National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas 77058

NSTS 22254
REVISION B
DECEMBER 30, 1993

REPLACES
NSTS 22254
REVISION A

SPACE SHUTTLE

METHODOLOGY FOR CONDUCT OF SPACE SHUTTLE PROGRAM HAZARD ANALYSES

REVISION LOG

REV LTR	CHANGE NO	DESCRIPTION	DATE
		BASELINE ISSUE (Reference: Level II PRCBD S40163R1 dated 5/15/87)	05/20/87
A	1	REVISION A (Reference: Level II PRCBD S052342 dated 2/11/91)	04/30/91
B	4	REVISION B (Reference: SSP DOC–149, dated 11/5/93) also includes Space Shuttle PRCBD S052730A, SSP DOC–106 and Changes 2 and 3.	12/30/93

CHANGE SHEET

FOR

NSTS 22254 – Space Shuttle
Methodology for Conduct of Space Shuttle Program Hazard Analyses

CHANGE NO. 7

Program Requirements Control Board Directive No. S053983CKR1/(4–1), dated 2/2/00.(1)

February 24, 2000

Robert H. Heselmeyer
Secretary, Program Requirements
Control Board

CHANGE INSTRUCTIONS

1. Remove the following listed pages and replace with the same numbered attached pages:

Page	PRCBD No.
2–1	S053983CKR1
2–2	
4–1 – 4–5A	S053983CKR1
G–3	
G–4	S053983CKR1

NOTE: A black bar in the margin indicates the information that was changed.

2. Remove the List of Effective Pages, dated August 13, 1997 and replace with List of Effective Pages, dated February 24, 2000.
3. Sign and date this page in the space provided below to show that the changes have been incorporated and file immediately behind the List of Effective Pages.

_____ _____
Signature of person incorporating changes Date

NSTS 22254 – Space Shuttle
Methodology for Conduct of Space Shuttle Program Hazard Analyses

*Revision B (Reference PRCBD No. S052730A, dated 10/20/93; SSP DOC–106 and SSP DOC–149)

LIST OF EFFECTIVE PAGES

February 24, 2000

The current status of all pages in this document is as shown below:

Page No.	Change No.	PRCBD No.	Date
i – v	Rev. B	*	December 30, 1993
vi	5	S060425A	June 20, 1996
vii – viii	Rev. B	*	December 30, 1993
1–1 – 1–4	Rev. B	*	December 30, 1993
2–1	7	S053983CKR1	February 2, 2000
2–2	Rev. B	*	December 30, 1993
3–1 – 3–18	Rev. B	*	December 30, 1993
4–1 – 4–5A	7	S053983CKR1	February 2, 2000
4–5B	5	S060425A	June 20, 1996
4–6 – 4–12	Rev. B	*	December 30, 1993
4–13	5	S060425A	June 20, 1996
4–14 – 4–24	Rev. B	*	December 30, 1993
5–1 – 5–2	Rev. B	*	December 30, 1993
6–1 – 6–2	Rev. B	*	December 30, 1993
A–1 – A–10	Rev. B	*	December 30, 1993
B–1 – B–8	Rev. B	*	December 30, 1993
C–1 – C–20	Rev. B	*	December 30, 1993
D–1 – D–8	Rev. B	*	December 30, 1993
E–1 – E–8	Rev. B	*	December 30, 1993
F–1 – F–8	Rev. B	*	December 30, 1993
G–1 – G–2	Rev. B	*	December 30, 1993
G–3	5	S060425A	June 20, 1996
G–4	7	S053983CKR1	February 2, 2000
H–1 – H–6	Rev. B	*	December 30, 1993
H–7 – H–8	6	S052730C	July 23, 1997
H–9	5	S060425A	June 20, 1996
H–10	Rev. B	*	December 30, 1993

NSTS 22254

SPACE SHUTTLE

METHODOLOGY FOR CONDUCT OF SPACE SHUTTLE PROGRAM HAZARD ANALYSES

THIS PAGE INTENTIONALLY LEFT BLANK

FOREWORD

Efficient management of the Space Shuttle Program (SSP) dictates that effective control of program activities be established. Requirements, directives, procedures, interface agreements, and system capabilities shall be documented, baselined, and subsequently controlled by SSP management.

Program requirements controlled by the Director, Space Shuttle Operations, are documented in, attached to, or referenced from Volume I through XVIII of NSTS 07700.

This document is to provide the methodology required for the preparation of Space Shuttle Program hazard analyses, hazard reports, safety analysis reports, and Management Safety Assessment. It further defines and implements the safety requirements contained in NSTS 07700, Volume V, Information Management Requirement; Volume X, Space Shuttle Flight and Ground System Specification; Volume XI, System Integrity Assurance Program Plan; and System Safety Analysis, Section 1D201 of NHB 5300.4 (1D–2), Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program. This document provides definitive and common hazard identification, and standardized hazard analysis documentation for the Space Shuttle Program.

All elements of the SSP must adhere to these baselined requirements. When it is considered by the Space Shuttle Program element/project managers to be in the best interest of the SSP to change, waive or deviate from these requirements, an SSP Change Request (CR) shall be submitted to the Program Requirements Control Board (PRCB) Secretary. The CR must include a complete description of the change, waiver or deviation and the rationale to justify its consideration. All such requests will be processed in accordance with NSTS 07700, Volume IV, and dispositioned by the Director, Space Shuttle Operations, on a Space Shuttle PRCB Directive (PRCBD).

