 6-6 Organizing Hazards Analysis of Mechanisms

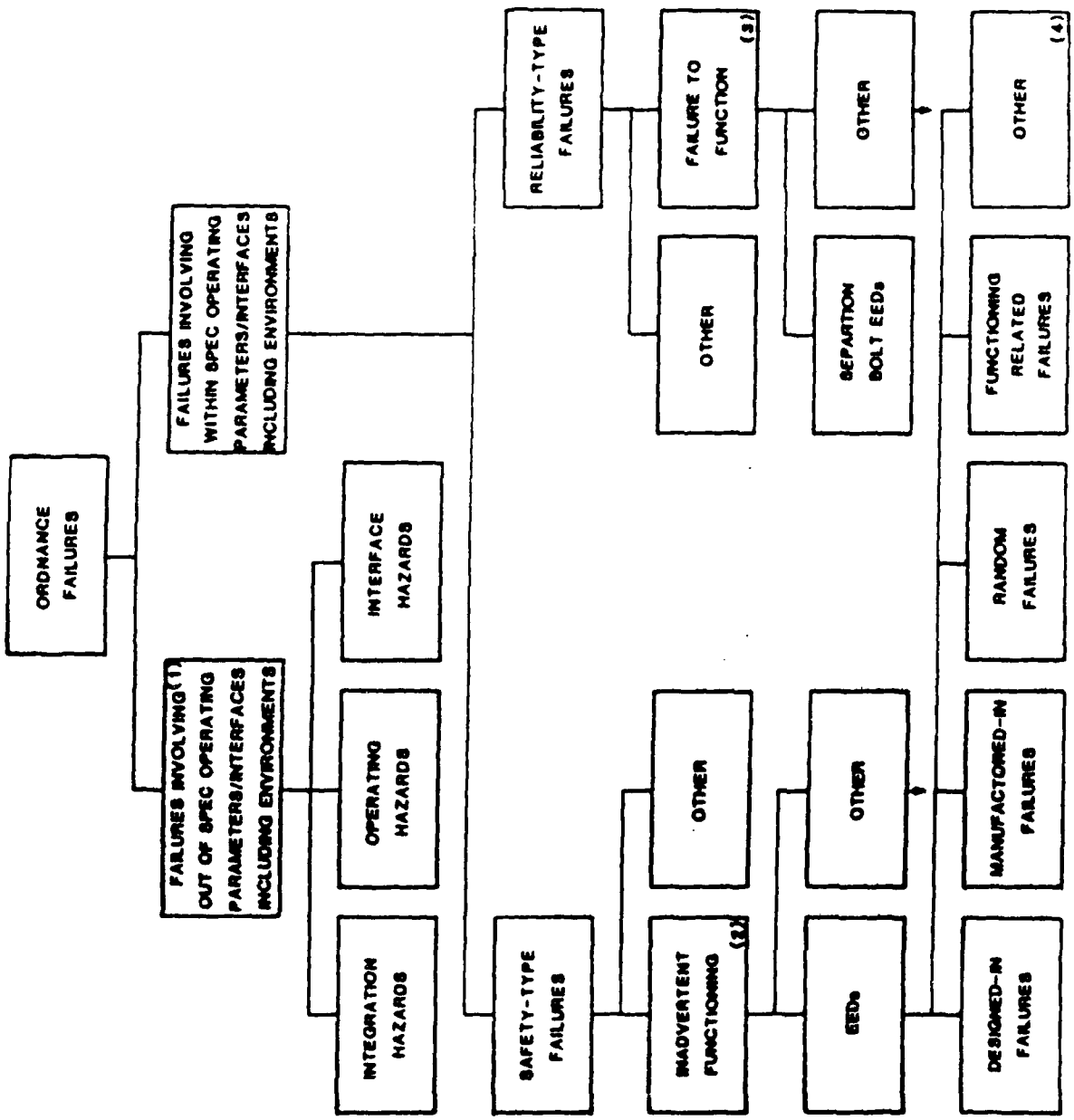


Figure 6-7 Organizing Hazards Analysis of Ordnance

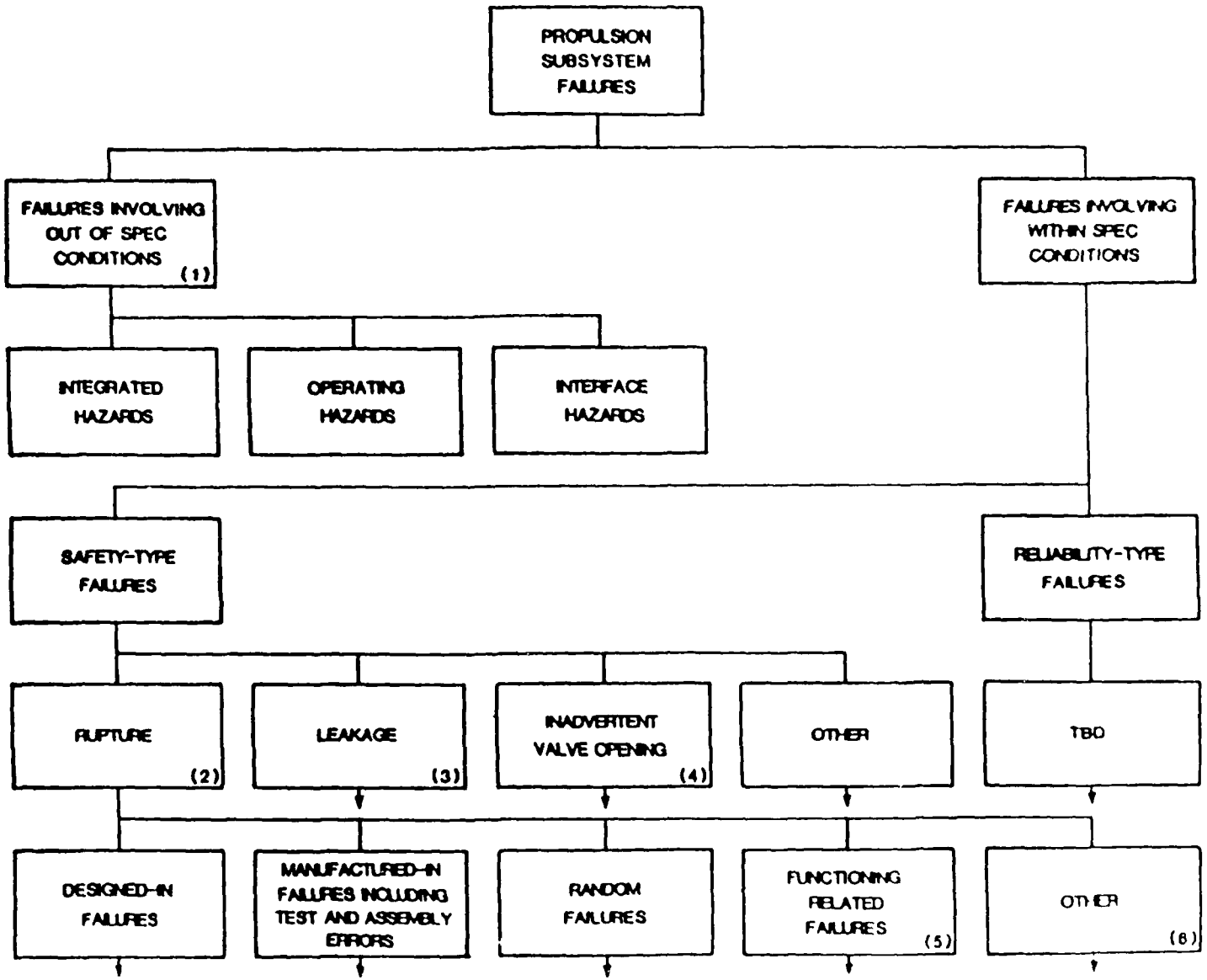


Figure 6-8 Organizing Hazards Analysis of Propulsion

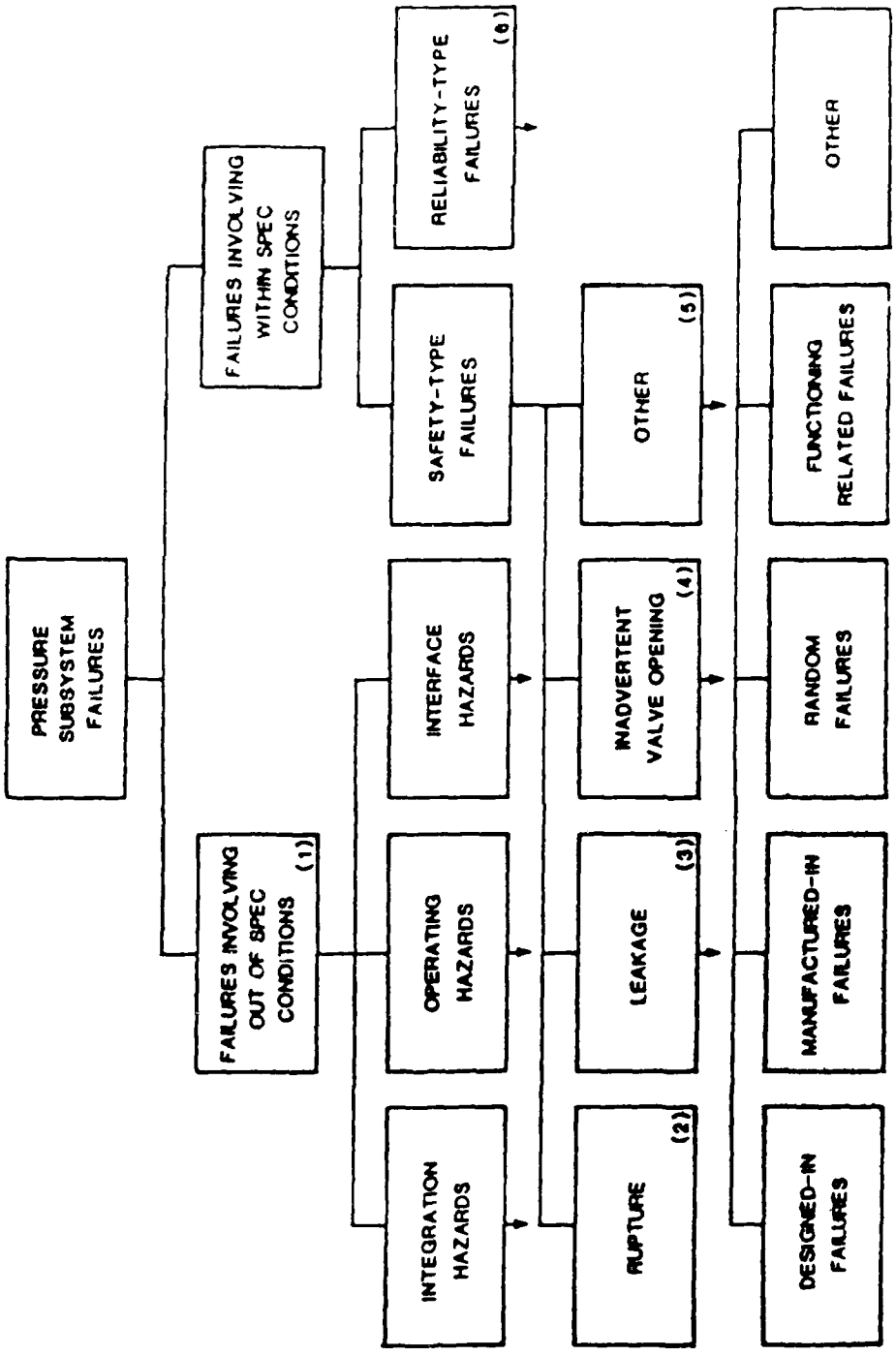


Figure 6-9 Organizing Hazards Analysis of Pressure

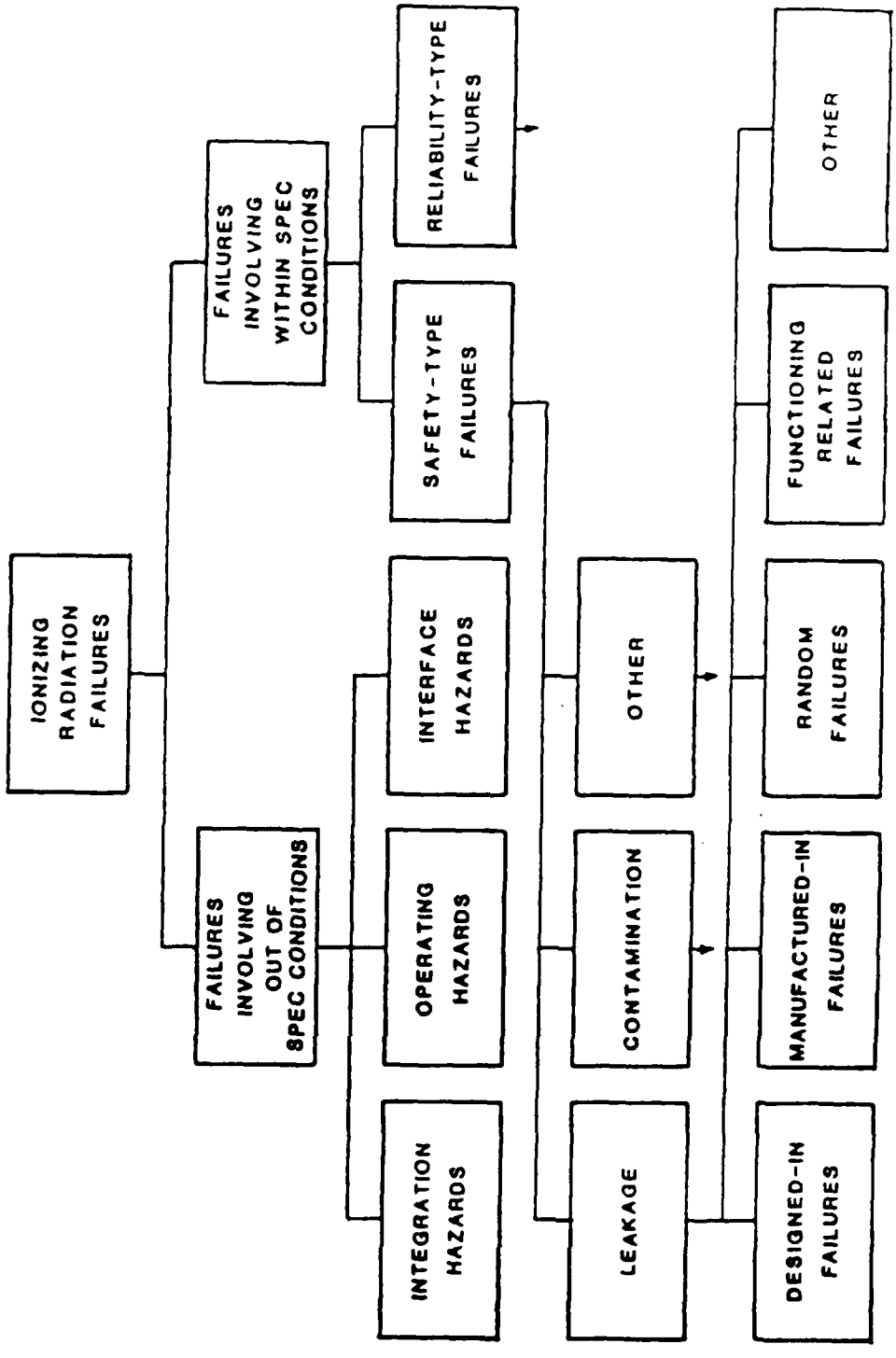


Figure 6-10 Organizing Hazards Analysis of Ionizing Radiation

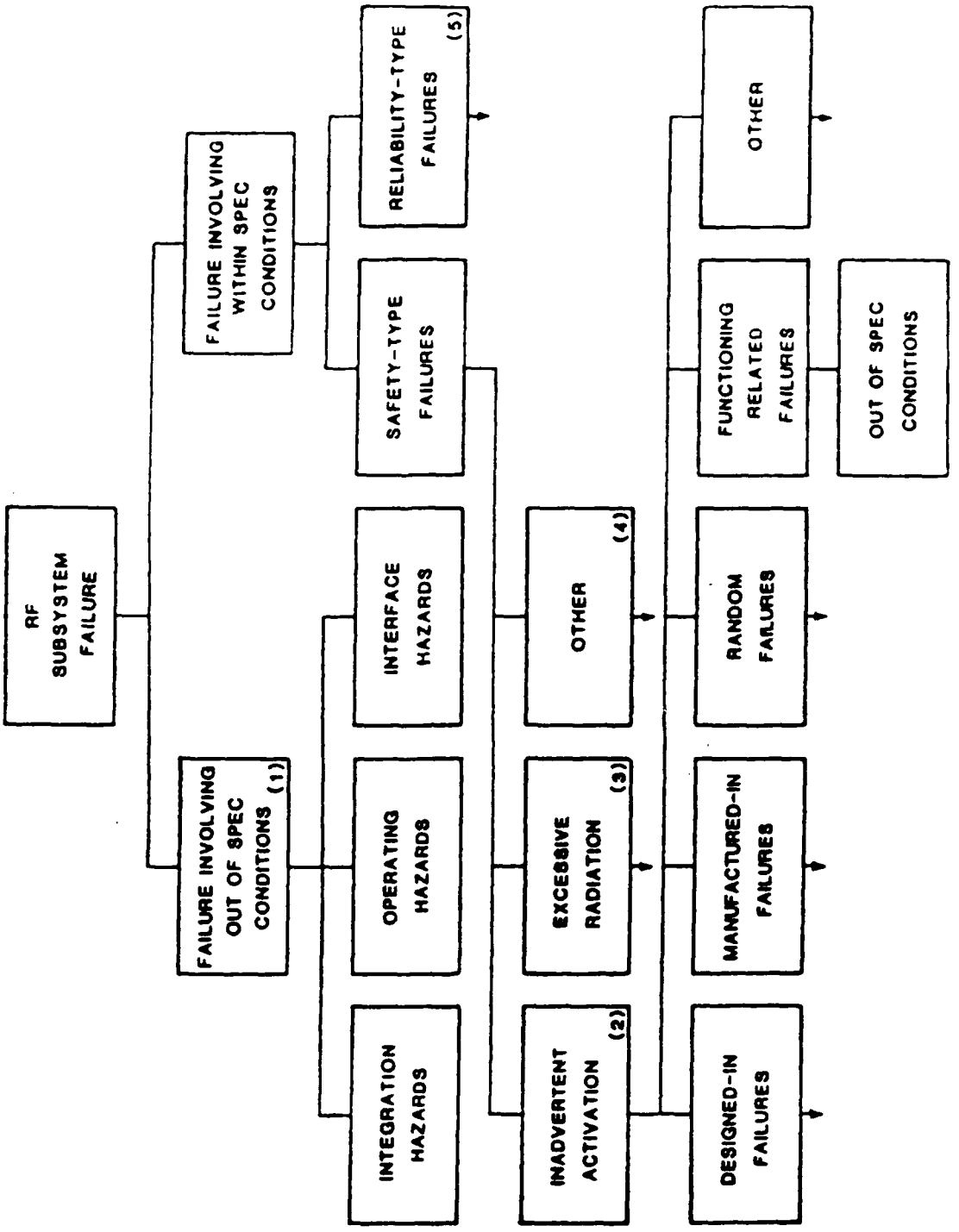


Figure 6-11 Organizing Hazards Analysis of RF

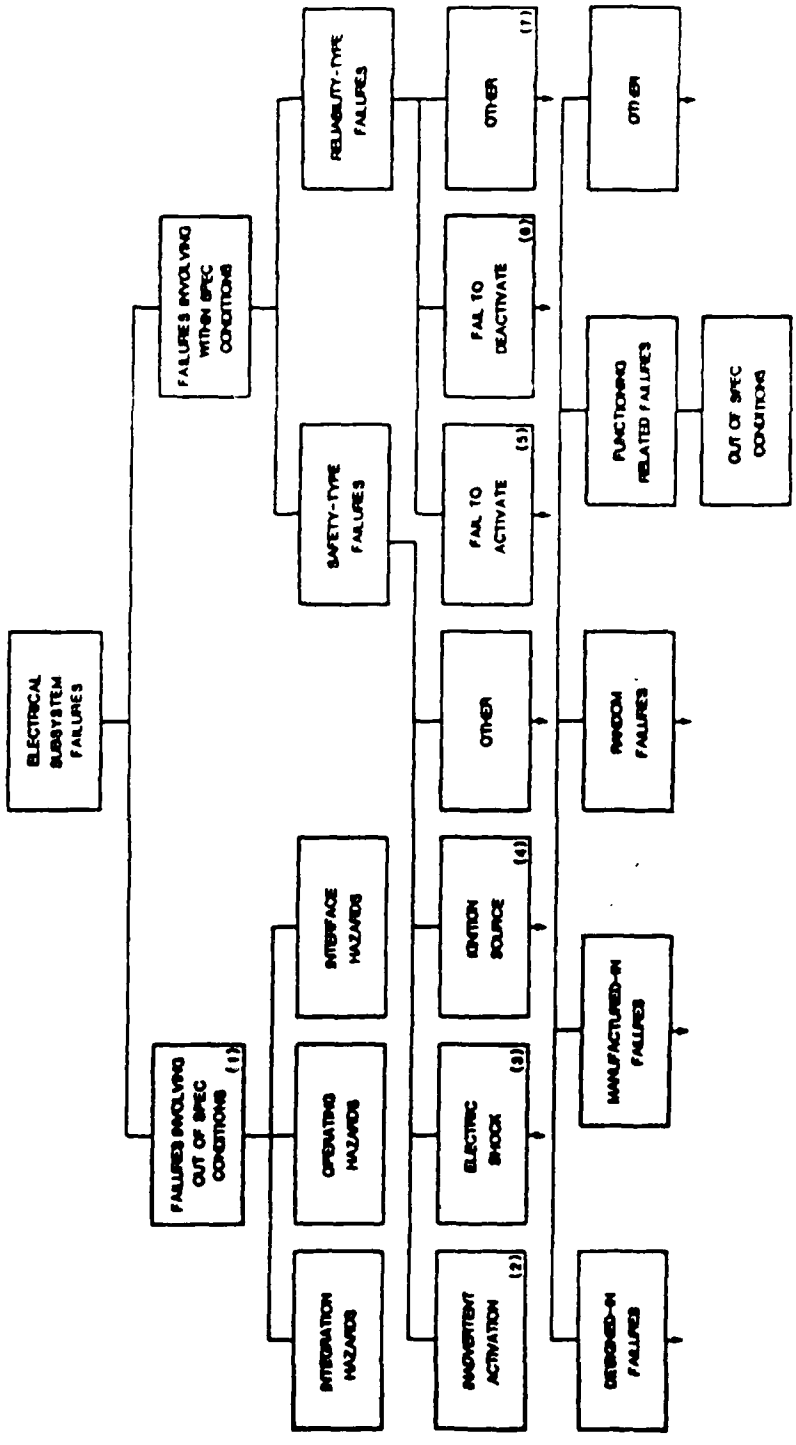


Figure 6-12 Organizing Hazards Analysis of Electrical Subsystem

Chapter 7
Risk Assessment

CHAPTER 7
RISK ASSESSMENT

TABLE OF CONTENTS

Section	Title	Page
7.0	Risk Assessment	7-1
7.1	Conformance to Program Requirements	7-1
7.1.1	Risk Factor	7-1
7.1.2	Compliance	7-1
7.1.3	Noncompliance Items	7-2
7.2	Mishap Severity	7-2
7.3	Mishap Probability	7-3
7.4	Credibility Determination	7-7
7.4.1	Non-Credible	7-7
7.4.2	Credible	7-7
7.5	Criticality	7-8
7.6	Criticality Ranking	7-8
7.7	Mishap Risk Controls	7-11
7.8	Mishap Cost Assessment	7-11
7.9	Accident Risk Assessment Reporting	7-12
7.10	References	7-13

LIST OF FIGURES

Figure No.	Title	Page
7-1	Acceptable Risk Probability	7-14
7-2	Expected Loss Index	7-14

LIST OF TABLES

Table No.	Title	Page
7-1	Mishap Severity Category	7-2
7-2	Program/Mishap Risk/Confidence	7-5
7-3	Qualitative Probabilities	7-6
7-4	Qualitative/Quantitative	7-6

CHAPTER 7
RISK ASSESSMENT

7.0 RISK ASSESSMENT

Mishap risk assessment is the evaluation process which follows identification of the system hazards and the events which can lead to a mishap. Once the hazards, events and mishaps have been identified and documented, each mishap risk is individually assessed to determine its degree of conformance to program risk acceptability parameters and its overall effect on program cost, schedule, personnel injury and system loss/damage (as applicable).