Brewster H. Shaw, Jr.
Director, Space Shuttle Operations

THIS PAGE INTENTIONALLY LEFT BLANK

CONTENTS

1.0 INTRODUCTION 1–1

1.1 PURPOSE 1–1

1.2 SCOPE 1–1

1.3 SAFETY HAZARD ANALYSIS REQUIREMENTS 1–2

1.4 HAZARD ANALYSES 1–2

1.5 FAULT TREE ANALYSES 1–2

1.6 HAZARD REDUCTION PRECEDENCE SEQUENCE 1–3

2.0 APPLICABLE DOCUMENTS 2–1

3.0 HAZARD ANALYSIS (HA) PREPARATION INSTRUCTIONS 3–1

3.1 PRELIMINARY HAZARD ANALYSIS (PHA) 3–3

3.1.1 Purpose 3–3
3.1.2 Description 3–3
3.1.3 Program Phase 3–4
3.1.4 Technique 3–4

3.2 SUBSYSTEM HAZARD ANALYSIS (SSHA) 3–5

3.2.1 Purpose 3–5
3.2.2 Description 3–5
3.2.3 Program Phase 3–5
3.2.4 Technique 3–5

3.3 SYSTEM HAZARD ANALYSIS (SHA) 3–6

3.3.1 Purpose 3–6
3.3.2 Description 3–7
3.3.3 Program Phase 3–7
3.3.4 Technique 3–7

3.4 OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA) 3–7

3.4.1 Purpose 3–7
3.4.2 Description 3–7
3.4.3 Program Phase 3–8
3.4.4 O&SHA Technique 3–8

4.0 HAZARD REPORTS 4–1

4.1 PURPOSE 4–1

4.1.1 Standardized Data Elements 4–1

CONTENTS

4.2 MAINTAINING HAZARD REPORTS CURRENT 4–1

4.3 HAZARD REPORT APPROVAL AND PROCESSING 4–2

4.3.1 Procedure for Processing New HRs or Increase in Risk HRs 4–2

4.4 MISSION–BY–MISSION SAFETY ASSESSMENT 4–3

4.4.1 Determination of Mission Effectivity 4–4

4.4.2 Safety Issue Briefings 4–4

4.5 CHANGE TO BASELINED HAZARD REPORTS THAT DO NOT REFLECT AN INCREASE IN RISK 4–5

4.6 HAZARD REPORT DATA ELEMENTS 4–5B

4.6.1 Part I of the HR 4–5B

4.6.2 Part II of the HR 4–6

4.6.3 Part III of the HR 4–10

4.6.4 Part IV of the HR 4–11

4.7 PROGRAM 4–12

5.0 MANAGEMENT SAFETY ASSESSMENT (MSA) 5–1

5.1 PURPOSE 5–1

5.2 SCOPE 5–1

5.3 APPROACH 5–1

5.4 RESPONSIBILITIES 5–2

6.0 SAFETY ANALYSIS REPORT (SAR) 6–1

APPENDICES

A	FAULT TREE ANALYSIS	A–1
B	SNEAK ANALYSIS	B–1
C	SOFTWARE HAZARD ANALYSIS	C–1
D	COMMON CAUSE FAILURE ANALYSIS	D–1
E	SAFETY ANALYSIS REPORT (EXAMPLE)	E–1
F	GLOSSARY OF TERMS	F–1
G	ACRONYMS AND ABBREVIATIONS	G–1
H	DATA FIELD DESCRIPTIONS	H–1

FIGURES

3–1 SPACE SHUTTLE PRELIMINARY HAZARD ANALYSIS (PHA) INSTRUCTIONS 3–11

3–2 LIST OF GENERIC HAZARDS 3–13

3–3 SPACE SHUTTLE SUBSYSTEM HAZARD ANALYSIS (SSHA) INSTRUCTIONS* 3–15

3–4 SPACE SHUTTLE OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA) INSTRUCTIONS 3–17

4–1 HAZARD REPORT APPROVAL PROCESS 4–13

4–2 SSP HAZARD REPORT EXECUTIVE SUMMARY 4–15

4–3 SSP HAZARD REPORT (Part I) 4–19

4–3 SSP HAZARD REPORT (Part II) 4–20

4–3 SSP HAZARD REPORT (Part III) 4–21

4–3 SSP HAZARD REPORT (Part IV) 4–22

4–4 RISK MATRIX TEST FOR AGREEMENT BETWEEN CLOSURE CLASSIFICATION AND RISK 4–23

4–5 SAMPLE COMPLETED RISK MATRIX 4–24

A–1 SUGGESTED FAULT TREE SEGMENTS A–7

A–2 FAULT TREE SYMBOLS A–8

A–3 LOGIC SYMBOLS LEGEND A–9

A–4 SAMPLE SYSTEM FAULT TREE A–10

B–1 BASIC TOPOGRAPHS B–7

B–2 SAMPLE SNEAK CIRCUIT REPORT B–8

C–1 INADVERTANT RCS JET FIRING SOFTWARE FAULT TREE C–15

C–2 CRITICAL FUNCTION TABLE C–16

C–3 SYSTEM/SUBSYSTEM DEFINITION C–17

C–4 SOFTWARE STIMULI WORKSHEET C–18

C–5 SOFTWARE MEASUREMENTS WORKSHEET C–19

D–1 COMMON CAUSE FAILURE ANALYSIS FLOW D–7

D–2 CCFA TRACKING AND RESOLUTION FORMAT D–8

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide the methodology required for the preparation of Space Shuttle Program Hazard Analyses, Hazard Reports (HRs), Safety Analysis Reports (SARs), and the Management Safety Assessment (MSA). It further defines and implements the safety requirements contained in NSTS 07700, Volume V, Information Management Requirements; Volume X, Space Shuttle Flight and Ground System Specifications; Volume XI, System Integrity Assurance Program Plan; and System Safety Analysis Section 1D201, of NHB 5300.4(1D–2), Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program (SSP). This document provides definitive and common hazard identification, and standardized Hazard Analysis (HA) methodology for the SSP. NSTS 07700, Volume XI, System Integrity Assurance Program Plan, implements NSTS 08216, Program Compliance Assurance and Status System (PCASS) Development Plan, which requires that all data contained in HRs be included in the PCASS data base. This data base provides a HR format which contains the minimum data items that are required for the SSP (reference Section 4.0).

1.2 SCOPE

The implementation of the tasks described herein is the responsibility of the Space Shuttle Program Systems Integration Office and the Integration Contractor, and the Space Shuttle Program Element Projects and their contractors. Included are current and proposed Shuttle elements, Contractor Furnished Equipment (CFE), Government Furnished Equipment (GFE), and Ground Support Equipment (GSE) used at or common to the launch sites and which interface with flight hardware at launch and landing facilities. This includes launch and landing site facility items such as crane lifts that interface and operate around flight hardware. Orbiter Experiments (OEX) Detailed Test Objectives (DTOs) involving flight hardware and Detailed Secondary Objectives (DSOs) are also included.

HA requirements are contained in Paragraph 1.4, and descriptions of HA methodologies to be applied are contained in Section 3.0. Additional HA techniques that may be used for conducting HAs at the discretion of the program and project offices include Fault Tree Analysis (Appendix A), Sneak Analysis (Appendix B), Software Hazard Analysis (Appendix C), and Common Cause Failure Analysis (Appendix D).

The HR data elements contained in Section 4.0 are applicable to all new and revised HRs submitted after release of Revision A of NSTS 22254.

Industrial safety assessments, including research and development and manufacturing activities need not be baselined at the Configuration Control Board (CCB) or Program

Requirements Control Board (PRCB). They are the responsibility of the center director where they apply.

HAs shall address design and operational hazards associated with hardware, software, operations, and environments.

Payload organization HA requirements are contained in NSTS 1700.7, Safety Policy and Requirements for Payloads. Payloads using the Space Shuttle will continue to be controlled by NSTS 1700.7.

1.3 SAFETY HAZARD ANALYSIS REQUIREMENTS

NHB 5300.4 (1D–2) requires that HAs be performed to identify hazards and that a closed–loop system be used to assure resolution of the hazards. NSTS 07700, Volume X, Space Shuttle Flight and Ground System Specifications, imposes Safety Analysis (SA) requirements on the SSP to be implemented by program integration and each element project. NSTS 07700, Volume V, Information Management Requirements, specifies what is to be delivered to the Space Shuttle Program Office for approval or as information. The audit provision imposed is to assure all supporting data will be available to demonstrate the depth, completeness, and accuracy of HAs performed.

1.4 HAZARD ANALYSES

The program office and element projects shall perform or ensure that the contractor performs the required SAs to identify hazards and ensure their resolution. The specified HA techniques to be employed as a minimum are detailed in Section 3.0 with optional additional analysis techniques described in the appendices. In addition to those elements specified in 1D200.3 and 1D201.5 of NHB 5300.4 (1D–2), the software, hardware, operations, and natural and induced environments must be considered.

1.5 FAULT TREE ANALYSES

Fault Tree Analyses (FTAs) or equivalent logic analyses are preferred for evaluating the effects of individual and multiple hardware and software faults, interfaces, environmental conditions, and human error on the system. The top–level fault tree will be based on the top undesired event, “loss of vehicle/personnel during Space Shuttle mission.” The top–level fault tree will be developed to identify program operation phases and the mission phases as they relate to the top undesired event. The mission phase events will be based on preliminary HAs, Subsystem Hazard Analyses (SSHAs), System Hazard Analyses (SHAs), Operating and Support Hazard Analyses (O&SHAs), and any other analyses, such as reliability analyses (i.e., Failure Modes and Effects Analyses [FMEAs]), which will support the further development of the detailed trees. For new projects/programs, use of FTAs will support the identification of hazards in the

design process and should be part of the Preliminary Design Review (PDR) and Critical Design Review (CDR) deliverable HA.