Several techniques, both qualitative and quantitative, have been published to assist in the assessment of mishap risk. Information on these is provided in the following paragraphs.

7.1 CONFORMANCE TO PROGRAM REQUIREMENTS

The System Safety Checklist, prepared and completed as described in Chapter 6.0, is a concise technique for determining and documenting how program mishap risk acceptability parameters have been satisfied. A properly completed checklist permits the identification of safety concerns, describes the degree of compliance to each requirement and identifies each item of noncompliance for which a deviation will be sought or additional controls must be implemented. Checklist assessment will lead to identification of risk factors, development/verification of controls to comply with requirements and the identification of items not in compliance.

7.1.1 Risk Factor

A risk factor is a triggering mechanism which has the effect of release of a hazard (energy source).

The engineering response to each checklist item should be carefully evaluated to detect any risk factor which is not eliminated or controlled by design. For each risk factor found, a Hazard Report will be initiated and tracked until the issue is closed. Any resulting safety concern shall be formally identified to the purchasing office for resolution.

Another source of risk factor identification is the Preliminary Hazard Analysis (PHA) which is used to identify mishap risks which are not covered by the contractually imposed standards and requirements. Each mishap risk identified by the PHA will also be documented on a Hazard Report and tracked to closure.

7.1.2 Compliance

For each Hazard Report generated, the system safety engineer will identify controls required for elimination or control of the risk factor. The responsible engineering element will respond by selecting a control and implementing it in a descending order of precedence, starting with design. The selected control must eliminate or control the risk factor and must be verified in effect before the Hazard Report is closed.

7.1.3 Noncompliance Items

Items of noncompliance fall into several categories including: (a) those that do not meet the letter of the requirement but provide equivalent safety of design; (b) risk factors whose credibility and/or probability of occurrence are so low that the cost of reducing risk is not warranted; (c) items of safety concern which cannot be resolved at the contractor level and must be elevated to the purchasing office for resolution (e.g., although the resulting hazardous event has a very low predicted level of probability, the result is catastrophic); and (d) recognized noncompliance to new requirements on a previously approved flight qualified design with successful operational experience.

With the exception of category (a), noncompliance items require submission of a Deviation Request and approval by the purchasing office. If the approval is not granted then a design change or other satisfactory measures to mitigate the mishap risk must be implemented.

For category (a) items, the customer group responsible for evaluation must be contacted and the details of each item discussed and agreed upon. Then a thorough description and rationale for design equivalency must be formally prepared for each item and submitted through the purchasing office. To prevent an unwarranted loss of time, and perhaps design changes, it is imperative that the details of equivalency and preliminary approval be coordinated prior to submission of the equivalency agreement.

When the approved deviation requests or equivalency letter have been received, the appropriate Hazard Reports can be closed. The associated data presented with each deviation request or equivalency justification must be carefully documented in the appropriate Hazard Report.

7.2 MISHAP SEVERITY

The risk associated with any mishap always has the dimensions of severity (i.e., consequence of or loss from) and probability of occurrence. For the purposes of uniformity in developing risk acceptability requirements and in developing risk assessments, mishap severity is often identified by category of severity. Mishap severity categorization is an early step in risk assessment. It categorizes mishap severity by the degree of personnel injury and system damage expected as a consequence of a mishap. The mishap severity categories used by Mil-Std-882B are illustrated in Table 7-1. These mishap severity categories are consistent with those of NHB 1700.7A.

Table 7-1 Mishap Severity Category

Description	Category	Mishap Definition
CATASTROPHIC	I	Death or system loss.
CRITICAL	II	Severe injury, severe occupational illness, or major system damage.
MARGINAL	III	Minor injury, minor occupational illness, minor system damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or system damage.

Mishap categorization is not sensitive to mishap controls or probabilities of occurrence. A mishap will retain its classification (Category I, II, III or IV) for as long as the source of the mishap exists. However, the risk associated with the mishap (i.e., predicted frequency of occurrence and resultant effects) may be acceptable if controlled effectively by design changes, reduction of exposure, the inclusion of safety devices or procedural constraints.

Mishap severity categorization will not always be adequate as a measure of mishap severity for risk assessment purposes. This will be true where the most severe category does not adequately measure the real consequence of a mishap. Examples of such consequences are:

(1) Those which threaten public acceptance of a program.

(2) Those which result in failure of a mission vital to national security.

(3) Those which threaten the environment of the system where the risks are largely involuntary.

In the case where categorization of the severity of mishap is not an adequate measure, the consequences of a mishap should be estimated explicitly. The estimated consequence of a mishap can be maintained as a measure of mishap risk separate from probability of occurrence as it can be combined with probability of occurrence to yield an "expected" consequence. An excellent reference to this approach is William Rowe's An Anatomy of Risk (Wiley 1977)[3].

7.3 MISHAP PROBABILITY

Normally the level of risk associated with each mishap severity category is identified as being acceptable or unacceptable. This determination of risk acceptability may be based on a quantitative analysis, which numerically predicts the probability of occurrence of the undesired event. Program requirements usually dictate the probability of occurrence level at which a given mishap category becomes acceptable. For example, a given program may accept each catastrophic event with a probability of occurrence less than or equal to 1×10^{-6}. A guideline suggested by the US Navy for the development of acceptable risk parameters is shown in Fig. 7-1. In this example, category I risks above 1.0×10^{-6} are not acceptable. Similarly, category II, and III risks above 1.0×10^{-5} and 1.0×10^{-2} respectively are not acceptable.

Although the acceptable risk probabilities shown in this figure are not directly applicable to booster and space systems, similar figures can be developed to meet individual program requirements.

For risk assessment purposes, the development of mishap risk probabilities will normally consider the probability of one or both of the following phenomenon to occur.

(1) A mishap occurs in a single mission for an individual item or system.

(2) A mishap occurs over a series of planned missions/systems, or the life of a program.

Mishap risk for an individual item or system in a single mission will generally result from the event probabilities calculations as described or referenced in Chapter 4.0. In the context of reliability, mishap risk will always be identical to the calculated event probability where the mishap is the event of interest. The confidence that a mishap will not occur is always equivalent to the reliability, or probability of success, i.e.,

$$\text{Confidence} = 1.0 - \text{Mishap Risk}$$

It must be remembered that the credibility of any risk assessment is totally contingent upon the credibility of a scenario of events, and the credibility of the failure probability models for each event in the scenario. These models and assessments are always predictive in nature, regardless of the historical basis. For this reason, the concept of statistical confidence does not apply. Any attempt to do so is potentially misleading. The term confidence in this discussion does not mean or imply statistical confidence. It is used here to denote the assessed probability of success.

Mishap risk over a series of missions or the life of a program can be viewed most clearly as

$$\text{Mishap Risk} = \text{Probability that one or more mishaps occur}$$

$$\text{Confidence} = \text{Probability that no mishaps occur}$$

Where the event probability for each mission in a program (i.e., the mishap risk for each mission) are small (say less than 0.01), the mishap risk for the program can be considered to be the sum of the a-priori mishap risks for each mission, where that sum is also small (say less than 0.10). In effect,

$$\text{Mishap Risk}_{\text{Program}} = \text{SUM}\ (\text{Mishap Risk}_{\text{Mission}})$$

for all n missions, and $\text{confidence}_{\text{program}} = 1.0 - \text{Mishap Risk}_{\text{program}}$.

It will be rare that the mishap risk on a given mission will be so large as to invalidate this approximation. However, the aggregate of a-priori mishap risk (which really is an expected number) may be large enough to invalidate the previous result. In that case, the mishap risk and confidence for the program can be calculated from the Poisson, i.e.,

$$\text{Mishap Risk}_{\text{Program}} = \text{Probability of one or more failures} = 1.0 - e^{-\text{lamda}}$$

where lamda = expected number of failures
= SUM ($\text{Mishap Risk}_{\text{mission}}$) for all n missions.

Table 7.2 illustrates the above approximations for various combinations of $\text{Mishap Risk}_{\text{Mission}}$ and number of missions.

Table 7-2 Program Mishap Risk/Confidence

Mishap Risk (Mission)	Confidence (Mission)	Missions (n)	n X Mishap Risk (Mission)	Mishap Risk (Program)	Confidence (Program)
0.001	0.999	1	0.001	0.001	0.999
0.001	0.999	50	0.050	0.049	0.951
0.01	0.990	10	0.100	0.095	0.905
0.01	0.990	50	0.500	0.393	0.607
0.01	0.990	100	1.000	0.632	0.368

Most frequently, the probability that the mishap will occur is deduced qualitatively because insufficient data is available to support a quantitative analysis. The qualitative determination is generally based on research, analysis, historical safety data, or sometimes engineering judgment.

A guideline for the qualitative probability prediction of mishap risk is provided in Table 7-3. For example, mishaps with a predicted occurrence rate of levels A, B or C and having a mishap severity rating of I, II or III (Table 7-1), must be classified as unacceptable until further analysis, or invoked controls, provide evidence that the mishap risk has been eliminated, controlled or reduced to an acceptable level.

It will often be necessary to convert qualitative probability to quantitative probabilities for the decision making process. A common approach is to assign quantitative probability levels to the qualitative levels. Table 7-4 illustrates the process of assignment for the qualitative levels of Table 7-3. It must be noted that the assigned values of Table 7-4 are arbitrary. The set of values of Table 7-4, for example, are not consistent with the acceptability boundries of Figure 7-1. It should also be noted that the conversion process will be most meaningful if the assigned quantitative levels are used as guidance during the very development of the qualitative probabilities for the mishap and the events that make up the mishap scenario.

Table 7-3 Qualitative Probabilities

Description*	Level	Specific Individual Item	Fleet or Inventory**
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in life of an item	Will occur frequently
OCCASIONAL	C	Likely to occur sometime in life of an item	Will occur several times
REMOTE	D	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	E	So unlikely it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

Table 7-4 Qualitative/Quantitative Conversions

Sverdrup** Handbook 6000-8		MIL-STD-882B(1)		
Threshold Level	Probability Value	Level	Descriptive Word	Definition
	3×10^{-1}	A	Frequent	Likely to occur frequently.
8×10^{-2}				
	3×10^{-2}	B	Probable	Will occur several times in life of an item.
8×10^{-3}				
	3×10^{-3}	C	Occasional	Likely to occur sometime in life of an item.
8×10^{-4}				
	3×10^{-4}	D	Remote	Unlikely but possible to occur in life of an item.
8×10^{-5}				
	3×10^{-5}	E	Improbable	So unlikely it can be assumed occurrence may not be experienced.

*Arbitrarily selected, dimensionless numbers
**Sverdrup Training Notes 6000-8i (3rd Edition), Sverdrup Technology Incorporated(4)

7.4 CREDIBILITY DETERMINATION

Credibility determinations are made on systems which produce mishap risk activity. Assessments of the efficiency of controls imposed to reduce the credible mishap risk to an acceptable level can be performed using the guidelines for probability assessment as discussed in Section 7.3. Credible mishaps deal only with systems/components which produce activity that can result in the release of energy, as illustrated by the following definitions.

7.4.1 Non-Credible

Systems/components which do not produce activity are those which contain or constrain energy, or have a supporting function. For this condition, mishap risks are controlled by the application of a fixed, recognized, standard, design allowance or minimum safety factor. For example, the ground pressurization system for a satellite booster is designed, installed, tested and operated to the requirements of the ASME Boiler and Pressure Vessel Code. This code defines a fixed set of standards. A pressurization system that is in accordance with these standards is not subject to over pressurization and rupture. Thus, the mishap risk of over pressurization rupture is considered non-credible.

7.4.2 Credible

Systems/components which produce activity are those which switch, modify, or transmit energy. In this condition, safety critical mishaps are controlled by imposing limitations on the operation, interaction, or sequencing of systems or components. Systems of this type require a detailed functional analysis to determine if component operation, interaction, sequencing, or failure will lead to any unsafe conditions.

For example, an Aerospace Ground Equipment (AGE), high pressure gas system provides pressurized nitrogen to a low pressure launch vehicle propellant tank. Overpressurization of the propellant tank beyond its design burst pressure therefore becomes a credible event. This credible mishap drives the analyst to a detailed functional analysis of the gas system which reveals a single, properly sized and adjusted relief valve is installed in the AGE pressurization line just upstream of the airborne interface. Failure of this relief valve, with full upstream pressure on the system, would result in a catastrophic event. Depending on the program status, at least two courses of action can be taken:

(1) When the program is in its design phase, the control is to add a redundant relief valve at the AGE/Airborne interface. The probability of two functionally verified relief valves failing simultaneously, in conjunction with the pressure regulator, is highly improbable and the hazard risk is reduced to an acceptable level.

(2) When an existing AGE pressurization system is being evaluated to support a new or modified vehicle configuration, cost and schedule may drive the procurring agency to direct the acceptance of some residual mishap risk. In this case the analyst is obliged to impose controls over the operation of the system to reach an acceptable risk level. For example:

(a) The relief valve will be functionally tested within 90 days of vehicle propellant tank pressurization. The valve shall meet the system specification criteria for initial relief, full flow, and reset pressures.

(b) Pressure is introduced into the propellant tank by means of a remote operate valve (ROV) located at the AGE/Airborne interface. This valve is controlled from the pressurization console. After carefully adjusting the pressure regulator to the procedurally defined pressure the console operator shall open the ROV to permit gas flow into the propellant tank. The console operator shall closely scrutinize the system pressure monitor and at any sign of regulator failure, or overpressurization, shall immediately close the ROV.

7.5 CRITICALITY

Criticality is a qualitative method of classification of component/subsystem failure modes by their propogated effect or mishap severity.

The component by its inherent nature may not necessarily be hazardous, nor does the failure of that component necessarily result in an event which damages equipment or injures personnel. The resultant event may be related to system availability, mission success, operational capability or excessive unscheduled maintenance.

The Society of Automotive Engineers (SAE), in Aerospace Recommended Practice 926,[5] categorizes criticality of failure modes as:

Category 1 - Failure resulting in potential loss of life
Category 2 - Failure resulting in potential mission failure
Category 3 - Failure resulting in delay or loss of operational availability
Category 4 - Failure resulting in excessive unscheduled maintenance

For mishap risk assessment we limit our concern to failures which can result in serious personnel injury, loss of life, major system damage or system loss, i.e., Category 1 and Category 2.

The criticality of an identified failure mode is determined by its most damaging effect, whether at the component, subsystem or system level. Once identified, the criticality of the failure mode remains the same, regardless of the controls employed to reduce the mishap risk an acceptable level. The results can be incorporated into the risk prediction and assessment discussed in Section 7.3.

7.6 CRITICALITY RANKING

Unlike criticality, criticality ranking is quantitative, rather than qualitative and incorporates probabilities, probable damage resulting from a failure, operating time, etc., into a formula that results in a criticality number. Criticality ranking is used to determine the following:

(1) Which items should be given more intensive study for elimination of the mishap risk that could cause the failure and for fail-safe design, failure rate reduction, or damage containment.

(2) Which items require special attention during production, require tight quality control, and need protective handling at all times.

(3) Special requirements to be included in specifications for suppliers concerning design, performance, reliability, safety, or quality assurance.

(4) Acceptance standards to be established for components received at a plant from subcontractors and for parameters that should be tested most intensively.

(5) Where special procedures, safeguards, protective equipment, monitoring devices or warning systems should be provided.

(6) Where accident prevention efforts and funds could be applied most effectively.

Criticality Ranking can be accomplished in many ways. The method described by the Society of Automotive Engineers in ARP 926[5] is made an extension of Failure Modes and Effects Analysis (FMEA) and the two are then designed Failure Modes, Effects, and Criticality Analysis (FMECA). In the procedure for quantitative criticality determination, the criticality number for any component or failure mode is indicated by the number of failures of a specific type expected during each million operations occurring in a critical mode. The criticality number, C_r is calculated by:

$$Cr = SUM\ (Beta \times Alpha \times K_E \times K_A \times Lamda_g \times t \times 10^{-6})_n,\ n=1,\ 2---j$$

where C_r = criticality number for the system component in losses per million trials

n = the critical failure modes in the system component that fall under a particular loss statement

j = last critical failure mode in the system component under loss statement

Lamda = generic failure rate of the component in failures per hour or cycle

t = operating time in hours or number of operating cycles of the component per mission

k_A = operational factor that adjust Lamda for the difference between operating stresses when Lamda was measured and the operating stresses under which the component is going to be used

k_E = environmental factor that adjusts Lamda for difference between environmental stresses when Lamda was measured and the environmental stresses under which the component is going to be used

NOTE: for simplified uses, omit K_E, K_A, and use Lamda as the estimated failure rate for the given failure mode and operating condition

Alpha = failure mode ratio of critical failure mode. The failure mode ratio is that fraction of Lamda attributable to the critical failure mode

Beta = conditional probability that the failure effects of the critical failure mode will occur, given that the critical failure mode has occurred. Values of Beta should be selected from an established set of ranges.

Failure Effects	Typical Value of Beta
Actual Loss	100%
Probable Loss	10% to 100%
Possible Loss	0% to 10%
None	0%

10^6 = factor that transforms C from losses per trial to losses per million trials, so C will normally be greater than one

This method requires a great deal of effort when used in this form. A simple method of quantitative criticality determination is to multiply the probability of failure by the damage that could generated. Another method entails ranking by:

$$CR = P_t \times Q \times Fg$$

where CR = criticality ranking
P_t = probable damage resulting from a specific failure mode
Q = probability of component failure (1 - reliability)
Fg = ratio of occurrence of a specific failure mode

The limitations, and strengths, of criticality ranking are as follows:

(1) Identification of the specific failures to which the criticality analysis is to be applied, must be accomplished by an adjunct technique. Due to the broad variety of components that can be considered critical, a variety of specific types of analysis must be selected from. Fault-free analysis, logic trees, network analysis, circuit analysis, or FMEAs can be used, depending upon the type of system. The thoroughness of damage potential ranking will rely on the accuracy and depth of the adjunct technique used.

(2) An assembly may have failure modes that do not result in accidents of concern. These modes must be eliminated before any determination of accident probabilities. Use of logic methods can assist in identifying events, failures, or operations that could contribute to catastrophic occurrences. Then the FMEA could study those conditions in detail, as well as the safety measures to be taken.

(3) Inadequate attention is paid to human error problems because of the concentration of hardware failures. Human errors potentially constitute a large percentage of all accident causes. This is a significant weakness in many safety studies.

(4) Environmental factors are usually considered in establishing stress on hardware. However, environmental profiles are seldom considered.