1.6 HAZARD REDUCTION PRECEDENCE SEQUENCE

The actions to eliminate or control hazards shall be as specified in 1D201.6 of NHB 5300.4 (1D–2). The hazard reduction precedence sequence is as follows:

a. Design for Minimum Hazard. The major goal throughout the design phase shall be to ensure inherent safety through the selection of appropriate design features as fail–operational/fail–safe combinations and appropriate safety factors. Hazards shall be eliminated by design where possible. Damage control, containment, and isolation of potential hazards shall be included in design considerations.

b. Safety Devices. Known hazards which cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment.

c. Warning Devices. Where it is not possible to preclude the existence or occurrence of a known hazard, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application shall be designed to minimize the probability of wrong signals or of improper personnel reaction to the signal.

d. Special Procedures. Where it is not possible to reduce the magnitude of existing or potential hazards through design, or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations shall be standardized.

THIS PAGE INTENTIONALLY LEFT BLANK

2.0 APPLICABLE DOCUMENTS

The following documents of the date and issue shown form a part of this document to the extent specified herein. "(Current Issue)" is shown in place of a specific date and issue when the document is under Space Shuttle PRCB control. The current status of documents shown with "(Current Issue)" may be determined from NSTS 08102, Program Document Description and Status Report.

NSTS 07700, Volume IV (Current Issue)	Configuration Management Requirements Ref. Foreword; Para. 3.0, 4.2
NSTS 07700, Volume V (Current Issue)	Information Management Requirements Ref. Foreword; Para. 1.1, 1.3, 3.0, 4.1, 4.3.1, 4.4.1, 4.4.2, 4.5
NSTS 07700, Volume X (Current Issue)	Space Shuttle Flight and Ground System Specification Ref. Foreword; Para. 1.1, 1.3
NSTS 07700, Volume XI (Current Issue)	System Integrity Assurance Program Plan Ref. Foreword; Para. 1.1
NSTS 08080–1 (Current Issue)	Manned Spacecraft Criteria and Standards Ref. Para. 3.2.4
NSTS 08216 (Current Issue)	Space Shuttle Program Compliance Assurance and Status System Development Plan Ref. Para. 1.1
NSTS 22973	Management Safety Assessment For Space Shuttle Program Ref. Para. 5.0, 5.4

NHB 1700.1 (V1–A)	Basic Safety Manual Ref. Apx. F
NHB 5300.4(1D–2)	Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program Ref. Foreword; Para. 1.1, 1.3, 1.4, 1.6, 4.6.2; Apx. F
NSTS 1700.7	Safety Policy and Requirements for Payloads Para. 1.2, Fig. 4–1
NUREG–0492	Fault Tree Handbook Ref. Apx. A, Para. 4.0
DOD–HDBK–217	Reliability Prediction for Electronic Parts Ref. Apx. A, Para. 4.0

3.0 HAZARD ANALYSIS (HA) PREPARATION INSTRUCTIONS

Preparation of HAs will begin at the concept phase of a program or program item to evaluate different concepts and develop appropriate safety requirements for early risk management decisions. The analysis shall identify causes down to the level at which controls are to be applied. All hazards including those resulting from failures, regardless of subsystem or component redundancy, shall be analyzed. In addition to hazards resulting from failures, those emanating from normal or emergency equipment operations, environment, personnel error, design characteristics, and credible accident scenarios shall be analyzed. Hazards resulting from failure to meet program requirements and Single Failure Points (SFPs) will be identified.

The analysis shall identify the necessary actions to eliminate or control any failures or malfunctions that could independently or collectively present a hazard to interfacing hardware (e.g., facility to flight hardware, GSE to flight hardware, element to element, element to cargo). Individual causes shall be listed along with the controls which are applied to those causes. For Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) items, a summary of the causes leading to the hazardous condition (failure mode) may be provided at the failure mode level; however, each HA unique cause will be itemized individually.

Control and verification summaries will include sufficient detail/explanation of testing, inspection, and/or analysis to clearly reflect critical controls which mitigate the hazard and support hazard closure or risk acceptance rationale. Interface hazards outside of element–sustaining engineering will be identified to the System Safety Review Panel (SSRP) for formal intercenter coordination/ resolution. Integrated HRs will document inter–element hazards and ensure that element hazards properly address the controls necessary for safe integrated operation.

Hazardous functions will be identified, and software which controls hazardous functions, or which generates information upon which decisions to control hazardous functions are made, will be analyzed to ensure the system operates at an acceptable risk level.

A fault tree (reference Appendix A) or similar logic analysis shall be developed to aid in the identification of all hazards. The logic analysis shall have sufficient detail to provide a positive trail from the top–level hazard event down to the cause level at which controls must be applied, including FMEA failure modes and CIL failure causes. Traceability to FMEA/CIL failure mode/cause numbers must be provided. Hazard control verification will be accomplished and maintained by the project office for all hazard causes identified in the logic analysis. The logic analysis shall be completed prior to the preparation of the HRs.

Since the SSP is a mature program, the element projects have the flexibility to identify the specific types of analyses required to achieve the desired results.

It is recommended that the Preliminary Hazard Analyses (PHAs) be used to develop the requirements for new procurements while developing the statement of work or procurement specification for new hardware for the program. Completion is required in support of the PDR to verify that the technical safety requirements have been incorporated into the preliminary design of the item for procurement. It can be updated as the design progresses, but most likely a transition to the SSHA and SHA will be desired.

The SSHA section of the overall HA is recommended when design data starts to become available for the PDR and updated throughout the design and development phase to provide inputs to the design and operations activities for control of identified hazardous conditions. The PHA should identify areas requiring a SSHA. Significant design changes, operational failures, problems, or human factors could be a reason for updating the analysis. The SHA is recommended for combining the SSHAs to a higher level. It has been previously referred to as an integrated HA on the SSP. The initial release should be completed to support the CDR phase. At that development phase, the PHA, SSHA, and other data sources are available to identify interacting and operational type hazardous conditions that require resolution. The SHA and SSHA should be continually updated to reflect changes that may be incorporated by operations, software, or hardware design changes or new or modified environmental conditions.

The O&SHA is recommended to support all phases of hardware manufacturing, mission use, and reuse operations. Proper conduct of this analysis should identify hazardous conditions to personnel through all ground and flight phases, and potential damage to the hardware induced from processes and procedures that could later impact system operation. The O&SHA is performed using all previous HAs and operational concepts/planning as prime inputs.

The long–term nature of the SSP and the need to reuse hardware will result in the need for replacement units throughout the life of the program. These units may be new production of existing designs or new designs. The element project offices and their contractors are responsible for imposing the requirements necessary to ensure that production units include safety features designed into the previous units and that they do not introduce new hazards. If the unit is a redesign or a new design, these offices are responsible for imposing the appropriate requirements in the procurement contract to ensure that the new units are properly evaluated for hazards in accordance with the requirements of this document. For new procurements, all HA requirements apply and reports will be submitted to the SSP after the CDR.

NSTS 07700, Volume IV, Configuration Management Requirements, provides the requirements for HAs to be presented during program milestone reviews (e.g., PDR,

CDR). The level of the analysis shall be commensurate with the design completion. NSTS 07700, Volume V, Information Management Requirements defines the safety deliverables.

The reports prepared as the results of a specific HA are specified in Sections 4.0 and 6.0. Section 4.0 defines the minimum data element to be contained in the HRs. Section 6.0 defines the minimum data to be contained in the SAR. These data elements reflect the results of all the analyses performed and defines the integrated reporting required for submittal.