The analysis is not completed by the ranking process. Evaluations must also establish the measures to be implemented to assure the mishap risks generated by critical component failure are controlled. An effective program should consider the above limitations, as well as the cost-effectiveness of control measures.

7.7 MISHAP RISK CONTROLS

The controls imposed to mitigate each identified mishap risk are individually assessed by a thorough functional analysis, to determine technical adequacy, and evaluated against the degree of compliance with a generally universal "order of precedence" for mishap prevention. Mishap risks are dealt with at the highest feasible level, consistent with the established program cost, performance, schedule and safety requirements. The following order of precedence is extracted from MIL-STD-1574A and is consistent with both DoD and NASA requirements.

(1) Design for minimum hazards.

(2) Safety devices.

(3) Protective systems.

(4) Warning devices.

(5) Special procedures.

When assessing the technical adequacy of the controls, the analyst must have sufficient detailed schematics/drawings to perform a thorough evaluation of the system/subsystem function and assess the efficiency of the selected controls. The presence of the schematics/drawing also permits a reasonable evaluation of the selected order of precedence. In this assessment process the outcome is twofold:

(1) The detailed functional analysis must demonstrate that the identified controls will eliminate the mishap risks or reduce them to an acceptable level.

(2) The selected level of precedence must conform to the specified safety requirements for the appropriate program phase. Risks, for example, which can and should be corrected by design, but are not, must be submitted to the purchasing office for formal acceptance of the added mishap risk.

7.8 RISK COST ASSESSMENT

Unless mishap causes are eliminated, some mishap risk must be accepted and the acceptability limit is determined by the purchasing office. That decision is affected by many factors. One of these factors is cost.

Figure 7-2 illustrates use of the expected dollar loss from a mishap as the measure of mishap risk. In Figure 7-2, any combination of mishap dollar loss and mishap probability that yields an expected mishap dollar loss greater than 5 is unacceptable. It should be emphasized that this example only considers system loss, and does not consider personnel injury or death. In the illustration, a system with a mishap probability of one in a thousand would be acceptable if the dollar loss were $5,000 or less. If the dollar loss was five million dollars, a probability of occurrence of one in a million would be acceptable. Using this concept as a baseline, quantitative design limits can then be defined.

As tradeoffs are being considered and as the design progresses, it may become evident that some contractually defined safety parameters are forcing higher program risk. From the purchasing office perspective, a relaxation of the imposed safety parameters may appear to be advantageous when considering the broader perspective of cost and performance optimization. However, the program director will require that an in-depth assessment of the added mishap risk to both personnel and the environment be made and presented to aid in the decision. After a review of the added mishap risk, the director must make the decision whether to fix the identified problem or formally document acceptance of the added risk.

Whenever cost avoidance, schedule, or mission impact is the prime justification for acceptance of added mishap risk, it is imperative that a detailed system level assessment be performed to assure that risks involving the reasonable possibility of personnel death/injury or environmental impacts are not overlooked. Public opinion, in the case of a major adverse incident, can have an overwhelming effect on a space program. Examples are the resultant effect of public response to the loss of astronauts during ground operations on the Apollo space program or the in-flight destruction of the space shuttle Challenger and death of its crew of seven.

7.9 ACCIDENT RISK ASSESSMENT REPORT (ARAR)

Through implementation of MIL-STD-1574A, the U.S. Air Force requires the preparation and submittal of an ARAR which provides the System Operator and the Test Range Safety Organization with a comprehensive description of potentially hazardous subsystems and operations associated with the primary system(s) and interfaces. The report also includes a comprehensive identification of the mishap risks assumed during the system(s) life cycle and provides a means of substantiating compliance with program safety requirements. It also satisfies the safety data submittal requirements of both the Eastern Space and Missile Center and Western Space and Missile Center.

The NASA does not require the submittal of the ARAR or an equivalent document. NASA relies on the contractors safety analysis and hazard reporting, which are reviewed during the phase safety review process.

The advantage the ARAR has over the individual reports is the comprehensiveness of the contained information. A properly prepared ARAR permits a qualified second party to not only assess the efficiency of the safety analyses but to personally assess the safety critical systems for mishap risks which may have been overlooked in the initial analysis. This is advantageous, not only to the Range Safety Organization, but to any activity tasked with evaluating the prime system contractor's mishap risk assessment and analyses. For that reason we recommend that the preparation of an ARAR prerequisite to safety approval of any booster, upper stage or satellite system.

7.10 REFERENCES

(1) Mil-Std-882B, System Safety Program Requirements, 30 March 1984.

(2) NHB 1700.7A, "Safety Policy and Requirements for Payloads using the Space Transportation System, 9 December 1980.

(3) Rowe, William, An Anatomy of Risk, Wiley, 1977

(4) Sverdrup Technology Inc., Sverdrup Training Notes 6000-8i, 3rd Edition

(5) Society of Automotive Engineers, Aerospace Recommended Practice (ARP) 926

(6) Mil-Std-1574A, System Safety Program for Space and Missile Systems, 15 August 1979.

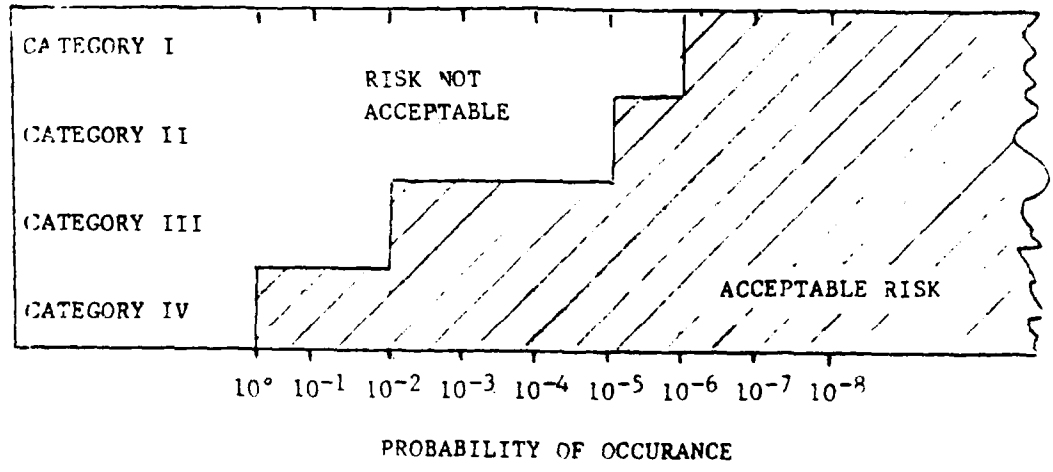


Figure 7-1 Acceptable Risk Probability

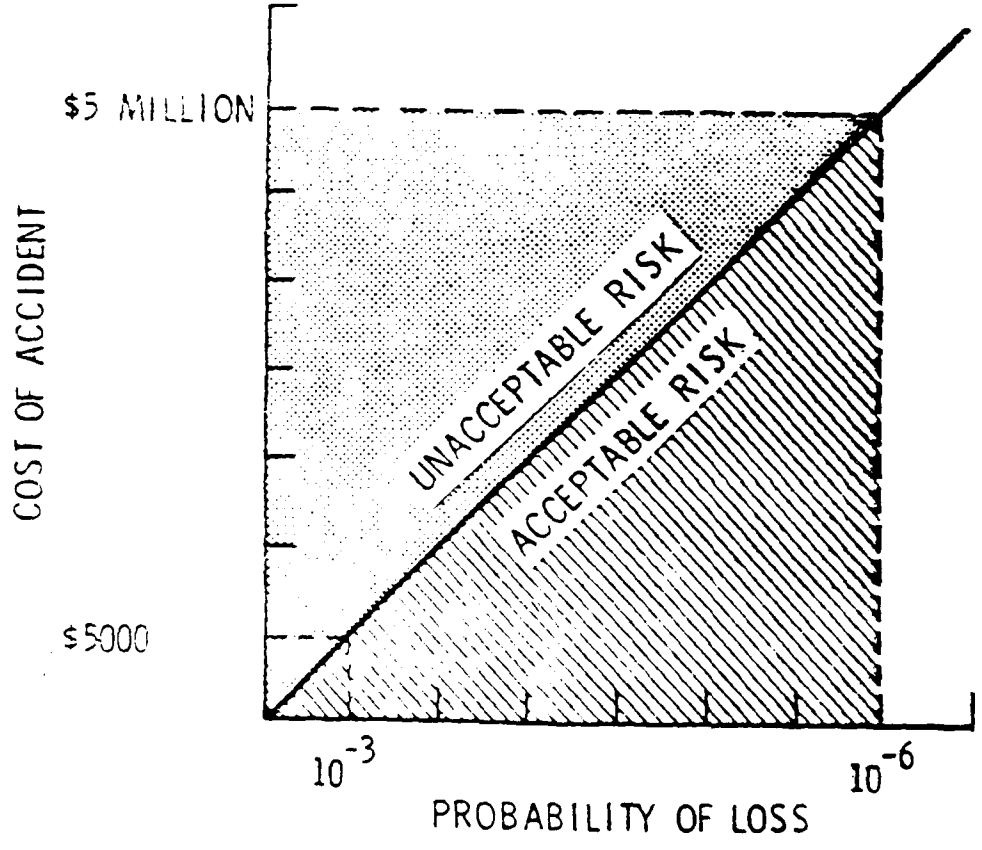


Figure 7-2 Expected Loss Index

Chapter 8
Hazards Analysis and Sa
Approval

CHAPTER 8
HAZARDS ANALYSIS AND SAFETY APPROVAL

TABLE OF CONTENTS

Section	Title	Page
8.0	Introduction	8-1
8.1	Department of Defense (DOD) (Excluding USAF) Approval	8-2
8.2	Department of the Air Force (USAF) Approval	8-2
8.3	Interagency Nuclear Safety Review Panel (INSRP) Approval	8-3
8.4	National Aeronautics and Space Administration Approval	8-4
8.5	National Range Approval	8-4
8.6	References	8-6

LIST OF FIGURES

Figure No.	Title	Page
8-1	The Range Safety Process	8-7

LIST OF TABLES

Table No.	Title	Page
8-1	Requirements for Safety Approval	8-1

CHAPTER 8
HAZARDS ANALYSIS AND SAFETY APPROVAL

8.0 INTRODUCTION

Space launch programs must obtain safety approvals from a variety of government and DOD elements before they can complete their program missions. The approval process and requirements depend on the regulatory, acquisition and user agencies involved and on the major range or test facility utilized. This chapter summarizes the safety approval process and requirements in current use by DOD, USAF, NASA, INSRP and the National Ranges.

In general, the required safety approval can be identified with the type of operations performed and the hazards associated with each, i.e.,

(1) manufacturing and assembly

(2) pre-launch and launch operations

(3) launch vehicle flight and payload on-orbit operations

The procuring and regulatory agencies have the prime responsibility to ensure the safety of hardware manufacture and transportation. The Program Office will provide or coordinate safety approval for these operations. The National Major Ranges and Test facilities are responsible to ensure the safety of prelaunch, launch and flight operations at those locations. The range or test facility commander must approve operations conducted at his facility. Presently no single element is responsible for on-orbit safety. On-orbit safety approval authority currently resides with the user such as NASA, APL or the Air Force Space Command, although the National Range(s) or another single element may be responsible in the future.

The principal sources of requirements for safety approval are identified in Table 8-1 by operational phase:

Table 8-1 Requirements for Safety Approval

PHASE	Reference Requirements Documents
Manufacturing	SPO Specifications and Requirements in Contract ESMC-WSMC Regulations 127-1(1,2) National Standards MIL-STD-882B(3) (1574A-USAF)(4)
Prelaunch/Launch	ESMC/WSMC Regulations 127-1 MIL-STD 1522(5) MIL-STD 882-B DOD 3200.11(6)
Flight/On-Orbit	ESMC/WSMC Regulations 127-1 DOD 3200.11

It should be noted from Table 8-1 that the USAF MIL-STD-1574A, "System Safety Program for Space and Missile Systems," is a tailoring of DOD MIL-STD-882A for missile and space systems. MIL-STD-1574A requirements are likely to be phased out after incorporation into a revision of MIL-STD-882. It should also be noted from Table 8-1 that even though the System Program Office is responsible to levy the requirements of the National Ranges during system development, it is the Range Commander who will approve the proper interpretation and compliance to those requirements prior to the ground processing and launch operations phases.

The safety approval processes and requirements identified in Chapter 8 generally encompass the analysis, data and actions which result from hazards analysis. However, the review and approval of specific hazards of concern and their associated controls must be approached on an individual basis. These must be reviewed with procuring agency for disposition at the earliest possible point in time.

8.1 DEPARTMENT OF DEFENSE (DOD) (EXCLUDING USAF) APPROVAL

The current DOD level safety document in general use for systems procurement is MIL-STD-882B, "System Safety Program Requirements." This standard details the "uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing the associated risk to a level acceptable to the managing activity."

MIL-STD-882B is separated into twenty-two (22) separate tasks. The managing authority is responsible for selecting the appropriate tasks to be imposed on the contractor, based on the complexity, criticality and damage potential of the system. Guidance for the selection of each task is provided in Appendix A to MIL-STD-882B.

When the managing authority elects to require formal approval of the contractors hazard assessment, Task 103, "System Safety Program Reviews," is invoked. The contractor responds by providing scheduled "system safety program reviews to periodically report to the managing authority and the status of hazard analyses, safety assessments, and other parts of the system safety program." The contractor may also be required to support presentations to other Government certifying boards (e.g., nuclear safety board.)

Approval of the contractor's hazard assessment by the managing authority is not delegated to a specifically defined individual or group having qualifications for assessing hazards. In specific instances, where the managing activity has established a safety office with well-defined objectives, qualifications, and authority, the DOD MIL-STD-882B, Task 103, approval process has been very effective. The process can be vulnerable to management authority, however.

8.2 DEPARTMENT OF THE AIR FORCE (USAF) APPROVAL

The USAF uses MIL-STD-1574A, "System Safety Program for Space and Missile Systems," to implement a system safety program for space and missile systems procurement. The MIL-STD "establishes administrative and technical means by which accident prevention requirements and policies are planned,

managed and implemented into the total program effort." It defines the requirements for implementation of system safety activities covering the life cycle of the program that includes design, development, test, checkout modification, production, servicing, refurbishing maintenance, transportation, handling, training, disposal, and contingency operations.

Paragraph 4.5 of MIL-STD-1574A provides for system development contractor support of a System Safety Group (SSG). The SSG is comprised of assigned Air Force program-personnel and appropriate contractor system safety managers. It functions in accordance with the SSG charter established by the Air Force Program Director. The function of the SSG is to deal with safety concerns but generally does not become involved in program level safety reviews.

For space systems, the Air Force implements Space Division Regulation (SDR) 127-8 in conjunction with MIL-STD-1574A. SDR 127-8 implements a formal safety assessment process to support the Program Office responsibility to comply with safety requirements and minimize mishap risk. The safety assessment process includes a Safety Review Team (SRT) which meets in a series of incremental reviews that correspond closely with the critical phases of System Development. SDR 127-8, Volume I, establishes the review process requirements for DOD payloads for the National Space Transportation System (NSTS). Volume 1 has been implemented. SDR 127-8, Volume II, establishes the safety assessment process for expendable launch vehicles. Volume II is in development. SDR 127-8, Volume III, will provide safety certification procedures for facilities.

The function of the SRT is to review the contractor technical data and hazard assessment provided at the review meetings, and to recommend action and direction. MIL-STD-1574A does not require system development contractors to deliver their hazard assessment data to the SRT which is implemented by SDR 127-8. This can result in abbreviated data presentations to the SRT and make reasonable evaluation difficult. The Program office and the system development contractor should ensure that the SRT has all necessary program safety data prior to a scheduled review to permit a thorough evaluation.

8.3 INTERAGENCY NUCLEAR SAFETY REVIEW PANEL (INSRP) APPROVAL

The launch of major radioactive sources into space requires Presidential approval. The current Interagency Nuclear Safety Review Panel (INSRP) was established by Presidential Directive/National Security Council (NSC) Memorandum 25 (December 14, 1977) to perform safety assessments. Three coordinators direct the activities of INSRP, with one coordinator from each of the agencies; the Department of Defense, the Department of Energy, and the National Aeronautics and Space Administration. The coordinators have established five subpanels, with members from various government agencies, private industry, and consultants, to perform the detailed technical safety analyses of space missions that carry radioactive material. These subpanels are: Launch Abort Subpanel, Reentry Subpanel, Meteorological Subpanel, Oceanographic Subpanel, and Biomedical and Environmental Effects Subpanel.

The agency sponsoring the development of a space launch mission carrying a major radioactive source initiates the INSRP safety review process by request. Both informal and formal safety review meetings are held. Formal reviews are conducted for the program's Preliminary Safety Analysis Report (PSAR) and the Updated Safety Analysis Report (USAR). The PSAR should be prepared as early as possible in the development program while the USAR should be accomplished as soon as possible after the design concept is frozen. The INSRP, having no directional authority, makes recommendations to the mission sponsor regarding safety issues.

At the end of the program development effort, and approximately one year prior to launch, the mission sponsor submits a Final Safety Analysis Report (FSAR) to INSRP for review. From this, and other information, the INSRP performs a detailed technical safety review and prepares a Safety Evaluation Report (SER). The SER is submitted to the Office of Science and Technology Policy (OSTP). Launch approval may be granted by the Director of OSTP or by the President when necessary.

8.4 NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA) APPROVAL

The NASA Headquarters document, "Safety Policy and Requirements for Payloads Using the Space Transportation System," NHB 1700.7A[8], establishes the technical and system safety requirements applicable to all STS payloads. The launch/landing site safety requirements are specified in the joint NASA/Air Force document SAMTO HB S-100/KHB 1700.7, "Space Transportation System Payload Ground Safety Handbook."[9]

The requirements of the safety review process for STS payloads are defined in NASA document JSC 13830A, "Implementation Procedure for STS Payloads System Safety Requirements."[10] It describes the initial contact meeting between the Safety Review Panel (SRP) and the Payload organization (contractor) and defines the subsequent safety reviews necessary to assure compliance with the safety requirements contained in NHB 1700.7A and KHB 1700.7. These reviews occur in four phases (0, I, II, and III) and are timed to coincide with Payload/GSE conceptual design, Payload/GSE preliminary design, Payload/GSE final design and Payload/GSE fabrication and Payload/GSE testing, respectively.

8.5 NATIONAL RANGE APPROVAL

The DOD has two National Ranges, both managed by the Air Force. These are the Eastern and Western Space and Missile Centers (ESMC and WSMC). The majority of payloads launched into space will fly from one of these two Ranges. Their approval requirements are discussed in detail in this section.

DOD Directive 3200.11 designates the Center Commanders as the responsible agents for prelaunch, launch, and flight safety or all launch vehicles, upper stages and payloads launched from their respective Ranges. The safety approvals required by each Range and their design and operational requirements are identified in their Range Safety Manuals, ESMCR and WSMCR 127-1. These documents are very similar and identify the same approval requirements: flight plan approval; prelaunch, missile/launch vehicle checkout and assembly approval; flight termination system approval; radioactive material launch and use approval; and systems safety approval. Figure 8-1 illustrates a general timeline for the Range Safety Process.

The National Ranges use the review processes discussed earlier to accomplish other goals. For example; the Safety Review Team (SRT) used for STS payloads is supported by the Ranges. It may fulfill some of their requirements although it does not deal with Flight Termination System (FTS) or flight plan approvals. The INSRP review is used as an input to the Range's decision to approve the launch of radioactive material. Portions of MIL-STD-1574A and MIL-STD-882B are used in the systems safety approval by each Range.

Compliance with the technical requirements of the Range Safety Manuals, ESMC and WSMC 127-1, is necessary to obtain Range approval to conduct operations on or from the ranges. The approval process normally includes the Program Offices Preliminary and Critical Design Review processes with interim Technical Interchange Meetings to discuss major safety issues as necessary. To demonstrate compliance with the Range's requirements, an Accident Risk Assessment Report (ARAR) or Missile Systems Prelaunch Safety Package must be provided along with the FTS report, the detailed mission flight plan, and the vehicle performance and breakup data. The Range Safety review and acceptance process is documented and established by the respective Range Safety Manuals, ESMC and WSMC 127-1.

The final decision regarding acceptance of a program on a National Range rests with the Center Commander.

The on-orbit safety approval authority has not been clearly defined by the DOD. At present, the Center Commanders, through their safety staffs, work with individual payload program offices to resolve on-orbit safety issues; with normal approval authority rests with the Secretary of Defense.

8.6 REFERENCES

(1) Eastern Space and Missile Center Regulation (ESMCR) 127-1, "Range Safety," 30 July 1984.

(2) Western Space and Missile Center Regulation (WSMCR) 127-1, "Range Safety Requirements,"1 April 1983.

(3) Military Standard (MIL-STD)-882B, "System Safety Program Requirements," 30 March 1984.

(4) Military Standard (MIL-STD)-1574A, "System Safety Program for Space and Missile Systems," 15 August 1979.

(5) Military Standard (MIL-STD)-1522A, "Standard General Requirements for Safe Design and Operation of Pressurized Space and Missile Systems," 28 May 1984.

(6) Department of Defense Instruction (DOD) 3200.11, "

(7) Space Division Regulation 127-8, "

(8) NASA Handbook (NHB) 1700.7A, "Safety Policy and Requirements for payloads using the Space Transportation System," 9 December 1980.

(9) SAMTO HB-S-100/KHB 1700.7, "Space Transportation System Payload Ground Safety Handbook," 30 November 1984.

(10) JSC 13830A, "Implementation Procedure for STS Payloads System Safety Requirements," 16 May 1983.



THE RANGE SAFETY PROCESS



- CONCEPT

SYSTEM SAFETY

- PROGRAM INTRODUCTION
- SITING
- FLIGHT PLAN ANALYSIS
- DESIGN REVIEWS
- HARDWARE DEVELOPMENT/TEST
- DESTRUCT CRITERIA/DESIGN/TEST
- PROCESS FLOW
- PAD SAFETY PLAN & SOP'S
- PROCEDURES
- TRAINING
- HAZARD TASK MONITORING
- FLIGHT CONTROL
- LAUNCH

T - 5 YEARS | T - 0 | IMPACT ORBIT

Figure 8-1 The Range Safety Process

Chapter 9
Index, Glossary, Conversion Factors

CHAPTER 9
INDEX, GLOSSARY, ACRONYMS, CONVERSION FACTORS

TABLE OF CONTENTS

Section	Title	Page
1.0	Index to SPHAM	9-1
2.0	Glossary of Terms	9-27
3.0	List of SPHAM Acronyms	9-45
4.0	SPHAM Conversion Factors	9-54

CHAPTER 9
INDEX, GLOSSARY, ACRONYMS, CONVERSION FACTORS

1.0 INDEX TO SPHAM

	Page
A.D. Little Tests	5-7
AFT Skirt (SRB)	C1(S)-10
ALGOL IIC Rocket Motors - Scout	C7-7
ALGOL III Rocket Motors - Scout	C7-8
ASE Avionics - PAM-D	C13-2
Abort - Centaur G Prime	C9-10
Abort Operations	
Galileo	C19-25
Ulysses	C19-34
Accident Definitions	3-8
Accident Dynamics	3-11
Accident Risk Assessment Reporting	7-12
Accident Scenarios	
Accident Definitions	3-8
Accident Dynamics	3-11
Analytical	3-14
Development	3-12
Flight Termination Systems	3-4
General	3-1
Liquid Propellants	3-2
Solid Propellants	3-3
Accident/Loss Model	1-3, 1-16
Acoustic Environment Example Data - STS	5-56
Acoustic Post Accident Environments	5-56
Adiabatic Flame Temperature - Fireball	5-35
Aeropass Recovery Orbit - Orbit Transfer Vehicle	C12-27
Air, Compressed	B26-1
Air, Liquid	B26-1
Airborne Hydraulic - Transtage	C14-7
Airborne Support Equipment	
Inertial Upper Stage	C10-9
PAM-D	C13-2
P80-1	C18-2
Aircraft Turbine and Jet Engine Fuel, Thermally Stable	B2-1
Alcohols	B22-1
Alcyone (BE-3-A9) Rocket Motor - Scout	C7-14
Altair II (X258) Rocket Motor - Scout	C7-12
Altair III Rocket Motor - Scout	C7-13
Ammonia, Anhydrous	B3-1
Antares Rocket Motor - Scout	C7-10
Appearance, Material (see specific hazardous material, App. B)	
Argon	B21-1
Ascent Operations - Global Positioning System	C17-12
Ascent Profile - Orbit Transfer Vehicle	C12-25
Asteroid Encounter Option - Galileo	C19-25

Page

Atlas F
Countdown Exercises C3-16
Flight Control System C3-6
General Description C3-1
Launch Complex C3-1
Launch Vehicle C3-14
Missile C3-1
Missile Electrical System C3-11
Missile Explosives C3-12
Missile Flight Safety System (VAFB Only) C3-15
Missile Hydraulic System C3-8
Missile Pneumatic System C3-9
Mission Scenario C3-14
Propellant Utilization System C3-6
Propulsion System C3-3
Re-Entry Vehicle C3-15
Systems Descriptions, Hazardous Materials, Schematics C3-3
Atlas/Centaur
Atlas Stage C4-1, C4-3
Centaur Stage C4-2, C4-7
General Description C4-1
Launch Countdown Automatic Sequence Functions C4-13
Launch Vehicle C4-1
Mission Scenario C4-12
Nonstandard Sequencing C4-16
Systems Descriptions, Hazardous Materials, Schematics C4-3
Atmospheric Dispersion 5-42
Attitude Control
Defense Satellite Communications System C15-9
Defense Systems Program C16-4
P80-1 . . . . . C18-1
Scout C7-5
Transtage C14-6
Ulysses C19-19
Attitude and Articulation Control Subsystem - Galileo C19-6
Autogenous Pressurization System - Titan II C6-12
Auxiliary Power Units - STS/Centaur C1-7
Avionics
Centaur G Prime C9-5
Centaur G Prime C9-7
Inertial Upper Stage C10-7
Titan IV C8-13
Batteries 4-35
Blast (Overpressure) 5-1
Blast
Characteristics of Blasts and Explosions 5-1
Database for Liquid-Propellant Explosions 5-6
Database for Solid-Propellant Explosions 5-18
TNT Equivalent Weights 5-3

Page

Blast Danger Area Controls . . . . . C1(S)-30
Blast Data
A.D. Little Tests 5-7
JSC (Fletcher Analysis) 5-7
Other Investigators 5-7
Pyro Project 5-6
Sandia Laboratories 5-7
Blast Methods
Failure Other than HVI 5-22
Hypergolic Bi-Propellant Systems 5-16
LO2/LH2 Systems 5-9
LO2/RP-1 Systems 5-12
Overpressures and Impulse from Values of Y 5-17
XDT (High Velocity Impact) 5-21
Bromochlordifluoromethane (Halon 1211) B23-1
Bromotrifluoromethane (Halon 1311) B23-1
CPF (Chlorine Pentafluoride) B13-1
CTF (Chlorine Trifluoride) B13-1
Cable Failure Matrix Analysis (CFMA) 6-20
Carbon Dioxide B27-1
Carbon Monoxide B10-1
Carbon Tetrachloride (Tetrachloromethane) B23-1
Case (Propulsion) - PAM-D C13-6
Castor II Rocket Motors - Scout C7-9
Centaur G Prime
Abort Modes C9-10
CISS Avionics System C9-7
Centaur/Spacecraft Weight Summary C9-8
Failure C9-13
Fluid Systems C9-4
General Description C9-1
Integrated Support System Mechanisms C9-7
Mission Scenario C9-9
Mission Event Timeline C9-10
Prelaunch Timeline C9-9
Propulsion and Hydraulic Systems C9-3
Pyrotechnic System C9-8
Reaction Control System C9-4
Secondary Failure C9-14
Structural System C9-1
Support Structure C9-3
Systems Descriptions, Hazardous Materials, Schematics C9-1
Vehicle Avionics C9-5
Centaur Integrated Support System - Centaur G Prime C9-7
Change Analysis 6-2
Chemical Compounds 5-41
Chemical Properties, Material (see specific hazardous material, App. B)
Chlorine B17-1
Chlorine Pentafluoride (CPF) B13-1
Chlorine Trifluoride (CTF) B13-1

	Page
Chloroform (Trichloromethane)	B23-1
Circular Mission - Orbit Transfer Vehicle	C12-26
Command Shutdown and Destruct System - Transtage	C14-9
Command and Data Subsystem - Galileo	C19-6
Common Data Buffer (CDBFR)	C1(S)-27
Common Events - Human Death Rates	4-45
Communications	
Defense Satellite Communications System	C15-5
Defense Systems Program	C16-7
Jovian Probe - Galileo	C19-12
Compatibility (see specific hazardous material, App. B)	
Compliance for Risk	7-1
Component Reliability Data	4-24
Compression Ignition and Turbine Engine Fuel	B2-1
Contingency Analysis	6-3
Core Vehicle - Titan IV	C8-1
Countdown - Atlas F	C3-16
Cradle Structure Assembly - PAM-D	C13-2
Cradle-Mounted Sunshields - PAM-D	C13-11
Cradle-Mounted Thermal Control - PAM-D	C13-11
Credibility Determination	7-7
Critical Incident Technique	6-4
Criticality	7-8
Criticality Analysis	6-5
Criticality Ranking	7-8
DETA (Diethylenetriamine)	B4-1
DSCS II - Defense Satellite Communications System	C15-2
DSCS III - Defense Satellite Communications System	C15-3
Data Analysis	4-9
Decontamination (see specific hazardous material, App. B)	
Defense Satellite Communication Systems	
Attitude Control Subsystem (ACS)	C15-9
Communication Subsystem	C15-5
DSCS II	C15-2
DSCS II Satellite System	C15-12
DSCS II/DSCS III (A-2) on Titan 34D/Transtage	C15-11
DSCS III	C15-3
DSCS III Satellite System	C15-13
Electrical Power and Distribution Subsystem (EPDS)	C15-10
General Description	C15-1
Mission Scenario	C15-12
Propulsion	C15-5
Structure	C15-1
Systems Descriptions, Hazardous Materials, Schematics	C15-1
Thermal Control Subsystem (TCS)	C15-9
Defense Systems Program	
General Description	C16-1
System Descriptions, Hazardous Materials, Schematics	C16-1
Spacecraft Structure Subsystem	C16-1
Propulsion Subsystem	C16-2
Attitude Control Subsystem	C16-4

Page

Defense Systems Program - continued
Electrical Power and Distribution Subsystem C16-4
Thermal Control Subsystem (TCS) C16-5
Communication and Command Subsystem C16-7
Ordnance Subsystem C16-7
Separation Nut (Separation System) C16-8
Shock Reduction C16-8
Pin Puller (Deployment System) C16-8
Mission Scenario C16-8
Delta
Description of Safety Critical Subsystems, Hazardous Materials, Schematics C5-1
Electrical Systems (First Stage) C5-7
Electrical Systems (Second Stage) C5-7
Electrical Systems (Third Stage) C5-8
General Description C5-1
Liquid Propellant Systems (First Stage) C5-1
Liquid Propellant Systems (Second Stage) C5-2
Mission Scenario C5-13
Ordnance Systems (First Stage) C5-12
Ordnance Systems (Second Stage) C5-13
Ordnance Systems (Third Stage) C5-13
Propellant Pressurization Systems (First Stage) C5-8
Propellant Pressurization Systems (Second Stage) C5-10
Pyrogen Igniter Assembly C5-5
Solid-Propellant Systems (First Stage) C5-4
Solid-Propellant Systems (Second Stage) C5-5
Solid-Propellant Systems (Third Stage) C5-5
Third-Stage Solid Propellant Motor Igniter C5-6
Vehicle Hydraulic Systems (First Stage) C5-12
Vehicle Hydraulic Systems (Second Stage) C5-12
Department of Defense (Excluding USAF) 8-2
Department of the Air Force 8-2
Deployment - Defense Systems Program C16-8
Descent Operations - Global Positioning System C17-15
Deuterium B8-1
Diborane B9-1
Dibromodifluoromethane (Halon 1202) B23-1
Dibromotetrafluoroethane (Halon 2402) B23-1
Dichlorodifluoromethane (Freon 12) B23-1
Dichloromonofluoromethane (Freon 21) B23-1
Diethylenetriamine (DETA) B4-1
Difluorochloromethane (Freon 22) B23-1
Display Feedback 4-44
Disposal, Material (see specific hazardous material, App. B)
Earth-Jupiter Operations - Ulysses C19-32
Electrical
Atlas F C3-11
Delta C5-7, C5-7, C5-8

	Page
Electrical Inhibits - Galileo	C19-13
Electrical Power	
Defense Satellite Communications System	C15-10
Defense Systems Program	C16-4
Galileo	C19-7
Jovian Probe - Galileo	C19-13
Orbit Transfer Vehicle	C12-11
P80-1	C18-1
PAM-D	C13-3
STS/Centaur	C1-7
Titan II	C6-13
Ulysses	C19-19
Electrical Subsystem Failures	6-66
Emergency Equipment, Material (see specific hazardous material, App. B)	
Energy Analysis	6-6
Environmental Effects, Material (see specific hazardous material, App. B)	
Equipment Cleaning (see specific hazardous material, App. B)	
Equipment Compatibility (see specific hazardous material, App. B)	
Ethyl Alcohol	B22-1
Ethylene	B2-1
Ethylene Oxide	B6-1
Event Probabilities in Risk Assessment	4-1
Event Tree	6-20
Explosion Hazards, Material (see specific hazardous material, App. B)	
Exposure Limits, Material (see specific hazardous material, App. B)	
External Tank Systems - STS/Centaur	C1-7
FLOX (Fluorine Mixtures	B12-1
Failure Modes & Effects Analysis (FMEA)	6-21
Failure Other than HVI	5-22
Failures - Centaur G Prime	C9-13
Fault-Tree Analysis	6-23
Fault-Tree Scenarios	4-14
Fire and Combustion Product Hazards, Material (see specific hazardous material, App. B)	
Fireball Development Time-History	5-30
Fireball Duration	5-32
Fireball Size	5-31
Fireball Size and Duration - Liquid	5-31
Fireball Thermal Effects	5-35
Firefighting (see specific hazardous material, App. B)	
First Aid (see specific hazardous material, App. B)	
Flammability - Galileo	C19-16
Fletcher Analysis	5-7
Flight Control	
Atlas F	C3-6
Titan 34D	C2-16
Titan II	C6-15
Titan IV	C8-12

Page

Flight Operations Support - Orbit Transfer Vehicle C12-11
Flight Termination Systems . . . . . 3-4, C1(S)-25
Flight Termination System
  Atlas F C3-15
  Inertial Upper Stage C10-10
  STS/Centaur C1-13
  Scout C7-2
  Titan 34D C2-14
  Transtage C14-7
Flow Analysis. 6-7
Fluorine B12-1
Fluorine Mixtures (FLOX) B12-1
Forward Skirt (SRB) . . . . . C1(S)-10
Fragmentation 5-24
Fragmentation
  Pressurized Tanks and General Applications 5-27
  Propellant Tanks 5-26
  SRM 5-24
Freon 11 (Trichlorofluoromethane) B23-1
Freon 113 (Trichlorotrifluoroethane) B23-1
Freon 12 (Dichlorodifluoromethane) B23-1
Freon 21 (Dichloromonofluoromethane) B23-1
Freon 22 (Difluorochloromethane) B23-1
Frustum (SRB) . . . . . C1(S)-10
Fuming Nitric Acids, Type IIIB and IV B15-1
Furfuryl Alcohol B22-1
GEO Delivery Vehicle - Orbit Transfer Vehicle C12-5
Galileo
  Abort Operations C19-25
  Asteroid Encounter Option C19-25
  Attitude and Articulation Control Subsystem C19-6
  Command and Data Subsystem C19-6
  Communications Subsystem C19-12
  Electrical Inhibits C19-13
  Electrical Power Subsystem C19-13
  Flammability C19-16
  General Description C19-1
  Jovian Atmospheric Entry Probe C19-9
  Jovian System Exploration C19-25
  Launch to Jupiter Arrival C19-21
  Mission Functions C19-27
  Mission Phases C19-20
  Mission Scenario C19-20
  Nuclear and Electromagnetic Radiation C19-17
  Orbiter Communications Subsystem C19-6
  Post-Separation to Jupiter Arrival C19-24
  Power Subsystem (RTG) C19-7
  Pyrotechnic Subsystem C19-8, C19-12
  RTG Cooling C19-15

Page

Galileo - continued
RTG Shorting C19-15
Retropropulsion Module (RPM) C19-9
Safety Design Features C19-13
Separation (From Shuttle and Centaur) C19-22
Structural Safety Fractures C19-16
Structure Subsystem C19-10
Systems Descriptions, Hazardous Materials, Schematics C19-2, C19-17

General Description
Atlas F C3-1
Atlas/Centaur C4-1
Centaur G Prime C9-1
Defense Satellite Communications System C15-1
Defense Systems Program C16-1
Delta C5-1
Galileo C19-1
Global Positioning System C17-1
Inertial Upper Stage C10-1
Orbit Transfer Vehicle C12-1
P80-1 . . . . . C18-1
PAM-D C13-1
STS/Centaur C1-1
STS/IUS . . . . . C1(S)-1
Scout C7-1
Titan 34D C2-1
Titan II C6-1
Titan IV C8-1
Transtage C14-1
Ulysses C19-1
Geostationary Missions - Titan IV. C8-33
Global Burst Detector - Global Positioning System C17-10
Global Positioning System
Ascent Operations Phase C17-12
Descent Phase C17-15
General Description C17-1
Global Burst Detector C17-10
Hazardous Voltage Sources C17-11
Ignition of Flammable Atmospheres C17-10
Ignition of Flammable Materials C17-10
Integrated Transfer Subsystem C17-2
Interface Configuration C17-9
Interface Control Drawings C17-9
Interface Description C17-9
Ionizing Radiation Data C17-2
L-Band Subsystem (LBS) C17-2
Mission Phases C17-12
Mission Scenario C17-11
On-Orbit Storage Operations Phase C17-16
Operational Phase C17-14
Orbit Insertion Phase C17-14

Page

Global Positioning System - continued
Orbit Operations Phase C17-14
Ordnance C17-11
Parking Orbit Operations Phase C17-13
Post-Landing Operations Phase C17-15
Preflight Operation C17-12
Production Space Vehicle Processing C17-12
Propulsion C17-7
Radiation, Ionizing/Non-Ionizing C17-10
Radioactive Sources C17-6
Radiological Safety Data C17-4
Reaction Control Subsystem C17-8
Special Range Safety Considerations C17-5
Systems Description, Hazardous Materials, Schematics C17-2
Telemetry, Tracking, and Command C17-2
Toxic Materials C17-11
Transfer Orbit Operations Phase C17-13
Venting of Sealed or Unsealed Components C17-10
Ground Operations Aerospace Language . . . . . C1(S)-28
Ground Processing - Orbit Transfer Vehicle C12-10
Ground Range Safety Systems (RSS) . . . . . C1(S)-24
Ground to Space - Orbit Transfer Vehicle C12-13
Guidance - Titan 34D C2-13
Guidance and Control System - Scout C7-20
Halogen Fluorides B13-1
Halon 1202 (Dibromodifluoromethane) B23-1
Halon 1211 (Bromochlorodifluoromethane) B23-1
Halon 1301 (Bromotrifluoromethane) B23-1
Halon 2402 (Dibromotetrafluoroethane) B23-1
Handling, Material (see specific hazardous material, App. B)
Hazard Analysis
Conceptual Phase 2-35
Manufacture/Test Phase 2-38
Project Interfaces 2-32
System Definition Phase 2-36
System Development Phase 2-37
System Use Phase 2-39
Hazard Analysis Documentation Instructions 2-18
Hazard Analysis Report
Documentation 2-29
Identifying/Classifying/Describing Hazards 2-30
Identifying/Potential Causes 2-30
Propose/Track Controls 2-31
Verifying/Finalizing Controls 2-31
Hazard Analysis Sheet - Documentation. 2-18
Hazard Catalog - Documentation 2-28
Hazard Reports - Generic 6-72
Hazardous Materials - Transtage C14-9
Hazardous Subsystem Methods
Electrical Subsystem Failures 6-66
Integrated Hazard Analysis 6-43

Page

Hazardous Subsystem Methods - continued
Interface Hazard Analysis 6-52
Ionizing Radiation Failures 6-63
Mechanism Failures 6-55
Operating Hazard Analysis 6-51
Ordnance Failures 6-57
Pressure Subsystem Failure 6-61
Propulsion Subsystem Failures 6-59
RF Subsystem Failures 6-65
Structural Failures 6-53
System (Design) Hazard Analysis 6-39
Hazardous Voltage Sources - Global Positioning System C17-11
Hazards - Generic 6-71
Hazards Analyses
Approach 2-5
Implementation 2-1
Objectives 2-3
Process 2-2
Responsibilities 2-4
Hazards Analysis Approval
Department of Defense (Excluding USAF) 8-2
Department of the Air Force 8-2
Interagency Nuclear Safety Review Panel (INSRP) 8-3
National Aeronautics and Space Administration 8-4
National Range 8-4
Hazards Analysis Methods
Analytical 6-1
Cable Failure Matrix Analysis (CFMA) 6-20
Change Analysis 6-2
Contingency Analysis 6-3
Critical Incident Technique 6-4
Criticality Analysis. 6-5
Electrical 6-66
Energy Analysis 6-6
Event Tree 6-20
Failure Modes & Effects Analysis (FMEA) 6-21
Fault-Tree Analysis 6-23
Flow Analysis 6-7
Hazardous Subsystem 6-36
Integrated Hazard Analysis 6-43
Interface Analysis/System Hazard Analysis 6-8
Interface Hazard Analysis 6-52
Ionizing Radiation 6-63
Job Safety Analysis 6-9
Management Oversight and Risk Tree Analysis 6-24
Maximum Credible Accident/Worst Case Condition 6-10
Mechanism 6-55
Methodology Source Matrix 6-34
Naked Man 6-11
Network Logic Analysis. 6-26
Operating Hazard Analysis/Procedure Analysis 6-11