3.1 PRELIMINARY HAZARD ANALYSIS (PHA)

3.1.1 Purpose

The purpose of the PHA is to identify safety–critical areas, to identify and evaluate hazards, and to identify the safety design and operations requirements needed in the program concept phase. The PHA provides management with knowledge of potential risks for alternative concepts during feasibility studies and program definition activities.

3.1.2 Description

The PHA is performed to document an initial risk assessment of a concept or system. It is based on the best available data, including mishap data from similar systems, and lessons learned from other programs. The hazards associated with the proposed design or function are identified and evaluated for potential hazard severity, probability, time of exposure, and hazard classification. Design controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level shall be considered and documented. The PHA provides consideration of the following, as a minimum, for identification and evaluation of hazards:

a. Hazard sources (e.g., propellants, lasers, explosives, toxic substances, corrosives, hazardous construction materials, pressure systems, and other energy sources).

b. Safety–related interface considerations among various elements of the system, facilities, and GSE (e.g., material compatibility, contamination, electro–magnetic interference, inadvertent activation, fire/explosion initiation and propagation, and hardware and software controls).

c. Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, confined spaces, fire, electrostatic discharge, lightning, electromagnetic environmental effects, and ionizing and non–ionizing radiation).

d. Operating, test, maintenance, and emergency procedures (e.g., human error analyses of operator functions, tasks, and requirements; ergonomics; effects of factors such as equipment layout and lighting requirements; effects of noise or radiation on human performance; life support requirements and their safety implications in manned systems; crash safety; egress; rescue; survival; and salvage).

e. Facilities, support equipment (e.g., provisions for storage, disposal, assembly, checkout, proof–testing of hazardous systems/assemblies which may include toxic, flammable, explosive, corrosive or cryogenic fluids; radiation or noise emitters; and electrical power source), and training (e.g., training and certification pertaining to safety operations and maintenance).

f. Safety–related equipment, safeguards, and possible alternative approaches (e.g., monitoring, interlocks, system redundancy, hardware or software fail–operational/fail–safe design considerations, subsystem protection, fire detection/suppression systems, personal protective equipment, ventilation, and noise or radiation attenuation).

3.1.3 Program Phase

The PHA effort should be initiated during the initial concept phase of a program so that safety considerations are used to evaluate design alternatives and trade studies. The PHA should be used as the baseline for performing future analyses, such as the SSHA, SHA, and O&SHA. The PHA may be continued and updated during later phases.

3.1.4 Technique

The PHA information may be recorded in the form and content of the columnar matrix contained in Figure 3–1. The PHA format provides a systematic method for performing the analysis, has wide applicability, and provides documented evidence of the analytical procedure. Other aids, such as top–level fault trees, SAs, SHAs, FMEA/CILs, and safety checklists, may be used to identify hazardous conditions. The following steps are provided as a guide to assist the analyst and ensure the performance of a comprehensive PHA. Additional data elements may be added.

a. Data Accumulation. The safety analyst must be familiar with the conceptual system and its planned functions and interfaces. The analyst must accumulate and use data such as preliminary systems and mission descriptions, flow diagrams, design drawings, operational concepts/plans, related failure and flight anomaly reports, and other technical data as may be available.

b. Hazard Analysis. Having accumulated the necessary information, the safety analyst can make entries in the columnar matrix HA worksheet. The format

provides for hazardous conditions, hazard causes, hazard effect, severity level, safety requirements, hazard elimination/control provisions, verifications, and likelihood of occurrence. HA worksheet instructions are provided in Figure 3–1. Checklists are also provided in Figure 3–2, which will be helpful as a guide throughout the analysis.

3.2 SUBSYSTEM HAZARD ANALYSIS (SSHA)

3.2.1 Purpose

The purpose of a SSHA is to identify hazards to personnel, vehicle, and other systems. The hazards may be caused by loss of function; accidental activation; energy source; hardware failures; personnel actions or inactions; software deficiencies, interaction of components within the subsystem, inherent design characteristics such as sharp edges and incompatible materials; and environmental conditions such as dust, radiation, and sand.

3.2.2 Description

The SSHA defines the safety–critical functions, component fault conditions, generic hazards, safety–critical operations and environments associated with the subsystem under the column heading “Hazardous Condition”. This approach allows use of the same form for the PHA, SSHA, and SHA. Separately addressing all four hazardous conditions (generic hazards, safety–critical component fault conditions, safety–critical operations, and environment) for each SSHA provides a better opportunity to identify all hazardous conditions.

3.2.3 Program Phase

The SSHA effort should begin when the preliminary design and concept definition are established and progress through the detailed design of components, equipment, and software. The SSHA shall be updated as the result of any subsystem design change, new or modified hardware, and analyses of appropriate hardware and software failure history documented during the ongoing program activity.

3.2.4 Technique

A similar columnar matrix is used for the SSHA (Figure 3–3) as is used for the PHA. The approach for SSHA is to:

a. First identify the hazardous conditions from the list of generic hazards (the first of the four hazardous conditions to be addressed) in Figure 3–2 and then determine the causes that generate each hazardous condition listed. The

causes will be from (1) hardware failure modes, (2) personnel actions or inaction, (3) software deficiency(ies), (4) component interactions, and (5) environmental condition(s) (induced or natural). This should include energy sources and operating conditions. After completing the hazardous condition and hazard causes columns, the hazard effect, severity level, safety requirements, hazard elimination/control provisions, verifications, and likelihood of occurrence columns should be completed.

b. Identify the hazardous condition associated with safety–critical component fault condition number one. List the failure mode(s) under hazard causes considering (1) hardware design; (2) personnel action(s)/interaction(s) that can cause the failure mode(s); (3) software deficiency(ies) that can cause the failure modes; (4) interaction(s) with other component(s) that can cause the failure modes; (5) environmental condition that can cause the failure mode; and (6) manufacturing and processing–induced condition(s) that can cause the failure mode.

c. List the hazardous conditions associated with safety–critical operations (functions) associated with the subsystem considering all use phases such as manufacturing, servicing, refurbishment, and in use, considering items (1) through (6) in Subparagraph b. above.

d. List the environmental hazards, such as sunspot radiation, that may cause system loss, hardware damage, or personnel injury/death.

The common cause failure conditions that may cause hazardous conditions are identified in the FMEA/CIL Criticality 1 and 1R items. Revisions to the FMEA process now require an evaluation of the common cause conditions in NSTS 08080–1, Manned Spacecraft Criteria and Standards. This aspect of the CIL items (1 and 1R) should be evaluated for additional hazardous conditions and subjected to an end–to–end analysis.

3.3 SYSTEM HAZARD ANALYSIS (SHA)

3.3.1 Purpose

The purpose of the SHA is identical to the SSHA, but at the system level. Once the subsystem levels have been established, a combination of subsystems make up a system. In turn, a group of systems may compose another system until the top system is identified. Consequently, a system to one project may be a subsystem to another project.

3.3.2 Description

The SHA accomplishes the same purpose as the SSHA, but at a higher level. In general, the previous analyses are extended to encompass the total system. The unique aspect of the SHA is its view of interfaces between subsystems which make up a system. Hence, it is a form of an integrated HA.

3.3.3 Program Phase

The SHA effort shall begin as a system and subsystem design, and interfaces, including software, are defined. The SHA shall be updated when needed as a result of system design, or interface changes, failure reports, and flight anomaly reports.

3.3.4 Technique

The SHA uses the same technique as previously described in Paragraph 3.2.4, technique for the SSHA, except at a higher level.

3.4 OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA)

3.4.1 Purpose

The purpose of an O&SHA is to identify hazards and recommend risk reduction alternatives in procedurally controlled activities during all phases of intended system/hardware/facility use.