Page

Hazards Analysis Methods - continued
Operating Hazard Analysis 6-51
Ordnance 6-57
Pin Fault/Pin Short Analysis 6-27
Preliminary Hazard Analysis 6-12
Pressure 6-61
Propulsion 6-59
Prototype 6-13
Qualitative 6-2
Quantitative 6-20
RF 6-65
Scenario 6-14
Sneak Circuit Analysis 6-28
Software Safety Analysis 6-14
Statistical 6-30
Structural 6-53
Subsystem Hazard Analysis 6-17
System (Design) Hazard Analysis 6-39
Systematic Inspection 6-18
Hazards Analysis Program Elements 1-6
Health Hazards, Material (see specific hazardous material, App. B)
Heat Flux - Fireball 5-35
Helium B21-1
Human Actions - Coupling 4-42
Human Engineering of Controls and Displays 4-40
Human Reliability
Coupling of Human Actions 4-42
Level of Presumed Psychological Stress 4-40
Personnel Redundancy 4-44
Presence and Quality of Written Instructions 4-41
Quality of Human Engineering of Controls and Displays 4-40
Quality of Training and Practice 4-41
Type of Display Feedback 4-44
Human Reliability Data 4-36
Hydraulic Fluids B24-1
Hydraulics
Atlas F C3-8
Delta C5-12
STS/Centaur C1-7
Scout C7-4
Titan 34D C2-12
Titan II C6-13
Hydraulics Failures - Centaur G Prime C9-14
Hydrazine B4-1
Hydrazine Fuels B4-1
Hydrocarbon Fuels B2-1
Hydrogen B8-1
Hydrogen Peroxide B19-1
Hypergolic Bi-Propellant Systems 5-16
IAPS Mercury Tanks - P80-1 . . . . . C18-3
IAPS System Configuration - P80-1 . . . . . C18-3

	Page
IKS75 Spin Rocket Motor - Scout	C7-16
ION Auxiliary Propulsion System - P80-1	C18-2
Ignition System - Scout	C7-2
Ignition of Flammable Atmospheres - Global Positioning System	C17-10
Ignition of Flammable Materials - Global Positioning System	C17-10
Impact Limit Line Controls	C1(S)-30
Inadvertent Separation Destruct System - Transtage	C14-9
Inclined Missions - Titan IV	C8-33
Inertial Guidance - Transtage	C14-6
Inertial Upper Stage	
Airborne Support Equipment (ASE)	C10-9
Avionics Module	C10-7
General Description	C10-1
Mission Scenario	C10-10
Propulsion Module	C10-1
Propulsion System	C10-1
Reaction Control System (RCS)	C10-5
Structures and Mechanisms	C10-10
Systems Descriptions, Hazardous Materials, Schematics	C10-1
T34D/IUS Flight Termination System	C10-10
Initiator Assembly (Propulsion) - PAM-D	C13-8
Instrumentation	4-35
Insulation (Propulsion) - PAM-D	C13-7
Integrated Hazard Analysis	6-43
Integrated Transfer Subsystem - Global Positioning System	C17-2
Interagency Nuclear Safety Review Panel (INSRP)	8-3
Interface Analysis/System Hazard Analysis	6-8
Interface Configuration - Global Positioning System	C17-9
Interface Control Drawings - Global Positioning System	C17-9
Interface Descriptions - Global Positioning System	C17-9
Interface Hazard Analysis	2-14, 6-52
Interfaces (Propulsion) - PAM-D	C13-6
Investigators (Genera)	5-7
Iodine	B16-1
Ionizing Radiation - Global Positioning System	C17-2
Ionizing Radiation Failures	6-63
Isopropyl Alcohol	B22-1
Jet Fuel, Grade JP-10	B2-1
Jet Fuel, Grade JP-4 (Turbine Fuel, Aviation)	B2-1
Jet Fuel, Grade JP-5 (Turbine Fuel, Aviation)	B2-1
Jet Fuel, Grade JP-6	B2-1
Jet Fuel, Grade JP-7	B2-1
Jet Fuel, Grade JP-8	B2-1
Jet Fuel, Grade JP-9	B2-1
Jet Fuel, Grades I and II (Referee)	B2-1
Job Safety Analysis	6-9
Jovian Atmospheric Entry Probe - Galileo	C19-9, C19-27
Jovian System Exploration - Galileo	C19-25
Jupiter Flyby Operations - Ulysses	C19-33

	Page
KSC Launch Site	C1(S)-16
Krypton	B21-1
L-Band - Global Positioning System	C17-2
LO2/LH2 Systems	5-9
LO2/RP-1 Systems	5-12
LOX (Liquid Oxygen)	B11-1
Launch Complex - Atlas F	C3-1
Launch Countdown Automatic Sequence Functions - Atlas/Centaur	C4-13
Launch Operations	
Orbit Transfer Vehicle	C12-10
Titan II	C6-18
Launch Processing System	C1(S)-26
Launch Propellant Loading Cleared Area	C1(S)-30
Launch and Injection Operations - Ulysses	C19-30
Launch to Jupiter Arrival - Galileo	C19-21
Launch/Landing Site Safety	C1(S)-26
Lifetime Released Chemicals	5-41
Liquid Propellant Blast Determination Methods	5-9
Liquid Propellant Tank Fragmentation	5-26
Liquid Propellants in Accident Scenarios	3-2
Liquid Rocket Engines - Titan 34D	C2-9, C2-11
Liquid-Propellant Explosions	5-6
Loads - Titan IV	C8-4
Lunar Missions - Orbit Transfer Vehicle	C12-22, C12-26
MAF-1,3,4 (Mixed Amine Fuels)	B4-1
MARC-4 Spin Rocket Motor - Scout	C7-16
MMH (Monomethylhydrazine)	B4-1
MON-1,3,10,25 (Mixed Oxides of Nitrogen)	B14-1
MPS - General System Overview	6-36
Main Engines	C1(S)-13
Management Oversight and Risk Tree Analysis	6-24
Mass Properties - Titan IV	C8-29
Material Compatibility (see specific hazardous material, App. B)	
Maximum Credible Accident/Worst Case Condition	6-10
Mechanical Systems - STS/Centaur	C1-7
Mechanism Failures	6-55
Mechanisms - Ulysses	C19-18
Mercury	B25-1
Mercury Information - P80-1	C18-4
Meteorological Systems	C1(S)-29
Methane	B2-1
Methodology Source Matrix	6-34
Methyl Alcohol	B22-1
Methylene Chloride (Dichloromethane)	B23-1
Mishap Cost Assessment	7-11
Mishap Probability in Risk Assessment	7-3
Mishap Risk Controls	7-11
Mishap Severity in Risk Assessment	7-2
Missile Guidance Set - Titan II	C6-15

	Page
Mission Capability - Titan IV	C8-34
Mission Event Timeline - Centaur G Prime	C9-10
Mission Functions - Galileo	C19-27
Mission Phases	
Galileo	C19-20
Global Positioning System	C17-12
Mission Scenario	
Atlas F	C3-14
Atlas/Centaur	C4-12
Centaur G Prime	C9-9
Defense Satellite Communications System	C15-12
Defense Systems Program	C16-8
Delta	C5-13
Galileo	C19-20
Global Positioning System	C17-11
Inertial Upper Stage	C10-10
Orbit Transfer Vehicle	C12-15
Orbit Transfer Vehicle	C12-23
Orbit Transfer Vehicle	C12-24
P80-1	C18-6
PAM-D	C13-12
STS/Centaur	C1-14
Scout	C7-20
Titan 34D	C2-15
Titan II	C6-16
Titan IV	C8-32
Transtage	C14-11
Ulysses	C19-28
Mission Summary - Ulysses	C19-33
Mission and Performance Requirements - Titan 34D	C2-16
Mixed Amine Fuels (MAF-1,3,4)	B4-1
Monomethylhydrazine (MMH)	B4-1
Motors	4-34
Multipurpose, Fuel Antarctic MP-1	B2-1
NSTS Payload Hazards (Example Analysis, Reports)	6-70
NTO	B14-1
Naked Man	6-11
National Aeronautics and Space Administration	8-4
National Range	8-4
Near-Earth Operations - Ulysses	C19-32
Neon, Liquid	B21-1
Network Logic Analysis	6-26
Nitrogen Oxides	B14-1
Nitrogen Tetroxide	B14-1
Nitrogen Trifluoride	B18-1
Nitrogen, Gaseous	B20-1
Nitrogen, Liquid	B20-1
Nitromethane	B5-1
Nitrous Oxide	B28-1
Noble Gases	B21-1
Nominal Mission - Ulysses	C19-30

Page

Noncompliance Items in Risk Assessment 7-2
Nonstandard Sequencing - Atlas/Centaur C4-16
Nose Cap (SRB) . . . . . C1(S)-11
Nozzle - PAM-D C13-7
Nuclear and Electromagnetic Radiation - Galileo C19-17
Operating Hazard Analysis/Procedure Analysis 6-11
Operating Hazard Analysis 6-51
Operating and Support Hazard Analysis 2-15
Operation Cycle . . . . . C1(S)-11
Operation Cycles - STS/Centaur C1-14
Orbit Insertion Operations - Global Positioning System C17-14
Orbit Operations Operations - Global Positioning System C17-14
Orbit Transfer Vehicle
  Ascent Profile C12-25
  Avionics and Power Equipment-Cryo Stages C12-11
  Cryo Configuration Summary C12-15
  Deorbit, Aeropass, and Recovery Orbit C12-27
  Flight Operations Support C12-11
  GEO/HEO Delivery Capability-Ground Based Cryo C12-19
  General Description C12-1
  Ground Based 12-Hour Circular Mission C12-26
  Ground Based Planetary Mission C12-25
  Ground to Space Evolution-Storage OTV C12-13
  Ground-Based ACC-Storable C12-3
  Ground-Based Cryo C12-1
  Ground-Based Mission C12-23
  Ground-Based P/L-Bay-Storable C12-3
  Ground-Based-ACC/P/L Bay Storable Performance C12-20
  Growth Space-Based Cryo C12-2
  HEO Capability-53K/90K Space Based Srotable C12-21
  Initial Space-Based Cryo C12-2
  Launch Operations C12-10
  Lunar Missions C12-26
  Lunar Missions with Storable C12-22
  Manned GEO/HEO Sortie Capability-Growth Space-Based Cryo C12-19
  Manned/Unmanned Servicing Mission C12-26
  Mission Scenario C12-15
  OTV/Orbitor Trajectory Plot C12-25
  Planetary Missions With Storable C12-21
  Propulsion System Equipment-Cryo Stages C12-13
  Space Based Ground Processing C12-10
  Space Based Planetary Mission C12-26
  Space-Based Manned Servicing C12-10
  Space-Based Mission C12-24
  Space-Based Unmanned Servicing C12-5
  Space-Based-GEO Delivery C12-5
  Storage Configuration Summary C12-20
  Systems Descriptions, Hazardous Materials, Schematics C12-11
Orbital Maneuvering System - STS/Centaur C1-2
Orbital Manuevering Subsystem Engines . . . . . C1(S)-14
Orbiter Communications Subsystem - Galileo C19-6

	Page
Orbiter Interfaces - PAM-D	C13-4
Orbiter Safety - STS/Centaur	C1-19
Orbiter Structure - STS/Centaur	C1-1
Orbiter Subsystems - STS/Centaur	C1-1
Ordnance Failures	6-57
Ordnance Ring (SRB)	C1(S)-10
Otto Fuel II	B7-1
Out-of-Ecliptic Operations - Ulysses	C19-33
Overpressures and Impulse from Values of Y	5-17
Oxygen, Liquid (LOX)	B11-1
P80-1 Space Vehicle	
Airborne Support Equipment	C18-2
Attitude Control and Determination Subsystem	C18-1
Electrical Power Subsystem	C18-1
General Description	C18-1
IAPS System Configuration	C18-3
IAPS Mercury Tanks	C18-3
ION Auxiliary Propulsion System	C18-2
Mission Scenario	C18-6
Propulsion Subsystems	C18-1
Reaction Control System (Hydrazine)	C18-1
Reaction Control System (Cold Gas)	C18-1
Structures	C18-1
Systems Descriptions, Hazardous Materials, Schematics	C18-1
Telemetry, Tracking, and Command Subsystem	C18-2
Thermal Control Subsystem	C18-2
PAM Spintable Spring Separation System - PAM-D	C13-5
PAM/D	
ASE Avionics	C13-2
Airborne Support Equipment (ASE)	C13-2
Case (Propulsion)	C13-6
Cradle Structure Assembly	C13-2
Cradle-Mounted Sunshields	C13-11
Cradle-Mounted Thermal Control System (CTCS)	C13-11
Electrical System Description	C13-3
Expendable Vehicle	C13-1
General Description	C13-1
Initiator Assembly (Propulsion)	C13-8
Insulation (Propulsion)	C13-7
Interfaces (Propulsion)	C13-6
Mechanical Subsystem	C13-4
Mission Scenario	C13-12
Nozzle	C13-7
PAM Spintable Spring Separation System	C13-5
PAM/Orbiter Interface	C13-4
Payload Attach Fitting (PAF)	C13-1
Payload Restraint Mechanism	C13-5
Propellant Grain	C13-7
Propellant and Liner	C13-7
Propulsion Subsystem	C13-5
Pyrotechnics Subsystem	C13-8

Page

PAM/D - continued
Safe and Arm Device, P/N E29609 . . . . . C13-8
Solid Rocket Motor (SRM) C13-1
Spin Drive, Brake, and Index C13-4
Spintable Assembly C13-2
Spintable Clamp Band C13-5
Structures Subsystem C13-11
System Descriptions, Hazardous Materials, Schematics C13-3
TBI and ETA (Propulsion) C13-8
Thermal Control System C13-11
Pad Environmental Control System (ECS) GN_2 Subsystem . . . . . C1(S)-29
Parking Orbit Operations - Global Positioning System C17-13
Payload Attach Fitting (PAF) - PAM-D C13-1
Payload Environments - Titan IV. C8-27
Payload Fairing (PLF) - Titan IV C8-27
Payload Interfaces - Titan IV. C8-28
Payload Restraint Mechanism - PAM-D C13-5
Pentaborane B9-1
Perchloroethylene (Tetrachloroethylene) B23-1
Performance - Titan IV C8-32
Personnel Redundancy 4-45
Physical Properties, Material (see specific hazardous material, App. B)
Pin Fault/Pin Short Analysis 6-27
Pipe Testing 4-34
Planetary Missions - Orbit Transfer Vehicle C12-21, C12-25, C12-26
Pneumatics - Atlas F C3-9
Post-Landing Operations - Global Positioning System C17-15
Post-Separation to Jupiter Arrival - Galileo C19-24
Preflight Operation - Global Positioning System C17-12
Prelaunch Timeline - Centaur G Prime C9-9
Preliminary Hazard Analysis 6-12
Preliminary Hazards Analysis - PHA 2-6
Pressure Cartridge - Transtage C14-11
Pressure Subsystem Failure 6-61
Pressure Tanks - STS/Centaur C1-3
Pressure Tanks . . . . . C1(S)-15
Pressurized Tanks and General Applications 5-27
Probabilities
Common Events - Human Death Rates 4-45
Data Analysis 4-9
Event Probabilities in Risk Assessment 4-1
Program 624A 4-15
STS Failure Probabilites 4-19
Scenario Event Probability Models 4-3
Scenario Event Probability Modeling Process 4-4
Scenario Probability Modeling 4-13
System Failure Probability Methods 4-2
Processed Data Recorder/Shared Peripheral Area . . . . . C1(S)-28

	Page
Production Space Vehicle Processing - Global Positioning System	C17-12
Program 624A	4-15
Propellant - Titan II	C6-4
Propellant Feed - Titan 34D	C2-8, C2-11
Propellant Grain - PAM-D	C13-7
Propellant Pressurization - Delta	C5-8, C5-10
Propellant Safety - Titan II	C6-6
Propellant Tanks - Transtage	C14-2
Propellant Utilization - Atlas F	C3-6
Propellant and Liner - PAM-D	C13-7
Properties, Material (see specific hazardous material, App. B)	
Propulsion	C1(S)-13
Propulsion	
Atlas F	C3-3
Centaur G Prime	C9-3
Defense Satellite Communications System	C15-5
Defense Systems Program	C16-2
Delta	C5-1, C5-2, C5-4, C5-5, C5-5, C5-6
Global Positioning System	C17-7
Inertial Upper Stage	C10-1
Orbit Transfer Vehicle	C12-13
P80-1	C18-1
PAM-D	C13-5
STS/Centaur	C1-2
Titan II	C6-2
Titan IV	C8-10
Propulsion Subsystem Failures	6-59
Protective Measures, Material (see specific hazardous material, App. B)	
Prototype	6-13
Psychological Stress	4-40
Pumps	4-32
Pyro Project	5-6
Pyrotechnics	
Atlas F	C3-12
Centaur G Prime	C9-8
Defense Systems Program	C16-7
Delta	C5-5, C5-12, C5-13
Galileo	C19-8
Global Positioning System	C17-11
Jovian Probe - Galileo	C19-12
PAM-D	C13-8

Page

Pyrotechnics - continued
Scout C7-17
Titan 34D C2-14
Titan II C6-14
Transtage C14-10
Ulysses C19-19
RCRA Classification (see specific hazardous material, App. B)
RF Subsystem Failures 6-65
RTG Cooling - Galileo C19-15
RTG Shorting - Galileo C19-15
Radiation, Ionizing/Non-Ionizing - Global Positioning System C17-10
Radioactive Sources - Global Positioning System C17-6
Radiological Safety - Global Positioning System C17-4
Ramjet Engine Fuel, Grade RJ-1 . . . . . B2-1
Ramjet Engine Fuel, Grade RJ-4 . . . . . B2-1
Ramjet Engine Fuel, Grade RJ-5 . . . . . B2-1
Range Safety . . . . . C1(S)-24
Range Safety
Global Positioning System C17-5
STS/Centaur C1-13
Reaction Control - Global Positioning System C17-8
Reaction Control System . . . . . C1(S)-16
Reaction Control System
Centaur G Prime C9-4
Inertial Upper Stage C10-5
Scout C7-2
Reaction Control System (RCS) - STS/Centaur C1-3
Reaction Control System (Hydrazine) - P80-1 . . . . . C18-1
Reaction Control System (Cold Gas) - P80-1 . . . . . C18-1
Ready Storage (see specific hazardous material, App. B)
Relays 4-34
Reliability
Batteries 4-35
Human 4-36
Instrumentation 4-35
Motors 4-34
Pipe Testing 4-34
Pumps 4-32
Relays 4-34
Solid State Devices 4-35
Switches 4-35
Valves 4-33
Wires and Terminal Boards 4-36
Reliability Data 4-24
Requirements in Risk Assessment. 7-1
Retro Rockets - Titan 34D C2-12
Retropropulsion Module (RPM) - Galileo C19-9
Risk Assessment
Compliance Items 7-1
Conformance to Program Requirements 7-1
Cost Assessment 7-11

Page

Risk Assessment - continued
- Credibility Determination 7-7
- Credible Failures 7-7
- Criticality 7-8
- Criticality Ranking 7-8
- Mishap Severity 7-2
- Mishap Probability 7-3
- Non-Credible Failures 7-7
- Noncompliance Items 7-2
- Reporting 7-12
- Risk Controls 7-11
- Risk Factors 7-1

Risk Factors 7-1
Rocket Fuel, RP-1 (Propellant, Kerosene) B2-1
Rocket Motors - Scout C7-6
SPHAM Purpose 1-2
SPHAM Scope 1-2
SPHAM Summary 1-9
SPHAM User Guide 1-3, 1-15
SRBs . . . . . C1(S)-14
STS Acoustic Environment Example Data 5-56
STS Failure Probabilites 4-19
Safe and Arm Device, P/N E29609 - PAM-D C13-8
Safety Design Features - Galileo C19-13
Safety Measures, Material (see specific hazardous material, App. B)
Safety Plans . . . . . C1(S)-24
Safety Precautions, Material (see specific hazardous material, App. B)
Safing Procedures - Titan II C6-10
Sandia Laboratories 5-7
Scenario Analysis 6-14
Scenario Event Probability Models 4-3
Scenario Event Probability Modeling Process 4-4
Scenario Probability Modeling 4-13
Scout
- ALGOL IIC Rocket Motor C7-7
- ALGOL III Rocket Motor C7-8
- Alcyone (BE-3-A9) Rocket Motor C7-14
- Altair II (X258) Rocket Motor C7-12
- Altair III Rocket Motor C7-13
- Antares Rocket Motor C7-10
- Attitude Control System C7-5
- Castor II Rocket Motor C7-9
- Destruct System C7-2
- Explosive Device C7-17
- General Description C7-1
- Guidance and Control System C7-20
- Hydraulic Control System C7-4
- IKS75 Spin Rocket Motor C7-16
- Ignition System C7-2
- MARC-4 Spin Rocket Motor C7-16

Page

Scout - continued
Mission Scenario C7-20
Payload Separation System C7-5
Reaction Control System C7-2
Rocket Motors C7-6
Systems Descriptions, Hazardous Materials, Schematics C7-2
Separation
Defense Systems Program C16-8
Galileo C19-22
Scout C7-5
Separation (ET/Orbiter) - STS/Centaur C1-12
Separation (SRM/ET) - STS/Centaur C1-12
Separation SRB/ET and ET/Orbiter . . . . . C1(S)-14
Servicing Missions - Orbit Transfer Vehicle C12-26
Servicing Vehicle (Unmanned) - Orbit Transfer Vehicle C12-5, C12-10
Shock Reduction - Defense Systems Program C16-8
Sneak Circuit Analysis 6-28
Software - Titan IV C8-16
Software Safety Analysis 6-14
Solid Propellant Fireball Size and Duration - Solids 5-33
Solid Propellants in Accident Scenarios 3-3
Solid Rocket Motor . . . . . C1(S)-9
Solid Rocket Motor
A Case Study 4-6
PAM-D C13-1
STS/Centaur C1-9
Titan 34D C2-2
Titan IV C8-2, C8-5
Solid Rocket Motor Fragmentation 5-24
Solid State Devices 4-35
Solid-Propellant Blast Determination Methods 5-19
Solid-Propellant Explosions 5-18
Sound Suppression Water System . . . . . C1(S)-28
Space Transportation System/Centaur
Auxiliary Power Units (APU) C1-7
Command Destruct System C1-13
ET/Orbiter Separation C1-12
Electrical Power C1-7
External Tank C1-7
General Description C1-1
Hydraulic C1-7
Main Propulsion System C1-2
Mechanical Systems C1-7
Mission Scenario C1-14
Operation Cycle C1-14
Orbital Maneuvering System C1-2
Orbiter Safety C1-19
Orbiter Structure C1-1
Orbiter Subsystems C1-1

Page

Space Transportation System/Centaur - continued
Pressure Tanks C1-3
Range Safety C1-13
Reaction Control System (RCS) C1-3
SRM/ET Separation C1-12
Solid Rocket Motors (SRM) C1-9
Systems Descriptions, Hazardous Materials, Schematics C1-1
Thermal Control System (TCS) C1-2
Thermal Protection System (TPS) C1-2
Space Transportation System/IUS
General Description . . . . . C1(S)-1
Subsystems . . . . . C1(S)-2
Structures . . . . . C1(S)-6
Orbiter Structure . . . . . C1(S)-6
External Tank Structure . . . . . C1(S)-8
SRB Structure . . . . . C1(S)-9
Forward Skirt (SRB) . . . . . C1(S)-10
Ordnance Ring (SRB) . . . . . C1(S)-10
Frustum (SRB) . . . . . C1(S)-10
Nose Cap (SRB) . . . . . C1(S)-11
Systems Tunnel (SRB) . . . . . C1(S)-11
Operation Cycle . . . . . C1(S)-11
Propulsion . . . . . C1(S)-13
Main Engines . . . . . C1(S)-13
SRBs . . . . . C1(S)-14
Orbital Manuevering Subsystem Engines . . . . . C1(S)-14
Separation . . . . . C1(S)-14
Pressure Tanks . . . . . C1(S)-15
Orbiter Reaction Control Subsystem . . . . . C1(S)-16
KSC Launch Site . . . . . C1(S)-16
Safety Plans . . . . . C1(S)-24
Range Safety . . . . . C1(S)-24
Ground Range Safety Systems (RSS) . . . . . C1(S)-24
Flight Vehicle Range Safety Systems . . . . . C1(S)-25
Launch/Landing Site Safety . . . . . C1(S)-26
Launch Processing System . . . . . C1(S)-26
Subsystem Operator Consoles . . . . . C1(S)-26
Common Data Buffer (CDBFR) . . . . . C1(S)-27
Processed Data Recorder/Shared Peripheral Area . . . . . C1(S)-28
Ground Operations Aerospace Language . . . . . C1(S)-28
Sound Suppression Water System . . . . . C1(S)-28
Pad Environmental Control System (ECS) GN_2 Subsystem . . . . . C1(S)-29
Meteorological Systems . . . . . C1(S)-29
Launch Propellant Loading Cleared Area . . . . . C1(S)-30
Blast Danger Area Controls . . . . . C1(S)-30
Impact Limit Line Controls . . . . . C1(S)-30
Spin Drive, Brake, and Index - PAM-D C13-4
Spintable Assembly - PAM-D C13-2
Spintable Clamp Band - PAM-D C13-5
Statistical 6-30
Storage - Orbit Transfer Vehicle C12-20

Page

Storage Operations - Global Positioning System C17-16
Structural Failures 6-53
Structural Safety - Galileo C19-16
Structure (ET) . . . . . C1(S)-8
Structure (Orbiter) . . . . . C1(S)-6
Structure (SRB) . . . . . C1(S)-9
Structures . . . . . C1(S)-6
Structures
  Centaur G Prime C9-1
  Defense Satellite Communications System C15-1
  Defense Systems Program C16-1
  Inertial Upper Stage C10-10
  Jovian Probe - Galileo C19-10
  P80-1 . . . . . C18-1
  PAM-D C13-11
  Titan II C6-2
  Titan IV C8-10
  Ulysses C19-18
Subsystem Hazard Analysis 2-9, 6-17
Subsystem Operator Consoles . . . . . C1(S)-26
Subsystems . . . . . C1(S)-2
Switches 4-35
System (Design) Hazard Analysis 6-39
System Descriptions, Hazardous Materials, Schematics
  Atlas F C3-3
  Atlas/Centaur C4-3
  Centaur G Prime C9-1
  Defense Satellite Communications System C15-1
  Defense Systems Program C16-1
  Delta C5-1
  Galileo C19-2
  Global Positioning System C17-2
  Inertial Upper Stage C10-1
  Orbit Transfer Vehicle C12-11
  P80-1 . . . . . C18-1
  PAM-D C13-3
  STS/Centaur C1-1
  Scout C7-2
  Titan 34D C2-1
  Titan II C6-2
  Titan IV C8-5
  Transtage C14-1
  Ulysses C19-17
System Failure Probability Methods 4-2
System Hazard Analysis 2-10
System Safety Checklist 2-8
System Safety Checklist - Documentation. 2-21
Systematic Inspection 6-18
Systems Tunnel (SRB) . . . . . C1(S)-11
TNT Equivalent Weights 5-3

Page

Telemetry, Tracking, and Command
Global Positioning System C17-2
P80-1 . . . . . C18-2
Thermal Control
Defense Satellite Communications System C15-9
Defense Syster Program C16-5
P80-1 . . . . . C18-2
PAM-D C13-11
Ulysses C19-18
Thermal Control System - STS/Centaur C1-2
Thermal Post Accident Environment 5-30
Thermal Properties, Material (see specific hazardous material, App. B)
Thermal Protection System - STS/Centaur C1-2
Titan 34D
Airborne Hydraulic Systems C2-12
Flight Control System Operation C2-16
Flight Termination System C2-14
General Description C2-1
Inertial Guidance System C2-13
Introduction C2-1
Mission Scenario C2-15
Mission and Performance Requirements C2-16
Ordnance Items C2-14
Propellant Feed System C2-8, C2-11
Stage I Engine (LR87AJ-11) C2-9
Stage II Engine (LR91AJ-11) C2-11
Stage II Retro Rocket C2-12
Systems Descriptions, Hazardous Materials, Schematics C2-1
Titan Stage 0 (Solid Rocket Motor) C2-2
Titan Stage I C2-8
Titan Stage II C2-11
Titan II
Airborne Electrical System C6-13
Airborne Hydraulic System C6-13
Airborne Propellant System C6-4
Airframe. C6-2
Autogenous Pressurization System C6-12
Checklists C6-18
Explosive Components C6-14
Flight Control System C6-15
General Description C6-1
Launch and Alert Operations C6-18
Missile Guidance Set C6-15
Missile System C6-16
Mission Scenario C6-16
Propellant System Safety Requirements C6-6
Re-Entry Vehicle C6-17
Rocket Engine System C6-2
Special Safing Procedures C6-10

Page

Titan II - continued
System Equipment C6-5
Systems Descriptions, Hazardous Materials, Schematics C6-2
Titan IV
Alternative Upper Stage C8-3
Avionics (Core Vehicle) C8-13
Booster Modifications C8-2
Centaur Upper Stage C8-20
Controls (Core Vehicle) C8-12
Core Vehicle C8-1
General Description C8-1
Geostationary Mission C8-33
Inclined Missions C8-33
Loads C8-4
Mass Properties C8-29
Mission Capability C8-34
Mission Scenario C8-32
Payload Environments C8-27
Payload Fairing (PLF) C8-27
Payload Interfaces C8-28
Performance C8-32
Propulsion (Core Vehicle) C8-10
Software (Core Vehicle) C8-16
Solid Rocket Motors (SRM) C8-5
Structure (Core Vehicle) C8-10
Systems Descriptions, Hazardous Materials, Schematics C8-5
Titan Stage I - Titan 34D C2-8
Titan Stage II - Titan 34D C2-11
Toxic Chemicals
Atmospheric Dispersion 5-42
Chemical Compounds Released 5-41
Lifetime/Fate of Released Chemicals 5-41
Toxic Materials - Global Positioning System C17-11
Toxicity - Post Accident Environments 5-41
Toxicity, Material (see specific hazardous material, App. B)
Training and Practice 4-41
Trajectory - Orbit Transfer Vehicle C12-25
Transfer Orbit Operations - Global Positioning System C17-13
Transtage
Airborne Hydraulic Systems C14-7
Attitude Control Systems (ACS) C14-6
Command Shutdown and Destruct System C14-9
Flight Termination System Description C14-7
General Description C14-1
Hazardous Material Data C14-9
Inadvertent Separation Destruct System C14-9
Inertial Guidance System C14-6
Location of Pyrotechnics C14-10
Mission Scenario C14-11
Pressure Cartridge C14-11
Propellant Tanks C14-2

Page

Transtage - continued
Systems Descriptions, Hazardous Materials, Schematics C14-1
Transtage Hydraulic System C14-7
Trichloroethane B23-1
Trichloroethylene B23-1
Trichlorofluoromethane (Freon 11) B23-1
Trichlorotrifluoroethane (Freon 113) B23-1
Triorthocresyl Phosphate B24-1
UDMH (Unsymmetrical Dimethyl Hydrazine) B4-1
Ulysses
Attitude and Orbital Control Subsystem C19-19
Earth-Jupiter Operations C19-32
Jupiter Flyby C19-33
Launch and Injection Operations C19-30
Mechanism Subsystem C19-18
Mission Abort Operations C19-34
Mission Scenario C19-28
Mission Summary C19-33
Near-Earth Operations C19-32
Nominal Mission C19-30
Out-of-Ecliptic C19-33
Power Subsystem C19-19
Pyro Subsystem C19-19
Structure Subsystem C19-18
Thermal Subsystem C19-18
Unsymmetrical Dimethyl Hydrazine B4-1
Upper Stages - Titan IV C8-3
VRM Probability Results 4-15
Valves 4-33
Vapor Detection, Material (see specific hazardous material, App. B)
Venting of Sealed or Unsealed Components - Global Positioning System C17-10
Weight Summary - Centaur G Prime C9-8
Wires and Terminal Boards 4-36
Written Instructions 4-41
XDT (High Velocity Impact) 5-21
Xenon B21-1

2.0 GLOSSARY OF TERMS

AEDA (Ammunitions Explosives, and other Dangerous Articles) - Any substance that by its composition and chemical characteristics, alone or when combined with another substance, is or becomes an explosive or propellant or is hazardous or dangerous to personnel, animal or plant life, structures, equipment or the environment as a result of blast, fire, fragment, or toxic effects. It includes but is not limited to ammunition and explosives as defined herein.

AEPS - This term collectively represents rocket catapults and rocket motors utilized in Aircrew Escape Propulsion Systems.

AN/TNT - Amatols - Mixtures of ammonium nitrate and TNT varying in compositions from 80 Wt% AN: 20 Wt% TNT to 50:50 AN to TNT.

Absolute Zero - The theoretical temperature at which all thermal motion or heat action ceases. This is approximately -273.16° Centrigrade, -459.69° Fahrenheit, 0 Kelvin, or 0° Rankine.

Accessibility - The ease and safety of approaching a site.

Accident - An unplanned event, within the boundaries of the system, which results in damage to the system and/or to the environment of the system and which results directly from a hazardous event.

Accident Loss (Loss) - The total death, major injury, equipment or property damage beyond prescribed limits from damage to the system and/or its environment that results directly from the occurrence of an accident.

Accident Risk - The probability that a defined accident will occur in a defined mission for all possible scenarios.

Accident Scenario - Any scenario leading to and including a defined accident.

Accident Scenario Risk - The probability that a defined accident will occur in a defined mission for a defined scenario.

Acidic - A solution which contains excess (over neutral) concentration of hydrogen ions.

Additive - A substance added to a propellant to improve its performance, such as providing smoother burning rate, increased energy output, or lower freezing point.

Adiabatic Flame Temperature - Maximum theoretical temperature obtainable by a particular combination of chemicals.

Aerozine-50 - A mixture of 50 percent (by weight) hydrazine and 50 percent unsymmetrical dimethylhydrazine.

Alkaline - A solution in which the concentration of hydroxyl ions exceeds the concentration of hydrogen ions.

Alkanes - A chemical compound in the saturated hydrocarbon family, such as methane, ethane, propane, butane, etc.

All-up Missile - An all-up missile is one with all major components operationally joined, consisting of a warhead (explosive), propellant, guidance systems, fuze, etc. An all-up missile may or may not be assembled with less hazardous components such as igniter, wings and fins, tracking flares, etc.

Ambient Conditions - Conditions of temperature and atmospheric pressure of the surrounding environment. Reference point is 298 K (77°F) and 14.7 psia (101 kPa).

Ammunition - Type of munitions normally containing explosives, propellant, pyrotechnics, initiating composition, nuclear, or chemical material to inflict damage upon structures, personnel, materiel or military objectives. Ammunition includes cartridges, projectiles, grenades, bombs, pyrotechnics and mines together with projectiles such as bullets, shot and their necessary primers, propellants, fuzes, and detonators.

Ammunition and Explosives - As used herein, ammunition and explosives includes (but is not necessarily limited to) all items of ammunition; propellants, liquid and solid; high and low explosives; guided missiles; warheads, devices, pyrotechnics; chemical agents; components thereof, and substances associated therewith presenting real or potential hazards to life and property.

Anergolic Mixture - A mixture of fuel and oxidizer which will not ignite on contact, but which requires outside source of ignition. Anergolic is the opposite of hypergolic.

Applied impulse - Actual impulsive loading applied to a "target."

Autogenous - Self-Generating.

Ballistite - A double based propellant

Blast - Brief and rapid movement of air or fluid away from a center of outward pressure, as in an explosion; the pressure accompanying this movement.

Blast yield - Energy release in an explosion inferred from measurements of the characteristics of blast waves generated by the explosion.

Blasting Agent - A material designed for blasting which has been tested in accordance with Section 173.114a of DOT regulations and found to be so insensitive that there is very little probability of accidental initiation to explosion or of transition from deflagration to detonation.

Boiling Point - The temperature at which the vapor pressure of the liquid equals atmospheric pressure. The normal boiling point is at 101 kPa (760 mm Hg or 14.7 psia). Where an accurate normal boiling point is unavailable as in a hydrocarbon mixture (RP-1, Jp-fuels), the 10 percent point of distillation performed in accordance with ASTM-D-86-62 may be used as the boiling point of the liquid.

Bonding (Electrical) - Providing a path of low electrical resistance between two objects, usually one of which is at ground potential.

Booster - A high-explosive element of a warhead or similar explosive device used to initiate the high-explosive main charge.

Brisance - The shattering effect of an explosive.

Buddy System - The requirement that at least two persons will be present in any hazardous situation so that one may provide assistance to the other if a mishap occurs.

Bulk-Storage - Tanks, drums, cylinders or other containers used in storing liquid propellants in quantities larger than minimum operational requirements and used to supply ready storage facilities.

Burning Rate - The rate (may be meters/sec) at which a solid propellant burns at a given pressure.

Burst pressure - The pressure at which a storage vessel bursts or fails.

CH-6 - A booster explosive composed of 97% RDX.

Cast Propellant - A solid propellant charge produced from a quantity of casting power/casting or composite propellant and configured into a grain so as to possess certain desired burning characteristics.

Casting Powder - A grandular mixture of colloidized nitrocellulose (single-base) or nitrocellulose and nitroglycerine (double-base) used in ammunition propellant charges.

Catalyst - A substance which alters the speed of a chemical reaction without itself undergoing permanent change.

Cavitating Venturi - Venturi used for measuring liquid flowrates.

Chemical Agent - A solid, liquid, or gas which, through its chemical properties, produces lethal or damaging effects on man, animals, plants, or materials, or produces a screening or signaling smoke.

Combustible Liquid - As defined by the National Fire Protection Association, it means any liquid having a sufficient vapor to form an ignitable mixture with air near the surface of the liquid or within the vessel used. "Ignitable mixture is a mixture within the flammable range (between the upper and lower limits) that is capable of propagating the flame away from the source of ignition when ignited."

Combustible Material - A substance which will burn in the presence of air.

Combustion - An oxidation reaction in which heat or light energy is liberated.

Comp C-4 - Explosive main charge mixture, primarily 91% RDX plus plasticizer.

Compatibility - A relationship between different items of ammunition, explosives and other hazardous materials whose characteristics are such that a quantity of two or more of the items stored or transported together is not significantly more hazardous than a comparable quantity of any one of the items stored or transported alone.

Compatible Material - Having no undesirable reaction or physical effect with or upon another material.

Compatible Propellants - Propellants which may be stored together without increasing the hazards.

Composite Propellant - A propellant system comprising a discrete, solid phase dispersed in a continuous solid phase.

Compressed Gas - Any material or mixture having in its container either an absolute pressure exceeding 276 kPa at 294 K (40 psi at 70°F) or an absolute pressure exceeding 966 kPa at 328 K (140 psi at 130°F), or both; or any liquid flammable material having a Reid vapor pressure exceeding 276 kPa at 311 K (40 psi at 100°F). Such materials are classified as flammable compressed gases if a mixture of 13 percent or less (by volume) with air forms a flammable mixture or if the flammability range with air is greater than 12 percent regardless of the lower limit.

Conductive Floor - Floor made of a nonsparking material such as lead, or rubber or composition containing graphite or other conductive material which will not permit accumulation of electric charges.

Conductive Shoes - Shoes designed to dissipate static charges from the body.

Container - A general term that encompasses boxes; cartridge or powder tanks, cartons, drums, barrels, cylinders or cans; containers for long ordnance items; and cargo containers (Dromedaries, etc.) for shipments of sizeable quantities of hazardous materials. A pallet is not considered to be a container.

Contaminated Area - An area where a toxic chemical agent has been released and is present in any form.

Critical Diameter - Minimum diameter of a propellant grain that will sustain detonation.

Critical Failure - One that results in an actual or potential hazard to personnel or equipment.

Critical Pressure - The pressure required to liquify a gas at its critical temperature.

Critical Temperature - The maximum temperature at which a gas can be liquified. Above the critical temperature point the substance will remain in the gaseous state regardless of the pressure applied.

Critical Threshold Impulse - Blast wave impulse which determines the impulse asymptote for an isodamage contour.

Cryogen - A liquid which boils at temperatures of less than 114 K (-254°F) at atmospheric pressure, such as hydrogen, helium, nitrogen, oxygen, air, or methane.

Cyclotol - Main explosive charge of TNT and RDX.

DDT - Initial combustion that transitions to a detonation.

Decontaminating Agent - An agent having a desirable controlled reaction rate or solvent action which is used to purge materials, components, systems, or areas of residues or contaminants.

Deflagration - Burning at a rapid rate, but below the speed of sound in the unreacted medium.

Density - The ratio of mass to volume for a substance.

Deterrent - A material added to a propellant composition or applied to the surface of a grain to decrease the flame temperature or rate.

Detonation - An exothermic chemical reaction that propagates with such rapidity that the rate of advance of the reaction zone into the unreacted material exceeds the velocity of sound in the unreacted material. The rate of advance of the reaction zone is termed detonation velocity. When this rate of advance attains such a value that it will continue without diminution through the unreacted material, it is termed the stable detonation velocity. When the detonation velocity is equal to or greater than the stable detonation velocity of the explosive, the reaction is termed a "high order" detonation. When it is lower, the reaction is termed a "low order" detonation.

Dewar - A double-walled or multi-walled, vacuum-insulated vessel used to store cryogenic liquids.

Dike - An earth or concrete barrier surrounding a storage tank and intended to contain a spill.

Drag coefficient - Ratio or drag force to dynamic force exerted by wind pressure on a reference area.

Dunnage - Pallets and spacers used in shipping, storage, and handling; frequently made of wood, although metal is preferred.

Duration of Fireball - Length of time that heating occurs within the fireball.

EDNA - Haleita, white powder, ingredient of Ednatol.

EEL (Emergency Exposure Limit) - A single brief accidental exposure to air-borne contaminants that can be tolerated without permanent toxic effects.

Emergency Exposure Limit - See EEL.

Environmental Damage - Death, major injury, equipment or property damage beyond prescribed limits to the environment of the system outside the boundaries of the system.

Evaporation Rate - The ratio of the time required to evaporate a measured volume of one volatile material to the time required to evaporate the same volume of a reference solvent under identical test conditions (usually ethyl ether).

Event - The occurrence or realization of any definable, distinct state or condition or interest of a system or its environment within its boundaries.

Expected (Accident) Loss - Accident loss multiplied by accident risk.

Explosion Proof - The term used in connection with electrical equipment means that such equipment is enclosed in a case which is capable of withstanding an internal burning or explosion of elements contained inside the case and prevent ignition by spark, flash, or explosion of any outside gas or vapor surrounding the enclosured.

Explosive - The term "explosive," or "explosives," includes any chemical compound or mechanical mixture which, when subjected to heat, impact, friction, detonation or other suitable initiation, undergoes a very rapid chemical change with the evolution of large volumes of highly heated gases which exert pressures in the surrounding medium. The term applies to materials that either detonate or deflagrate.

Explosive Equivalent - The amount of a standard explosive which, when detonated, will produce a blast effect comparable to that which results at the same distance from the detonation or explosive of a given amount of the material for which performance is being evaluated. It is usually expressed a a percentage of the total net weight of all reactive materials contained in the item or system. For the purpose of this manual, TNT is used for comparison.

Explosive Hazard - The hazard resulting from the tendency for certain materials to detonate en masse or burn with violence, causing destruction and damage or propagating explosions from one explosive site to another by blast wave or flying fragments.

Explosive Limit - The maximum quantity of explosives or ammunition permitted in a magazine, production building, or other specified site. Explosive limits are based on quantity-distance damage considerations and are expressed in net pounds of explosive, number of rounds or units, or other measuring units. Also called Explosive Quantity.