3.4.2 Description

The O&SHA is performed to examine procedurally controlled activities. It identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons and equipment and considers (1) the planned system configurations at each phase of activity; (2) the facility interfaces; (3) the planned environments; (4) the supporting tools or other equipment specified in use; (5) the operation or task sequence, concurrent or parallel task effects, and limitations; (6) the biotechnological factors; (7) the regulatory or contractually specified personnel safety and health requirements; and (8) the potential for unplanned events, including hazards introduced by human error. The O&SHA identifies the safety requirements and controls needed to eliminate or control identified hazards, or to reduce the associated risk to an acceptable level. The analysis should identify:

a. Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risks during these activities. These activities must be analyzed to provide preventive measures to reduce the hazard to an acceptable level.

b. Changes needed to support functional or design requirements for system hardware and software, facilities, tooling, or support/test equipment to eliminate hazards or reduce associated risks. These changes must be analyzed to verify effectiveness of implementation.

c. Requirements for safety devices and equipment, including personnel safety and life–support equipment, must be identified.

d. Requirements for warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render–safe, and backout) must be specified and provided.

e. Requirements for handling, storage, transportation, maintenance, and disposal of hazardous materials must be analyzed and proper requirements and procedures implemented.

f. Potentially hazardous conditions that may be induced into flight hardware during manufacturing, test, inspections, etc., and show up later during flight hardware/software end use. These conditions must be analyzed and appropriate mandatory verification points implemented. (Included are such items as poor welding, unidentified hardware failures, x–ray effects on electronics, and contaminated fuel.)

g. Requirements for safety training and personnel certification. The O&SHA documents system safety assessments of procedures involving system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, and disposal.

3.4.3 Program Phase

The O&SHA effort should be conducted in parallel with development of procedures for manufacturing, processing, and operation. The O&SHA shall be updated, when needed, as a result of any system change, design change, procedure change, operational change, accident/incident report, and operational anomaly report.

3.4.4 O&SHA Technique

An O&SHA columnar format and recommended content are shown in Figure 3–4. This format is designed with the intent of establishing a systematic method whereby operations are broken down into incremental parts and consistently analyzed for hazards. The O&SHA form should be modified to the specific needs of the user. O&SHA hazards can be recognized through checklists by comparing the configuration of the operation being analyzed (hardware, tasks, sequences, tools, environment, etc.) against the hazardous elements and hazardous conditions on the checklists. Operational elements that correlate with items on the checklist can indicate a potential hazard

or a potentially safety–critical area. Again, note the similar content (additional information is required in the heading) and form of the O&SHA. This allows comparisons with the PHA, SHA, and SSHA.

THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE 3–1

SPACE SHUTTLE PRELIMINARY HAZARD ANALYSIS (PHA) INSTRUCTIONS

PHA NO: _____

MISSION PHASE: Flight Operations, Mission Operations, Turnaround, Etc. ENGINEER: _____

SUBSYSTEM OR OPERATION: Identify EPS, ECLSS, GN&C, Etc. DATE: 06/30/86

EFFECTIVITY: Ascent, On–Orbit, Entry, Approach and Landing Turnaround SHEET 1 of 1

HAZARDOUS CONDITION	HAZARD CAUSES	HAZARD EFFECT	SEVERITY LEVEL	SAFETY REQUIRE–MENTS	HAZARD ELIMINATION/ CONTROL PROVISIONS	VERIFICATIONS	LIKELIHOOD OF OCCURRENCE
Use the checklist below to identify potentially haz-ardous conditions. 1. Can the system/ subsystem fail to operate as intended? 2. Can the system/ sub–system operate inadvertently (untimely)? 3. Are there generic haz–ards? (See Figure 3–2) Record the identi-fied hazards.	Enter brief description of how each hazardous condition is created, i.e., rupture of the O_2 tank; wiring insulation overheating and igniting; etc.	Record the potential effect of each hazardous condition on critical equipment, personnel or the general public, i.e., loss of vehicle; emergency landing in inhabited area; etc.	Identify the severity level as one of the following for each hazardous condition: CA – Catastrophic (see glossary) CR – Critical (see glos-sary) MR – Marginal (see glos-sary)	Identify the existing or proposed safety requirement that will eliminate or control the hazardous condition by document and paragraph number.	Identify proposed hazard reduction methods for open hazards and implemented reduction methods for controlled hazards.	Identify the methods used to verify the hazard controls. Include sufficient detail/explanation of testing, inspection, and analysis which mitigate the hazard and support hazard closure or risk rationale. Verification methods include analyses, tests, inspections, and operations and maintenance requirements. Identify the verification reference by document number and title.	Assess the controls that are in place and classify them as one of the following: Probable; Infrequent; Remote; or Improbable.

THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE 3–2

LIST OF GENERIC HAZARDS

(Page 1 of 2)

GENERIC HAZARD	GENERIC HAZARD TYPE
I. CONTAMINATION/CORROSION	A. CHEMICAL DISASSOCIATION B. CHEMICAL REPLACEMENT/COMBINATION C. MOISTURE D. OXIDATION E. ORGANIC (FUNGUS/BACTERIAL, ETC.) F. PARTICULATE
II. ELECTRICAL DISCHARGE/SHOCK	A. EXTERNAL SHOCK B. INTERNAL SHOCK C. STATIC DISCHARGE D. CORONA E. SHORT
III. ENVIRONMENTAL/WEATHER	A. FOG B. FUNGUS/BACTERIAL C. LIGHTNING D. PRECIPITATION (RAIN/SNOW/SLEET/HAIL) E. SOLAR/COSMIC RADIATION F. SAND/DUST G. VACUUM H. WIND I. TEMPERATURE EXTREMES
IV. FIRE/EXPLOSION	A. CHEMICAL CHANGE (EXOTHERMIC/ENDOTHERMIC) B. FUEL AND OXIDIZER IN PRESENCE OF PRESSURE AND IGNITION SOURCE C. PRESSURE RELEASE/IMPLOSION D. HIGH HEAT SOURCE
V. IMPACT/COLLISION	A. ACCELERATION (INCLUDING GRAVITY) B. DETACHED EQUIPMENT C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL D. METEOROIDS/METEORITES E. MOVING/ROTATING EQUIPMENT

FIGURE 3–2

LIST OF GENERIC HAZARDS

(Page 2 of 2)

GENERIC HAZARD	GENERIC HAZARD TYPE
VI. LOSS OF HABITABLE ENVIRONMENT	A. CONTAMINATION B. HIGH PRESSURE C. OXYGEN CONTENT D. LOW PRESSURE E. TOXICITY F. LOW TEMPERATURE G. HIGH TEMPERATURE
VII. PATHOLOGICAL/PHYSIOLOGICAL/ PSYCHOLOGICAL	A. ACCELERATION/SHOCK/IMPACT/VIBRATION B. ATMOSPHERIC PRESSURE (HIGH, LOW, RAPID CHANGE) C. HUMIDITY D. ILLNESS E. NOISE F. SHARP EDGES G. SLEEP, LACK OF H. VISIBILITY (GLARE, WINDOW/HELMET FOGGING) I. TEMPERATURE J. WORKLOAD, EXCESSIVE
VIII. RADIATION	A. ELECTROMAGNETIC B. RADIOACTIVE ELEMENT
IX. TEMPERATURE EXTREMES	A. HIGH B. LOW C. VARIATIONS

FIGURE 3–3

SPACE SHUTTLE SUBSYSTEM HAZARD ANALYSIS (SSHA) INSTRUCTIONS*

(Page 1 of 2)

SSHA NO: _____

MISSION PHASE: Launch Through Landing ENGINEER: _____

SUBSYSTEM OR OPERATION: Identify EPS, ECLSS, GN&C, Etc. DATE: 06/30/86

EFFECTIVITY: All Flights SHEET 1 of 2

HAZARDOUS CONDITION	HAZARD CAUSES	HAZARD EFFECT	SEVERITY LEVEL	SAFETY REQUIREMENTS	HAZARD ELIMINATION/ CONTROL PROVISIONS	VERIFICATIONS	LIKELIHOOD OF OCCURRENCE
I. Hazard #1 (Generic) Note: (See Figure 3–2 for complete list)	A. Hardware failure mode(s). B. Personnel action(s) or inter-action(s). C. Software deficiency(ies) D. Component interaction(s) E. Environmental condition(s)	**	**	**	**	**	**
II. Safety–Critical component fault condition #1 Hazardous condition(s)	Failure Mode 1, Failure Mode 2, etc. 1. Personnel action(s)/ interaction(s) that can cause above failure modes 2. Software deficiency(ies) that can cause above failure modes	**	**	**	**	**	**

* Same for SHA with different title

** See Figure 3–1 for instructions

FIGURE 3–3

SPACE SHUTTLE SUBSYSTEM HAZARD ANALYSIS (SSHA) INSTRUCTIONS*

(Page 2 of 2)

SSHA NO: _____

MISSION PHASE: Launch Through Landing ENGINEER: _____

SUBSYSTEM OR OPERATION: Identify EPS, ECLSS, GN&C, Etc. DATE: 06/30/86

EFFECTIVITY: All Flights SHEET 2 of 2

HAZARDOUS CONDITION	HAZARD CAUSES	HAZARD EFFECT	SEVERITY LEVEL	SAFETY REQUIREMENTS	HAZARD ELIMINATION/ CONTROL PROVISIONS	VERIFICATIONS	LIKELIHOOD OF OCCURRENCE
	3. Interaction(s) with other compo-nent(s) that can cause above failure mode 4. Environmental condition that can cause failure mode 5. Manufacturing and processing induced condition(s) that can cause above failure mode	**	**	**	**	**	**
III. Safety Critical Operation #1 Hazardous Condition(s)	Same as above	**	**	**	**	**	**
IV. Environment #1 Hazardous Condition(s)	Same as above	**	**	**	**	**	**

* Same for SHA with different title

** See Figure 3–1 for instructions

FIGURE 3–4

SPACE SHUTTLE OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA) INSTRUCTIONS

O&SHA NO. _____
OPERATION: _____
TASK: _____
SUBTASK: _____
STEP: _____

ENGINEER: _____
DATE: _____

CRITERIA/CONSTRAINTS/ENERGY SOURCES: (Identify operational constraints and criteria such as: voltage levels, pressure ranges, and frequency. Identify presence and quantities of energy sources such as fuels, propellants, pressure vessels explosives.)

SHEET 1 of 1

HAZARDOUS CONDITION	HAZARD CAUSES	HAZARD EFFECT	SEVERITY LEVEL	SAFETY REQUIREMENTS	HAZARD ELIMINATION/ CONTROL PROVISIONS	VERIFICATIONS	LIKELIHOOD OF OCCURRENCE
Describe the hazard created by or during the operation.	Describe the mode(s) of failure or processing induced conditions. (Refer to SSHA instruc–tions)	Its potential effects or impact on personnel or equipment	Identify the severity level as one of the following for each hazardous condition. CA – Catastrophic (see glossary) CR – Critical (see glossary) MR – Marginal (see glossary)	Describe recommended measures for preventing, eliminating, or controlling the hazardous condition. Include guidelines, recommended design or operations requirements, and recommended further analyses.	Identify proposed hazard reduction methods for open hazards and implemented reduction methods for controlled hazards.	Identify the methods used to verify the hazard controls. Include sufficient detail/explanation of testing, inspection, and analysis which mitigate the hazard and support hazard closure or risk rationale. Verification methods include analyses, tests, inspections, and operations and maintenance requirements. Identify the verification reference by document number and title.	Assess the controls that are in place and classify them as one of the following: Probable; Infrequent; Remote; or Improbable.

One per page

THIS PAGE INTENTIONALLY LEFT BLANK

4.0 HAZARD REPORTS

Hazard Reports (HRs) are written to document hazardous conditions identified by the Space Shuttle Program HR originator/contractor HA process.

4.1 PURPOSE

The HR documents the identified hazardous condition and provides specific data element information that permits element project CCBs, Space Shuttle Program Office (SSPO), Integration Control Board (ICB), SSRP and PRCB technical management personnel to evaluate risk, and approve on the basis of documented rationale. HRs will be submitted in accordance with NSTS 07700, Volume V, Information Management Requirement 1SR–2, Table C.4.

4.1.1 Standardized Data Elements

All Space Shuttle Program projects, program elements, and contractors will use standardized HR data elements (see Paragraph 4.6, Figure 4–3, Parts I–IV, and Appendix H). Standardization of HR data element definitions and characteristics are required for automated Change Request (CR) processing.

These standardized data elements will be entered into Program Compliance Assurance and Status System (PCASS) and a standard HR format will be provided via PCASS.

4.2 MAINTAINING HAZARD REPORTS CURRENT

NSTS 07700, Volume IV, requires the originator of changes, waivers/deviations/Engineering Change Proposals (ECPs); i.e., Preliminary Interface Revision Notice (PIRN), Requirements Change Notice (RCN), Specification Change Notice (SCN), etc., to provide a safety impact assessment as part of the change package. Impact to baselined HR controls will be identified along with acceptance rationale. Any potential increase in HR baselined risk shall be identified. A change shall be considered to involve an increase in risk if any of the following is true:

a. The change introduces a new hazard or new hazard cause(s). This includes changes to the FMEA/CIL that involve a new critical failure mode or critical failure cause that are incorporated to HR(s) via reference.

b. The change eliminates or adversely affects previously defined hazard control or referenced CIL retention rationale.

c. The change invalidates previously identified hazard control or referenced CIL retention rationale verification data (e.g., thermal/structural analyses, tests, etc.).

d. The change reduces a margin of safety, even if the change still satisfies factor of safety requirements.

e. For any other reason, increases probability of a hazard or critical failure mode manifesting itself; or increases the consequences of a previously identified hazard, hazard cause, failure mode, or failure cause.

If the change resulted in an increase in risk but the HR remains valid as written, a presentation to the SSRP regarding the increased risk may be provided in lieu of an HR update.

4.3 HAZARD REPORT APPROVAL AND PROCESSING

4.3.1 Procedure for Processing New HRs or Increase in Risk HRs

HR changes required to reflect new hazards or increase in baselined risk shall be submitted on a SSP CR and approved in accordance with NSTS 07700, Volume V, Item 1SR–2, Table C.4. In all other cases or where the Space Shuttle Program Manager directs the update as a routine change, the HR will be updated as a Routine Update per NSTS 07700, Volume V, Item 1SR–2, Table C.4.

HRs will be processed as shown in Figure 4–1. The individual HRs must be processed and approved at the appropriate level CCB/ICB to assure management visibility and knowledge of hazardous conditions that could develop.