Explosive Sensitivity - A measure of the impulse required to cause the initiation of an explosive.

Explosives Facility - Any structure or location containing ammunition and explosives excluding Combat Aircraft Parking Areas or Ammunition and Explosives Aircraft Cargo Areas.

FLOX - Mixture of liquid fluorine and liquid oxygen.

Fading Detonation - The slowing down of an initial high-order detonation to a low order detonation or deflagration.

Failure - The inability of a system, subsystem, or component to perform its required function.

Failure Mode - A hardware, software or human malfunction, uniquely described, which constitutes loss of function or functional performance outside of specified limits.

Failure Mode Cause - The immediate or accumulated hardware, software or human state(s) or action(s) which leads directly to or precipitates a failure mode.

Failure Mode Effect - The state(s) or event(s) within the boundaries of the system which result directly or indirectly from the occurrence of a failure mode.

Local	- The immediate or initial effect.
Intermediate	- The effect propagated from the local effect.
System	- The highest, last or end effect within the boundaries of the system.

Failure Mode Effect Probability - The conditional probability that the effect of interest occurs given the preceding event.

Failure Mode Probability - Probability that the failure mode will occur in a defined mission.

Fault Tree - A symbolic logic diagram showing the cause-effect relationship between a top undesired event and one or more contributing causes. it is a deductive analytical means to identify all failure modes contributing the potential occurrence of a given top undesired event.

Fire Hazard - The hazard resulting from the tendency of certain materials to ignite spontaneously by chemical change, by spark, or by friction and contribute excessively to any fire in which they are involved.

Fire Hazard Area - A location in which the primary, but not necessarily the only, hazard is that of fire including "explosions" of gas or vapor and air mixtures.

Fire Resistive - A term used to indicate the design of a structure or materials and the like to resist a fire to which they might be subjected without themselves becoming weakened to the point of failure.

Fire Retardant - A term used to designate generally combustible materials or structures which have been treated or have surface coverings designed to retard ignition or fire spread.

Fireball Liftoff Time - Length of time between propellant ignition and fireball liftoff from ground.

Firebrand - A projected burning or hot fragment whose thermal energy is transferred to a receptor.

Flameproof - Combustible materials, such as clothing which have been treated or coated to decrease their burning characteristics.

Flammable - Materials which are easily ignited in air, oxygen, or other supporting atmosphere.

Flammable Limits - The upper and lower vapor concentration of fuel to air which will ignite in the presence of external ignition sources; often also referred to as the explosive range. Flammable limits in atmospheres other than air are so identified.

Flash Point - The mean temperature at which enough vapors of a liquid are given off to mix with air, ignite, and produce flames. Flash points are usually determined by the "closed-cup" method for liquids with flash points around normal temperatures; the "open-cup" method is used for liquids having relatively high flash points. Open-cup data are usually higher than closed-cup results.

Fragmentation - The breaking up of the confining material of a chemical compound or mechanical mixture when an explosion takes place. Fragments may be complete items, subassemblies, pieces thereof, or pieces of equipment or buildings containing the items.

Frangible - Fragile, breakable.

Freon 11 - Trichlorofluoromethane

Freon 113 - Trichlorotrifluoroethane, or 1,1,2-trifluoro-1,2,2-trichloroethane

Freon 12 - Dichlorodifluoromethane

Freon 21 - Dichloromonofluoromethane

Freon 22 - Difluorochloromethane

Fuel - A material which may be burned by itself or used with an oxidizer to liberate energy for use in vehicle propulsion systems.

Fume Scrubber - Equipment in which toxic or corrosive propellant fumes are neutralized so that the atmosphere will not be contaminated.

Furlable - Capable of being wrapped around or rolled around something.

Gimbaled - Inclined in any direction or suspended and remaining level when the support is tipped.

Grain - A single mass of solid propellant of the final geometric configuration as used is a gas generator or rocket motor. Gun propellant charges consist of a large number of very small grains.

Gun Propellant- See Grain.

Gun and Rocket Ammunition - A type of projectile and its propellant characterized by a ratio of explosive charge weight to total projectile weight of 30 percent or less. The explosive charge is designed to inflict its maximum damage by penetration of the target.

HMX - Cyclotetramethylenetetranitramine.

Halogenation - A chemical reaction in which a hydrogen atom in a hydrocarbon has been replaced by a halogen (see alkane).

Halogens - The elements fluorine, chlorine, iodine, and bromine.

Halon 1202- Dibromodifluoromethane

Halon 1211 - Bromochlorodifluoromethane

Halon 1301 - Bromotrifluoromethane

Halon 2402 - Dibromotetrafluoroethane - 1,1,2,2-tetrafluoro-1,2-dibromoethane

Hazard - A material and/or condition or a set of range of material(s) and/or condition(s) which must be precluded or otherwise controlled within the boundaries of the system to avoid major injury, death or other loss exceeding prescribed limits.

Hazard Control - Any feature, measure, procedure, etc., which singularly or in combination with other features, measures, procedures functions to maintain control of hazards and prevents accidents resulting from release or realization of hazards.

Hazard Control Function - A non-reduceable active or passive statement of the purpose or method (function) of a hazard control.

Hazard Level - Hazards are classified by MIL-STD-882 in four categories, based upon the most severe result of probable personnel error, environment, design characteristics, procedural deficiencies, or subsystem or component failure or malfunction. The four categories, and the most logical consequences under the circumstances and conditions cited, are:

Category I - Catastrophic - A hazardous occurrence whose worst-case effects will cause death or severe injury to personnel or loss of system.

Hazard Level - continued

Category II - Critical - A hazardous occurrence in which the worst case effects will cause severe personnel injury or major system damage, or will require immediate corrective action to prevent personnel death or loss of system. Severe injury is defined as injury requiring hospitalization. Major system damage is defined as extensive performance impairment.

Category III - Marginal - A hazardous occurrence whose worst case effects can be counteracted or controlled without serious personnel injury or equipment damage. Injury is limited to first-aid medical care. Equipment damage shall not impair system performance.

Category IV - Negligible - A hazardous occurrence in which the worst case effects could not result in personnel injury or equipment damage.

Hazardous Condition - A possible condition or state or the system or its environment which may cause major injury, death or other loss exceeding prescribed limits.

Hazardous Event - The occurrence or realization of the loss of control(s) of a hazard necessary to avoid major injury, death or other loss exceeding prescribed limits.

Hazardous Locations (Electrical Equipment) - Locations where flammable gases or vapors are or may be present in the air in explosive or ignitable mixtures or where combustible dust or easily ignitable particles or fibers may be present.

Hazardous Material - A poison or toxin, corrosive agent, flammable substance, explosive, radioactive chemical, or any other material which can endanger human health or well-being if handled properly. Any compound, mixture, element or assemblage of material which, because of these inherent characteristics, is dangerous to manufacture, process, store or handle.

High Explosive - An explosive in which the transformation from its original composition and form, once initiated, proceeds with virtually instantaneous and continuous (supersonic) speed throughout the total mass, accompanied by the rapid evolution of a large volume of gas and heat, causing very high pressure and widespread shattering effect. Some authorities classify high explosives by their sensitivity to initiation as "primary" explosives, those that are very sensitive and "secondary" explosives, those that are relatively insensitive. Primary explosives are also referred to as initiating explosives.

High Explosive Equivalent - See Explosive Equivalent

Hydrazine - Liquid fuel or monopropellant and a component of Aerozine-50.

Hydrocarbon - Chemical compounds composed only of hydrogen and carbon.

Hygroscopicity - The tendency of a material to absorb moisture from its surroundings.

Hypergolic - Term applied to the self-ignition of a fuel and an oxidizer upon mixing with each other without a spark or other external aid.

Hypergolic Mixture - A term applied to describe instantaneous self-ignition of certain fuels and oxidizers upon contact with each other.

Ignition Temperature - The mean temperature at which a combustible material can be ignited and will continue to burn when the ignition source is removed. The ignition temperature for any one substance will vary with its particle size, confinement, moisture content and ambient temperature.

Ignition Time - The time interval required for initiation of a propellant after application of an adequate stimulus.

Impulse Ammunition - Cartridges or charges consisting of specially prepared propellant charges contained in cartridge cases fitted with primers and assembled as blank cartridges for launching torpedoes, for propelling line throwing (carrying) projectiles, and for similar uses.

Incapacitating Agent - An agent that produces temporary physiological or mental effects, or both, which will render individuals incapable of concerted effort in the performance of their assigned duties.

Incendiary - A chemical agent used primarily for igniting combustible substances with which it is in contact by generating sufficient heat to cause ignition.

Inert Area - Any area other than an explosives or administration area within an establishment.

Inert Material - Material that contains no explosives, active chemicals, or pyrotechnics.

Inhabited Building - Any building or structure, other than an operating building, magazine or auxiliary building, occupied in whole or part as a habitation for human beings, or a building, structure or area where people are accustomed to assemble, both within and outside Government establishments. Land outside boundaries of establishments will be considered possible sites of inhabited buildings.

Inhibited Propellant - A propellant grain in which a portion of the surface area has been treated to reduce the surface burning area.

Inhibitor - A substance bonded, taped, or dip-dried onto a solid propellant to restrict the burning surface and to give direction to the burning process. Also, a substance which will slow down or stop the action of a chemical.

Initiator - An initiator is an electro-explosive or chemical device used to start a reaction in a propellant or explosive. Initiators may be igniters, gas generating devices, or shock producing devices.

Insoluble - Not capable of being dissolved, generally considered in water.

Interface Analysis - Term used interchangeably with System Hazard Analysis.

Inversion - An increase in ambient temperature with increase in altitude.

Isochoric Flame Temperature - The temperature of a propellant flame under constant volume conditions.

Life Support - Protection of personnel in environments which are immediately hazardous to life.

Liquid Propellant - The liquid substances used for propulsion or operation of missiles, rockets, and other related devices.

Liquified Gases - Substances which are gases at ambient conditions of temperature and pressure and have been converted to liquids under controlled pressure and temperature.

Longeron - A fore and aft framing member of an aircraft or launch vehicle fuselage.

Loss - See accident loss.

Loss Control - Any feature, measure, procedure, etc., which singularly or in combination with other features, measures, procedures functions to prevent or reduce possible system damage and/or environmental damage resulting from an accident.

Loss Scenario - Any scenario leading to and including a defined loss.

Low Explosive - An energetic material that reacts through a deflagration mechanism as opposed to a detonation (see High Explosive). A deflagration is characterized as an exothermic reaction propagating through the unreacted medium at a subsonic velocity and occurs through a diffusion mechanism through the total mass, as opposed to the shock wave mechanism of propagation in the case of high explosive. The velocity of combustion is fixed or controlled by the granulation, the density of loading, the confinement (surrounding pressure) and similar factors. Combustion occurs steadily over the surface of the powder grains and from layer to layer until the total mass is consumed. The resultant reaction causes evolution of heat and usually a large volume of gases. Some low explosives under conditions of proper flames, packing confinement, and initiation may detonate when ignited; conversely, some high explosives may simply burn if ignited under the proper conditions.

Lower Explosive Limit (LEL) - The lowest concentration by percent of volume of a gas or vapor in the atmosphere at normal temperatures and pressures at which the gas or vapor will ignite and sustain combustion.

METN (Metriol Trinitrate) - Trinitroxymethyl-2-methyl-1,3-propanediol Trinitrate (MTN)

MMH (Monomethylhydrazine) - Liquid fuel and a monopropellant.

Major Injury - Any injury which results in admission to a hospital and prolonged treatment such as a bond fracture, second or third degree burns, severe lacerations, internal injury, severe radiation exposure, chemical or physical agent toxic exposure or unconsciousness.

Mass Detonation - Virtually instantaneous explosion of mass of explosives when only small portion is subjected to an initiating agent or stimulus.

Mass ratio - Ratio of the weight of the propellant to the weight of the loaded rocket.

Max Q - Maximum Dynamic Load.

Maximum Allowable Concentration (MAC) - The maximum concentration of vapor in air to which workers may be exposed for eight hours daily, five days a week, over an indefinite period without injury to health. Differs from threshold limitation value TLV, which is an average concentration.

Maximum Credible Event (MCE) - In hazards evaluation, the maximum credible event from a hypothesized accident that is likely to occur. The event must be realistic with a reasonable probability of occurrence. The MCE evaluated on this basis may then be used as a basis for effects calculations and casualty predictions.

Mean Test Duration Time - Downtime.

Mishap - Synonymous with accident.

Molecular Weight - The weight of a formula unit equal to the sum of the atomic weights of the atoms which make up the molecular.

NEQ (Net Explosive Quantity [kg]) - Net Equivalent Quantity is a standard scaled distance (i.e., quantity-distance) calculation given by the formula, $d = m/kg^{1/3}$.

NEW (Net Explosive Weight [lb]) - Net Explosive Weight is a standard scaled distance (i.e., quantity-distance) calculation given by formula, $d = ft/lb^{2/3}$. It is the English unit equivalent of NEQ.

Net Explosives Weight (NEW) - See NEW.

Neutral Burning - The burning of a propellant grain in which the reacting surface ara remains approximately constant during combustion.

Neutralization - The adjustment of pH to approach a value of 7, in an aqueous system.

Nitrogen Padding (or Blanket) - The filling of the void or ullage of a closed container with nitrogen gas to prevent oxidation of the chemical contained therein and to avoid formation of a flammable mixture; also may be used to mean the maintenance of a nitrogen atmosphere in or around an operation, piece of equipment, and the like.

Nonflammable Gas - A gas that does not ignite and does not burn if ignited.

Nutation - Rocking on Axis, nodding.

Operating Hazard Analysis - Term used interchangeably with Procedure Analysis.

Ordnance - Military materiel such as combat weapons of all kinds with ammunition and equipment required for their use. Ordnance includes all the things that make up a ship's or aircraft's armament - guns, ammunition, and all equipment needed to control, operate, and support the weapons.

Oxidizer - A substance such as a chlorate, perchlorate, permanganate, peroxide, nitrate, oxide, or the like that yields oxygen readily to support the combustion of organic matter, powdered metals, and other flammable material.

Pallet - A wood or metal, square or rectangular platform upon which cargo is located so that the cargo and pallet may be moved as a unit and stacked without cargo rehandling. The platform is raised sufficiently to allow pallet engagement by the tines of a fork lift truck.

Partial Detonation - Only part of total explosive load in ammunition detonates. Strong air shock and small as well as large case fragments are produced. Small fragments are similar to those in normal complete detonation. Extensive blast and fragmentation damage results to the surrounding area. Amount of damage and extent of breakup of case into small fragments increase with increasing amount of explosive that detonates. Severity of blast could cause large ground crater, if ammunition is large bomb; hole size depends on amount of explosive that detonates.

Pentolite - A main explosive charge consisting of TNT and PETN.

Poison A - A gas or liquid of such nature that a very small amount of the gas or the vapor of the liquid mixed with air is dangerous to life.

Poison B - Class B poisons are those substances, liquid or solid (including pastes and semisolids, other than Class A poisons), which are known to be so toxic to man as to afford a hazard to health, or which, in the absence of adequate data on human toxicity, are presumed to be toxic to man based on toxicity tests conducted on laboratory animals.

Poisonous gas - A toxic or irritant gas or volatile liquid that is harmful to living tissues when applied in relatively small doses.

Post-Accident Environment - The conditions (e.g., thermal, radioactive, fragmentation, toxicity) resulting from the accident which, and in part or in total, cause the damage to the system and/or its environment and the accident loss.

Primer - A relatively small and sensitive initial explosive train component, which when actuated, initiates the function of the explosive train, and with an adequate booster, will reliability initiate high explosive charges.

Program Accident Loss - The incremental or additional loss to a program, exclusive of accident loss, which results from a single accident, such as the cost of schedule modification, lost security, etc.

Program Accident Risk - The probability that a defined accident will occur for all scenarios for the life of the program.

Progressive Burning - The burning of a propellant grain in which the motor pressure and/or gas effluent rate increases during the combustion.

Propagating Explosion - Communication of an explosion (detonation or deflagration) from one explosives source to another by fire, fragment, or blast (shock wave), where the time interval between explosions is sufficient to limit the total overpressure at any given time to that which each explosion produces independently. This condition, where detonation occurs, would be evidenced by a distinct shock wave from each detonation with a discernible pressure drop between each explosion.

Propellants - Are balanced mixtures of fuel and oxidizer designed to produce large volumes of hot gases at controlled, predetermined rates, once the reaction is initiated.

Propelling Charge - Charge of low explosive that is burned in a chamber to propel a projectile.

Protected - The term "protected" means shock wave, spill, or fragment protection provided by terrain, effective barricades, net or other physical means to inhabit buildings within the hazardous area distances expected from the propellant facilities.

Protective Clothing - Clothing especially designed, fabricated, or treated to protect personnel against hazards caused by extreme changes in physical environment or dangerous working conditions.

Protective Mask - A field protective mask consisting of a full face mask and all component parts used for protection against field concentrations of chemical agents. These are not gas masks.

Pyrophoric - Capable of spontaneous ignition upon contact with air, water, or other materials containing oxygen at or below 327.6 K (130°F).

Quantity-Distance (QD) - The quantity of explosives material and distance separation relationships which provide defined types of protection. These relationships are based on levels of risk considered acceptable for the stipulated exposures and are tabulated in the appropriate quantity-distance tables. Separation distances are not absolute safe distances but are relative protective or safe distances. Distances greater than those shown in the tables should be used wherever practicable.

Reliability - The probability that a system, subsystem, or component can perform its required functions under defined operating conditions.

Rocket - A missile which derives its thrust from ejection of hot gases generated from propellants carried in the missile motor.

Rocket Engine - Self-contained rocket propulsion unit containing an oxidizer and a fuel, or a monopropellant, each separated by an aluminum or stainless steel wall, and utilizing liquid rather than solid propellant material.

Rocket Motor - That portion of the rocket loaded with solid propellant.

Rocket Propellant - Any liquid, gaseous, or solid substances, or combination or solid substances, or combinations of component substances, which produce chemical reactions, whereby hot gases are generated in large volume and at adequate pressure and velocity for propulsion of guided missiles and other devices and crafts.

Rocket Warhead - That portion of the rocket loaded with high explosives, chemicals, or inert material.

Safety Design Reviews - Preliminary and critical design reviews provide an assessment of how well the system design conforms to safety criteria. They are normally accomplished during the validation and full scale production phases of the acquisition cycle.

Safety Distances - Safety distances are empirical distances in relation to quantities of explosives and are the minimum permitted for separation of facilities within a hazard area of possible explosions and for separation of the explosive hazard from inhabited buildings, passenger railroads, and public highways in order to control the magnitude of damage, loss of life, and serious injuries. Separation distances are not absolute safe distances but are relative protective or safe distances and must be graduated as to risk to provide for selected types of protection. See also Quantity-Distance.

Safety Shoes - Specifically designated footwear of three general types: (a) Industrial safety shoes with hard toes or other resistive physical characteristics, (b) Spark-proof shoes containing no exposed metal for use in locations where friction sparks are hazardous, and (c) Conductive sole safety shoes used where static electricity or friction hazards are present. Safety shoes can also consist of a combination of the above features.

Safety Tools - Tools constructed of wood, fiber, and other substances such as bronze, lead, K-Monel metal and beryllium alloys having low sparking characteristics and which will not produce sparks under normal conditions of use. The use of this type is mandatory when hand tools are used in connection with certain explosives and ammunition operations, at which time they will be so specified.

Saturation - A state of solution in which the dissolved solute is in equilibrium with excess undissolved solute.

Scenario - Any unique set of events and conditions leading to and including the event of interest.

SDT - Direct initiation of detonation by shock.

Self contained breathing apparatus - A breathing apparatus with air supply that keeps the individual completely independent of the surrounding atmosphere.

Single-base powder - A casting powder whose principal explosive ingredient is nitrocellulose.

Smokeless powder - Solid monopropellant comprising nitrocellulose, with or without oxidizing and/or fuel plasticizers.

Solvent - A substance capable of dissolving another substance (solute) to form a uniformly dispersed mixture (solution) at the molecular or ionic size level. Solvents are either polar (high dielectric constant) or non-polar (low dielectric constant).

Sparkproof - The term used to describe equipment which is so designed to ensure no flames or sparks will escape to the surrounding atmosphere from within its case or enclosure. Also referred to as spark-enclosed.

Spontaneous Ignition Temperature - Minimum autogenous ignition temperature when flammable component is in contact with a specified surface or heated element.

Stability - The ability of any ammunition or explosive to withstand adverse conditions and deterioration while in storage or use.

Stacks - Safe orderly groupings of explosives, ammunitions, and related component parts in storage.

Stage 0 - Solid Rocket Motors on Titan Systems.

Standard Job Procedure (SJP) - A locally devised procedure for a specific operation.

Standard Operations Procedure (SOP) - A document which prescribes operator instructions in a definite course of action for processing a work unit. It is a tool for managing resources through planning and scheduling manpower, equipment, facilities and material in producing a quality product safely and efficiently. An SOP includes specifications, safety instructions and performance standards.

Storage Building - Any building or structure, other than a magazine, used or intended to be used for storage of liquid propellants.

Storage Compatibility Group - The compatibility group for ammunition, explosives and/or other hazardous materials which can be stored together without significantly increasing the probability of accident or, for a given quantity, the magnitude of the effects of such an accident. The compatibility groups are based on the system recommended for international use by the United Nations Organization (UNO) and as adopted by the Department of Defense. Refer to volume 2 for the descriptions of each compatibility group.

Super * Zip - Trade Name.