Project and program elements are responsible for verifying that all hardware, software, and operations used in the SSP have complied with safety requirements. The approval process is as follows:

a. HRs will be approved by the originator/contractor/project. The NASA project or program element CCB/ICB approval is required prior to submittal of the SSP CR. The ICB is considered the SSP equivalent responsible for approval of HRs from the integration contractor. Following CCB/ICB approval, the HRs are provided to SSP Management Integration Office via CR. In addition to the CR, a summary briefing should be made available for each HR. The briefing (Figure 4–2) will include the following:

    1. Identification of CR number and title

    2. HR number and title

    3. Hazardous conditions description

4. Identification of HR classification changes (is/was)

5. Description of and reason for change

b. SSP HRs CRs will be reviewed by the SSRP prior to their review by the PRCB. The SSRP will recommend which hazards require formal presentation to the Space Shuttle PRCB for approval, or processing outside the PRCB (OSB) for approval. OSB processing is authorized when:

1. The new hazard or increase in risk topic has previously been briefed to the Space Shuttle Program Manager through a Special PRCB, PRCB, Flight Readiness Review (FRR) or Program Mission Management Team (PMMT); or

2. The new hazard cause or increase in risk is classified as a controlled hazard.

Hazards with element–to–element interactions will be presented to the SSRP for formal intercenter coordination and resolution and tracked by the SSRP.

c. All open HRs will be forwarded for a status through each level. Open HRs are those hazards on which corrective action to eliminate or control the hazard has not been completed and the corrective action is not scheduled to be performed. The status shall remain open until management has reviewed the actions taken and accepted the safety risk.

d. Upon approval of the CR, a PRCB directive will be issued to complete SSRP and PRCB action items. Upon closure of all SSRP and PRCB actions, the directive also requires an update to PCASS.

4.4 MISSION–BY–MISSION SAFETY ASSESSMENT

When preparing for each mission, the project element contractors and centers shall review all program and project changes to ensure all baselined HRs are current and technically correct for the upcoming mission. Evaluation will include project and SSP actions (end item specification waivers and exceptions, FMEA/CIL changes, Criticality 1 Change Action Request (CAR) review, crew procedure CRs, flight rule CRs, Operational Maintenance Requirements and Specifications Document (OMRSD) waivers/exceptions, OMRSD changes (RCN), launch commit criteria changes (LCN), software changes, element configuration changes, element In–flight Anomalies (IFAs), flow Problem Reports (PRs) and Interim Problem Reports (IPRs), unexplained anomalies, mission changes, GIDEP alerts/NASA TWX reviews, payload–specific integration issues, SSP test data, or countdown anomalies) and test results/failures/successes (qualification, certification, fleet leader, green run, etc.). There is a need to update the

HR if program and project changes and/or changes to the flight and test experience base have resulted in a risk increase as identified in Paragraph 4.2. Other changes to baselined HR will be submitted as a “Routine Update” document (no SSP CR required) as directed by the project or program element.

4.4.1 Determination of Mission Effectivity

a. Single mission effectivity items do not require HR updates, but must be presented to the SSRP and PRCB as Safety Issue Briefing.

b. Multi–mission items which require HR updates shall be submitted in accordance with NSTS 07700, Volume V, IR 1SR–2.

4.4.2 Safety Issue Briefings

If there is adequate time for submittal preparation, then updates required to reflect an increase in baselined risk are submitted on an SSP CR to the SSP Management Integration Office 30 days prior to the FRR, to allow review by the SSRP and subsequent presentations to the Space Shuttle PRCB as deemed necessary by the SSRP. For those mission–by–mission safety assessment items which do not have adequate time for an HR update, a limited flight effectivity waiver may be granted to NSTS 07700, Volume V, IR 1SR–2 without all the required documentation. This CR shall be presented to the SSRP for review and forwarded to the Space Shuttle PRCB for approval. A subsequent CR, containing appropriate program documentation and requesting formal program approval for additional flight effectivities, shall be processed through the PRCB if waiver effectivity was limited.

The NSTS 07700, Volume V waiver CR shall be accompanied by a Safety Issue Briefing which shall include as a minimum:

a. Description of the issue

b. HRs impacted (number and title)

c. Closure classification(s)

d. Description of impact to HR

   1. Causes

   2. Controls

   3. Verifications

   4. Risk acceptance rationale

e. Recommendations on HR updates and associated schedules

The SSRP will recommend presenting the Safety Issue Briefing to the PRCB when:

a. The new hazard or increase in risk topic has not previously been briefed to the Space Shuttle Program Manager through a Special PRCB, PRCB, FRR, PMMT; or

b. The new hazard cause or increase in risk is classified as an accepted risk.

4.5 CHANGE TO BASELINED HAZARD REPORTS THAT DO NOT REFLECT AN INCREASE IN RISK

Changes to baselined hazards that do not reflect a potential increase in risk as defined in Paragraph 4.2 will be provided to the NASA element Safety, Reliability and Quality Assurance (SR&QA) and the USA Program Integration Configuration Management Office and shall be updated in PCASS by the originator, contractor, or project office within 12 months of identified change (as a minimum). These changes will be submitted as a Routine Update in accordance with NSTS 07700, Volume V, Item 1SR–2, Table C.4.

NASA element project SR&QA organizations shall be responsible for implementing surveillance to assure that routine updates do not increase the risk level (Paragraph 4.2) of the affected baselined hazard(s). The HR originator, contractor shall include a tracking number with the Routine Update HR package as designated in Appendix H.

HR changes that result in a downgrade of hazard risk acceptance level or hazard cause classification shall be presented to the SSRP to ensure that the risk downgrade rationale is appropriate and that all element–to–element interfaces have been considered; however, causes that are eliminated as a result of the hardware being excessed or no longer used do not require review and approval by the SSRP.

4.6 HAZARD REPORT DATA ELEMENTS

For ease in explaining the data elements, an example HR has been divided into four parts. This HR format is not mandatory. The following HR data elements are mandatory.

4.6.1 Part I of the HR

Part I of the HR contains a management overview designed to provide a clear description of the hazardous condition, the acceptance rationale for accepting the risk(s), and the closure classification (eliminated, controlled, accepted risk) accepted by program management. The risk matrix provides program management with an overall risk picture for the hazardous condition.

a. The data elements contained in Part I of the HR are discussed below. (See Figure 4–3, page 1 of 4 for a sample HR). Reference <#> are provided that correlate the data element to the HR.

   1. Hazard Report Number (HR #). <1> Identification of the HR number unique within the system/subsystem (example ORBI 108). Whenever a change is made to the HR, the revision letter should be changed to identify the changed HR as the letter revision of the document.

      (a) Revision Letter: Revision to a baselined HR will be indicated by an alpha letter.

      (b) DCN Number: The DCN number will be documented in this data element.

2. Date. <2> Date of preparation/revision of this HR.

3. Hazard Report Status. <3>

   (a) Closed. Corrective action to eliminate or control the hazard has been implemented or scheduled for implementation. Program management accepts the risk pending completion of corrective action and verification. Baselining by the PRCB is required to approve a HR as closed.

   (b) Open. A HR status is open when the corrective action to eliminate or control the hazard has not been completed and the corrective action is not scheduled to be performed.

4. Title. <4> Provide a descriptive title of the hazard.

5. System. <5> Identify the system/subsystem/component within the element.

6. Vehicle Effectivity. <6> Identifies the major element to which the hazard is applicable. (Example OV–102)

7. Mission Phase. <7> (As appropriate) Prelaunch Engine Start, Pad Abort, Launch, Boost, Booster Separation, Main Engine Cutoff (MECO), ET Separation, On–Orbit, etc.

8. Hazardous Condition Description. <8> Include a description in terms of one or more generic hazards, such as fire/explosion, impact, or toxicity. The description should be made explicit to specify the equipment involved, such as, fire/explosion in the payload bay.

9. Acceptance Rationale. <9> Provide a summary rationale for accepting the HR classification. Also identify flight effectivity if HR is prepared for a specific flight effectivity (example STS–26).

10. Accepted Risk Causes. <10> Provide a management summary listing of each hazard cause that is classified as accepted risk.