System Accident Environment - The environment of the system existing at the time of an accident.

System Damage - Death, major injury, equipment or property damage beyond prescribed limits within the boundaries of the system.

TNT Equivalent Weight - Amount of TNT required to produce the same energy release, blast characteristic or explosion damage as the actual propellant or pressurized tank would upon explosion.

Terminal Yield - Blast yield from measurements made far enough from an explosion that the waves are similar to those generated by a specified mass of TNT.

Threshold Limit Values (TLV-ACGIH) - The upper values of a toxicant concentration to which an average healthy person may be repeatedly exposed to day after day without suffering adverse effects.

Thrust - The resultant force in the direction of motion, produced by a rocket motor.

Toxic - Relating to, or caused by, poison or toxic.

Toxicity - The property possessed by a material which enables it to injure the physiological mechanism of an organism by chemical means, with the maximum effect being death.

Triple-base Propellant - Propellant with three explosive ingredients, such as nitrocellulose, nitroglycerin, and nitroguanidine.

Vehicle Response Mode - Used interchangeably with System Failure Probability.

Volatile - A substance that will readily vaporize at a low temperature.

Web - In a solid propellant grain, the minimum distance which can burn through as measured perpendicular to the burning surface.

XDT - Delayed detonation induced by a shock.

3.0 LIST OF SPHAM ACRONYMS

2-NDPA	2-Nitrodiphenylamine
4-NDPA	4-Nitrodiphenylamine
AACS	Attitude and Articulation Control Subsystem
AAP	Army Ammunition Plant
ACC	Aft Cargo Carrier
ACE	Attitude Control Electronics
ACGIH	American Conference of Government Industrial Hygienists
ACS	Active Cooling System
ACS	Attitude Control System
AEDA	Ammunitions Explosives, and other Dangerous Articles
AEPS	Aircrew Escape Propulsion Systems
AFAL	Air Force Astronautics Laboratory
AFETR	Air Force Eastern Test Range
AFOSH	Air Force Occupational Safety and Health
AFRPL	Air Force Rocket Propulsion Laboratory
AFRSI	Advanced Flexible Reusable Surface Insulation
AFT-FUS	Aft Fuselage
AGE	Aerospace Ground Equipment
AICHE	American Institute of Chemical Engineers
AKM	Apogee Kick Motor
AMCR	Army Materiel Command Regulation
AMR	Atlantic Missile Range
AN	Ammonium Nitrate
ANSI	American National Standards Institute
AOA	Abort-Once-Around
AOCS	Attitude and Orbit Control Subsystem
AP	Ammonium Perchlorate
APCS	Automated Pressure Control System
APS	Accessory Power Supply
APU	Auxiliary Power Units
ARA	Accident Risk Assessment
ARAR	Accident Risk Assessment Report
ARP	Aerospace Recommended Practice
ARPA	Advanced Research Projects Agency
ASE	Airborne Support Equipment
ASI	Atmospheric Structure Instrument
ASI	Apollo Standard Initiator
ASME	American Society of Mechanical Engineers
ATO	Abort-To-Orbit
ATP	Authority to Proceed
BAT	Battery
BOS	Booster Ordnance Sequence
BTTN	1,2,4-Butanetriol Trinitrate
BVL	Butterly Valve Lock
BWR	Boiling Water Reactor
CAMBL	Continuous Automated Multi-Base Line
CAS	Chemical Abstract Service

CASBL	Continuous Automated Single-Base Line
CBGS	Confined by Ground Surface
CBM	Confined by Missile
CCAFS	Cape Canaveral Air Force Station
CCAM	Centaur Collision and Contamination Avoidance Maneuver
CCVAPS	Computer Controlled Vent and Pressurization System
CDF	Confined Detonating Fuse
CDR	Critical Design Review, Command Destruct Receiver
CDRL	Contract Dat Requirement List
CDS	Command & Data Subsystem
CDU	Control Distribution Unit
CE	Cargo Element
CEF	Crossrange Error Function
CFMA	Cable Failure Matrix Analysis
CG	Coast Guard (see USCG) or center of gravity
CHARM	Complex Hazard Air Release Model
CI	Contract Item
CIS	Centaur Integrated Support System
CL	Class
COM	Communications Subsystem
CPF	Chlorine Pentafluoride
CPIA	Chemical Propulsion Information Agency
CPOCC	Centaur Payload Operations Control Center
CRT	Cathode Ray Tube
CSD	Chemical Systems Division
CSDS	Command Shutdown and Destruct System
CSS	Centaur Support System
CTCS	Cracke-Mounted Thermal Control System
CTF	Chlorine Trifluoride
CU	Control Unit
DACC	Dedicated Aft Cargo Carrier
DATB	1,3-diamino-2,4,6-trinitrobenzene
DB	Double base
DCU	Digital Computer Unit
DDS	Dust Detector
DDT	See Glossary
DETA	Diethylenetriamine
DFCS	Digital Flight Control System
DFVLR	Deutsche Forschungsund-Versuchsanstalt fur Luft-und Raumfahrt
DIGS	Delta Inertial Guidance System
DMP	Dimethyl Phthalate
DNA	Data Not Applicable
DNT	2,4-Dinitrotoluene
DOA	Dioctyl Adipate
DOD	Department of Defense
DOP	Di-2-ethylhexyl Phthalate
DOT	Department of Transportation
DR	Data Requirements
DRIMS	Delta Redundant Inertial Measurement System
DS	Defense Support Program
DSCS	Defense Satellite Communications System
DSN	Deep Space Network
DUFTAS	Dual Failure Tolerant Arm/Safe Sequence

EAFB	Edwards Air Force Base
ECLSS	Environmental Control and Life Support Subsystem
ECS	Engineering Change Summaries
EDU	Electrical Distribution Unit
EEC	Extendable Exit Cone
EED	Electro-Explosive Device
EEL	Emergency Exposure Limit
EGSE	Electrical Ground Support Equipment
EIRP	Effective Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPD	Energetic Particles Detector
EPDM	Ethylene Propylene Terpolymer
EPDS	Electrical Power & Distribution Subsystem
EPT	Ethylene Propylene Terpolymer
ERDA	Energy Research and Development Agency
ESA	European Space Agency
ESD	Electrostatic Discharge
ESMC	Eastern Space and Missile Center
ET	External Tank
ETA	Explosive Transfer Assembly
ETM	Explosive Transfer Manifold
ETR	Eastern Test Range
EV	Expendable Vehicle
EVA	Extravehicular Activity
EWO	Emergency War Order
FAA	Federal Aviation Administration
FABU	Fuel Additive Blender Unit
FAX	Facsimile transfer
FBA	Fuse and Bleed Assembly
FC	Fuel Cell
FCS	Flight Control System
FCV	Flow Control Valve
FEAA	Ferric Acetylacetonate
FEFO	Bis(2,3-dinitro-2-fluoroethyoxy)methane
FLTSATCOM	Fleet Satellite Communications
FM	Factory Mutual
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FRR	Flight Readiness Review
FRSI	Flexible Reusable Surface Insulation
FS	Fire Switch
FTS	Flight Termination System
FVV	Fuel Vent Valve
FWC	Filament-Wound Case
GAP	Glycidyl Azide Polymer
GCMG	Guidance Control Monitor Group
GCS	Ground Control System
GD	General Dynamics
GD/C	General Dynamics/Convair
GDC	General Dynamics Corporation
GEO	Geosynchronous Earth Orbit
GFE	Government Furnished Equipment

GH_2	Gaseous Nitrogen
GNC	Guidance Navigation and Control
GPC	General Purpose Computer
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
H/W	Hardware
HAD	Helium Abundance Detector
HAN	n-hexylamine
HARM	Hypergol Accidental Release Model
HC	Hexachloroethane-zinc mix (smoke mixture)
HE	High explosive
HEO	High Earth Orbit
HF	Hydrogen Fluoride
HGA	High Gain Antenna
HGDS	Hazardous Gas Detection System
HM	Hazardous Material
HMDI	1,6-Hexamethylenediisocyanate
HMX	Cyclotetramethylenetetranitramine
HR	Hazards Report
HRSI	High Temperature Reusable Surface Insulation
HTPB	Hydroxy-Terminated Polybutadiene
HVI	High Velocity Impact
HVV	Helium Vent Valve
ICD	Interface Control Document
IDP	Isodecyl Pelargonate
IGS	Inertial Guidance System
IMG	Inertial Measurement Group
IMU	Inertial Measurement Unit
INSRP	Interagency Nuclear Safety Review Panel
IPDI	Isophorone Diisocyanate
ISDS	Inadvertent Separation Destruct System
ISR	Integrated Safety Review
ITIP	Improved Transtage Injector Pattern
ITL	Integrate-Transfer-Launch
IUS	Inertial Upper Stage
JANNAF	Joint Army-Navy-NASA-Air Force interagency Propulsion Committee
JCS	Joint Chiefs of Staff
JOI	Jupiter Orbiter Insertion
JP	Aviation jet fuel
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KOH	Potassium Hydroxide
KSC	Kennedy Space Center
LASS	Lateral Acceleration Sensing System
LCCFC	Launch Control Complex Facilities Console
LCS	Launch Control System
LGA	Low Gain Antenna
LH_2	Liquid Hydrogen
LOCA	Loss of Cooling Accident
LOX	Liquid Oxygen
LOX	Liquified Oxygen
LRAFB	Little Rock Air Force Base
LRD	Lightning & Radio Emission

LRSI	Low Temperature Reusable Surface Insulation
LSC	Linear-Shaped Charges
LSR	Launch Signal Responder
LWR-MID	Lower Midbody Compartment
LWT	Light Weight Tank
LeRC	Lewis Research Center
MAC	Maximum Allowable Concentration
MAF	Mixed Amine Fuels
MAG	Magnetometer
MAGE	Mechanical Aerospace Ground Equipment
MAMS	Missile Assemble and Maintenance Shops
MAPO	1-(2-methyl)aziridinyl phosphine oxide
MBA	Multi-Beam Antennas
MCAFB	McConnell Air Force Base
MCE	Maximum Credible Event
MDAC	McDonnell Douglas Astronautics Company
MDF	Mild Detonating Fuse
ME	Main Engine
MECO	Main Engine Cut-Off
MEOP	Maximum Expected Operating Pressure
MEOT	Maximum Expected Operating Temperature
MES	Main Engine Start
MET	Mission Elapsed Time
METN	Metriol Trinitrate
MFSOV	Main Fuel Shutoff Valve
MGS	Missile Guidance Set
MIL	Military
MLI	Multi-layer Insulation
MLP	Mobile Launch Platform
MMH	Monomethylhydrazine
MMS	Multimission Modular Spacecraft
MON	Mixed Oxides of Nitrogen
MOP	Maximum Operating Pressure
MOS	Mission Operations Segment
MOV	Motor Operated Valve
MPHT	Missile Potential Hazard Team
MPS	Main Propulsion System
MPS	Memory Power Subassembly
MSFC	Marshall Space Flight Center
MSHA	Mining Safety Health Administration
MTN	Metriol Trinitrate (METN)
N_2O_4	Nitrogen Tetroxide
NAS	Naval Air Station
NASA	National Aeronautics and Space Administration
NAVORD	Naval Ordnance
NAVSTA	Naval Station
NC	Nitrocellulose
NC	Normally Closed
NDI	Non-Destructive Inspection
NDT	Non-Destructive Tests
NEI	Nonexplosive Initiators
NEP	Nephelometer
NEQ	Net Explosive Quantity (kg)

NEW	Net Explosive Weight (lb)
NFPA	National Fire Protection Association
NG	Nitroglycerin
NHC	n-Hexylcarborane
NIMS	Near Infrared Mapping Spectrometer
NIOSH	National Institute for Occupational Safety and Health
NMS	Neutral Mass Spectrometer
NO	Normally Open
NOIBN	Not Otherwise Indexed by Name
NOSIH	Naval Ordnance Station - Indian Head
NSI	NASA Standard Initiator
NSWC	Naval Surface Weapons Center
NTO	Nitrogen Tetroxide
OAB	Ordnance Assembly Building
OD	Orbit Determination
OFI	Operational Flight Instrumentation
OHA	Operation Hazards Analysis
OMS	Orbital Maneuvering System
OSHA	Occupational Safety and Health Administration
OSS	Ordnance Safety Switch
OSTF	Operational Test Facility
OTV	Orbital Transfer Vehicle
OVV	Oxidizer Vent Valve
P/L	Payload
P/N	Part Number
PACE	Programmable Aerospace Control Equipment
PAF	Plasma-Arc Facility
PAF	Payload Attach Fitting
PAM	Payload Assist Module
PBAA	Polybutadiene Acrylic Acid
PBAN	Polybutadiene Acrylic Acid Acrylonitrile Terpolymer
PBX	Plastic bonded explosive
PBXN	Plastic bonded explosive - nylon
PC&E	Protective clothing and equipment
PCA	Pressurant Control Assembly
PCM	Pulse Code Modulation
PCP	Polycaprolactam
PCU	Pyro Control Unit
PCV	Pressure control valve
PDR	Preliminary Design Review
PDU	Power Distribution Unit
PETN	Pentaerylthritol Tetranitrate
PGA	Polyethylene Glycol Adipate
PHA	Preliminary Hazard Analysis
PIA	Propellant Isolation Assembly
PIC	Pyro Initiator Controller
PICU	Pyrotechnic Initiator Control Unit
PIDA	Payload Installation and Development Aid
PIM	Payload Interface Module
PJR	Perijove Raise
PLB	Payload Bay
PLCM	Propellant Loading Control Monitor
PLF	Payload Fairing

PLIU	Propellant Level Indicating Unit
PLS	Plasma
PLX	Propellant Loading Exercise Countdown
PNC	Plasticol Nitrocellulose
POGO	Longitudinal Vehicle Oscillation
PPM	Parts per Million
PPR	Photopolarimeter Radiometer
PRD	Pressure Release Device
PRD	Program Requirements Document
PS	Primary Structure
PSI	Pounds per Square Inch
PSIG	Pounds per Square Inch Gauge
PSU	Pyro Switching Unit
PSV	Pressure Sequence Valve
PSVOR	Pressure Sequencing Valve Override
PTA	Propellant Tank Assembly
PTM	Press-To-MECO
PTPMU	Propellant Tank Pressure Monitor Unit
PTS	Propellant Transfer System
PTSCU	Propellant Transfer System Control Unit
PTU	Power Transfer Unit
PU	Propellant Unit
PUU	Propellant Utilization Unit
PVD	Portable Vapor Detector
PVSS	Portable Vapor Suppression System
PWR	Pressurized Water Reactor
PWS	Plasma Wave
QAR	Quality Assurance Report
QD	Quick Disconnect
R&D	Research and Development
RADC	Rome Air Development Center
RADHAZ	Radiation hazard (to personnel, fuel and other flammable material)
RAM	Random Access Memory
RCE	Reaction Control Equipment
RCRA	Resource Conservation and Recovery Act
RCS	Reaction Control System
RDX	Cyclotrimethylenetrinitramine
REF	Range Error Function
REM	Reaction Engine Modules
RF	Radio Frequency
RFHCO	Rocket Fuel Handler's Clothing Outfit
RFI	Radio Frequency Interference
RFP	Request for Proposal
RGS	Radio Guidance System
RHU	Radioisotope Heater Unit
RI	Rockwell International
RMU	Redundant Measurement Unit
ROM	Read-Only Memory
ROV	Removet Operate Valve
RPM	Retropropulsion Module
RSC	Range Safety Command
RSI	Reusable Surface Insulation
RSO	Range Safety Officer

RSS	Radio Science
RTG	Radioisotope Thermoelectrical Generators
RTGPRD	Radioisotope Thermoelectric Generator Pressure Release Device
RTLS	Return-To-Launch-Site
RV	Reentry Vehicle
S&A	Safe and Arm
S/C	Spacecraft
SAC	Strategic Air Command
SAE	Society of Automotive Engineers
SBASI	Single Bridge-wire Apollo Standard Initiators
SC	Steel Case
SCA	Shuttle Carrier Aircraft
SCA	Sequence Control Assembly
SCG	Storage Compatibility Group
SCP	Safety Certification Panel
SCR	Silicon Controlled Recitipiers
SCRAM	[Reactor Protection System]
SCU	Sequence Control Unit
SD	Space Department
SDR	System Design Review, Space Division Regulation
SDT	See Glossary
SECO	Second Stage Engine Cutoff
SFP	Single Failure Point
SIT	Spontaneous Ignition Temperature
SIU	Servo Inverter Unit
SLA	Super-Lightweight Ablator
SMDC	Shielded Miled Detonating Chord
SODI	Spray-On Foam Insulation
SOW	Statement of Work
SPHAM	Space Propulsion Hazards Analysis Manual
SRB	Solid Rocket Booster
SRM	Solid Rocket Motor
SRP	Safety Review Panel
SRR	System Requirements Review
SRT	Safety Review Team
SSG	System Safety Group
SSI	Solid State Imaging
SSME	Space Shuttle Main Engine
SSP	Standard Switch Panel
SSPP	System Safety Program Plan
SSPU	Second Stage Propulsion Unit
SSR	System Safety Review
STDN	Space Tracking and Data Network
STP	Standard Temperature (273.15 K) and Pressure (101 kPa)
STS	Space Transportation System
SXA	S-Band/X-Band Antenna
T.O.	Technical Order
TAEM	Terminal Aera Energy Management
TAI	Toluene-2,4-diisocyanate
TAL	Transatlantic Abort Landing
TARS	Three Axis Reference System
TBD	To Be Determined
TBI	Through-Bulkhead Initiator

TCC	Transparent Conductive Coating
TCM	Trajectory Correcting Maneuver
TCS	Thermal Control System
TCV	Thrust Chamber Valve
TDMG	Telemetric Data Monitor Group
TDRS	Tracking and Data Relay Satellite
TEA	Triethyl Aluminum
TEB	Triethyl Boron
TEGDN	Triethylene Glycol Dinitrate
TFE	Tetrafluoroethylene polymer
TIU	Titan Interface Unit
TLV	Threshold Limit Value
TLV-TWA	Threshold Limit Value-Time Weight Average
TM	Thruster Modules
TMETN	Trimethylolethane Trinitrate (see METN)
TNT	2,4,6-trinitrotoluene, Trinitrotoluene
TOA	Time-Of-Arrival
TOPS	Transistorized Operational Phone System
TPS	Thermal Protection System
TSPC	Tank Shutoff Pilot Valve
TT&C	Telemetry, Tracking and Command
TTC	Telecommunications, Tracking and Command
TV	Television
TVC	Thrust Vector Control
TWA	Time Weight Average
TWTA	Traveling Wave Tube
UDMH	Unsymmetrical Dimethylhydrazine
UEL	Upper Explosive Limit
ULS	Ulysses Mission
UN	United Nations
USAF	United States Air Force
USCG	US Coast Guard
USEP	Ulysses Separation
USN	United States Navy
UT	United Technologies
UTC	United Technology Company
UVS	Ultraviolet Spectrometer
V&VSS	Verification and Validation Simulator Software
VAFB	Vandenberg Air Force Base
VECO	Vernier Engine Cutoff
VHPS	Vernier Hydraulic Power Supply
VRM	Vehicle Response Mode
VSS	Validation Simulator Software
WCP	Wing Command Post
XDT	See Glossary

4.0 SPHAM CONVERSION FACTORS

	Given	Multiply By	To Get
Mass	lb	0.4536	kg
	kg	2.2046	lb
Length	meters	3.2808	ft
	ft	0.3048	meters
Velocity	m sec^{-1}	3.2808	ft sec^{-1}
	f sec^{-1}	0.3048	m sec^{-1}
Force	kg m sec^{-2} (newton)	0.2248	lb_f
	lb_f	4.4482	kg m sec^{-2}
Pressure	atm	760	mm Hg
	mm Hg	1.316×10^{-3}	atm
	psia	0.1450	KPa
	atm	14.696	psia
Density	kgm^{-3}	0.06243	lb_m ft^{-3}
	lb_m ft^{-3}	16.0184	kgm^{-3}
Energy	Cal	.2390	J
	J	4.184	Cal
Specific Impulse	lb_f S lbm^{-1}	1	S
	S	1	lb_f S lbm^{-1}
Mass Flowrate	lb_m sec^{-1}	0.4536	kg sec^{-1}
	kg sec^{-1}	2.2046	lb_m sec^{-1}
Volume	liter	3.785	gal.
	gal.	0.2642	liter
Power	KW	0.7457	h_p
	h_p	1.3410	KW

Temperature	$°C = 5/9\ (°F - 32)$ $°F = 9/5°C + 32$ $°K = °C = 273$
Gas Constant	$R = 8.314\ J\ (g\ mol\ k)^{-1}$ $= .08205\ lt\ atm\ (g\ mol\ k)^{-1}$ $= 1.987\ cal\ (g\ mol\ k)^{-1}$ $= 0.7302\ (atm)\ (ft)^3\ (lb\ mol\ R)^{-1}$ $= 10.73\ (psia)\ (ft)^3\ (lb\ mol\ R)^{-1}$ $= 1{,}545\ ft\ lb_f\ (lbm\ mol\ R)^{-1}$ $= 1.986\ Btu\ (lb\ mol\ R)^{-1}$ $= 83.14\ (cm^3\ bar)\ (g\ mol\ K)^{-1}$
Boltzmanns Constant:	$0.1713 \times 10^{-8}\ BTU/(ft^2 \cdot h \cdot °R^4)$ $4.88 \times 10^{-8}\ Kcal/(m^2 \cdot h \cdot °K^4)$ $5.67 \times 10^{-12}\ w/(Cm^2 \cdot g\ °K^4)$