The criteria for determining the closure classification and risk matrix data in Part I are detailed in Paragraphs 4.6.2.7 and 4.6.2.8.

4.6.2 Part II of the HR

Part II of the HR (see Figure 4–3, page 2 of 4) will contain the following data elements: Cause(s), effect(s), safety requirements, control(s), verification(s), classification,

severity, and likelihood of occurrence. It must be understood that a HR is generated to address only one hazardous condition. The hazardous condition may result from several hazard causes. Therefore, in Part II of the HR each hazard cause is addressed separately by identifying the effect(s), the safety requirement(s), the controls that are in place, and the verification(s) of these hazard controls. Based on this data, each hazard cause will be assigned a classification. The severity and likelihood of occurrence will be assessed for each hazard cause. For each hazard cause, the worst case effect will determine the severity level to be assigned. For each hazard cause, the controls that are in place are assessed to determine the likelihood of occurrence. Eliminated hazard causes will not be documented or assessed in this part of the HR but may be included in the background section of the HR to maintain visibility of improvements made during the hazard analysis and reporting process.

a. Cause(s). <13> An unsafe act or condition which may lead to the hazardous event is defined as a cause. Hazard causes shall be identified down to the level at which controls are to be applied and shall consider environments, software errors, hardware failures, secondary failures/conditions, procedural errors, operationally induced external and internal failures and human errors/limitations. In addition to NSTS 22254 and NHB 5300.4 (1D–2) requirements, the following data will also be evaluated: Waivers/deviations for effectivity of more than one flight, post–flight/in–flight anomalies, alerts, trending data, and interface/integrated HRs. Single mission waivers should be briefed through the flight readiness process, starting with the element contractor's preflight assessment. For FMEA/CIL items, a summary of the causes leading to the hazardous condition (failure mode) may be provided at the FMEA level. Each hazard unique cause will be itemized individually and the fault tree reference will be included.

    1. Effect(s). <14> The effect(s) is/are the potential worst case results of the hazard cause.

    2. Control(s). <15> For FMEA/CIL items, provide a summary of controls with sufficient detail to clearly reflect critical controls which mitigate/control the hazard. Provide narrative description of the appropriate design, safety devices, alarm/caution and warning devices, or special automatic/manual procedures used to control the hazard. Reference must include document number. Crew training in specific instances may be accepted as a control.

    3. Verification(s). <16> Provide a summary of the methods used to verify the hazard controls. Summaries will include sufficient detail/explanation of testing, inspection, and analysis which mitigate the hazard and support hazard closure or risk acceptance rationale. Verification methods include

analyses, tests, inspections, and operations and maintenance requirements. Identify the verification reference by document number and title. Operations and Maintenance Instruction (OMIs) will only be listed when there is not an Operational Maintenance Requirements and Specifications Document (OMRSD) used as a control or requirement.

4. Severity Level. <17> The severity level is an assessment of the most severe effects of a hazard. Complete for each cause by assessing the most severe effect and documenting it as catastrophic, critical, or marginal.

   (a) Catastrophic: Hazard could result in a mishap causing fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility.

   (b) Critical: Hazard could result in serious injury to personnel and/or damage to flight or ground equipment which would cause mission abort or a significant program delay.

   (c) Marginal: Hazard could result in a mishap of minor nature inflicting first–aid injury to personnel and/or damage to flight or ground equipment which can be tolerated without abort or repaired without significant program delay.

5. Likelihood of Occurrence. <18> This part of the HR is completed for each cause by assessing the controls that are in place and documenting them as probable, occasional, remote, or improbable.

   (a) Probable: Expected to happen in the life of the program.

   (b) Infrequent: Could happen in the life of the program. Controls have significant limitations or uncertainties.

   (c) Remote: Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties.

   (d) Improbable: Extremely remote possibility that it will happen in the life of the program. Strong controls in place.

6. Classification. <19> Assign a classification to each hazard cause of controlled or accepted risk. Hazard cause with a classification of eliminated will not be included in the HR.

   (a) Eliminated Hazard: A hazard that has been eliminated by completely removing the hazard causal factors.

   (b) Controlled Hazard: The frequency of occurrence and/or severity level have been reduced by implementing the appropriate hazard

reduction precedence sequence to comply with program requirements.

(c) Accepted Risk: A hazard for which the controls for one or more hazard causes fail to meet the hazard reduction precedence sequence (as previously discussed in Paragraph 1.6) and, therefore, have limitations or uncertainties such that the hazard could occur during the life of the program. The following are examples of conditions that could be considered accepted risk hazards.

(1) Critical Single Failure Points.

(2) Limited controls, or controls that are subject to human error or interpretation.

(3) System designs or operations that do not meet industry or Government standards.

(4) Complex fluid system leaks.

(5) Safety detection and suppression devices which are not adequate.

(6) Uncontrollable random events which could occur even with established precautions and controls in place, such as weather or fires.

7. The remaining data elements in Figure 4–3, page 1 of 4 of a HR can be completed.

(a) As a check to ensure the proper severity and likelihood of occurrence, a risk picture is presented to the program management. A guideline risk matrix to ensure proper closure classification is provided in Figure 4–4. It should be noted that accepted risk hazard causes should only appear in the shaded area of the matrix: Controlled hazard causes appear in the unshaded areas of the matrix; and unaccepted risk appears in the asterisk block of the matrix. Unacceptable risk requires risk reduction prior to HR baselining and is a constraint to mission.

(b) Hazard Report closure classification. <11> The hazard closure classification is based on the most severe closure as shown for each hazard cause contained in Part II of the HR. The closure classification will be controlled, accepted risk or eliminated. The only time a HR will be rated eliminated is when all causes to a baseline HR have

been eliminated by removing the hazard source or by deleting the hazardous operations.

8. Risk matrix hazard severity and likelihood of occurrence. <12> A completed risk matrix sample is provided in Figure 4–5. The risk matrix will be completed by documenting each hazard cause severity, and likelihood of occurrence contained in Part II of the HR. The controls are considered to be in place when performing this severity and likelihood of occurrence assessment. For example, the matrix in Figure 4–5 represents a HR with four hazard causes. Three causes are rated with likelihood of occurrence as ”INFREQUENT” and severity level of ”CATASTROPHIC”. One hazard cause is rated with a likelihood of occurrence as ”REMOTE” and a severity level of ”CATASTROPHIC”. The alpha letters represent the cause paragraph from the HR.

4.6.3 Part III of the HR

Part III of the HR contains the reference information (see Figure 4–3, page 3 of 4) such as interfaces, FMEA/CIL, OMRSD, OMI, Launch Commit Criteria (LCC), Flight Data File (FDF), and Flight Rules (FRs).

a. Safety Requirement(s). <20> Provide narrative descriptions of the requirement(s) used to control the hazard. In addition to listing safety requirements used to control the hazard, provide other requirements used as controls. The reference must include document number and title. Project requirements should be used as primary references whenever possible, followed by SSP requirements.

b. Interfaces: <21> Identify system interface(s) that are affected by and cause hazard conditions within the report, including facilities, GSE, and other elements.

c. FMEA/CIL. <22> There shall be cross–referencing to the related FMEA/CIL items. Where the hazard causes and controls are the same as those listed in the FMEA/CIL, the causes, effects, and controls shall be summarized in the HRs. The information contained in this data element should be completed as follows (this is optional for FMEA):

   FMEA/CIL Number: 03–1–0205–2

   Criticality: 1/1

   Item: SSME Helium Regulator

   Failure Mode: Output pressure high

d. OMRSD. <23> Document all OMRSDs that are used. The OMRSD data element should be completed as follows:

File: III

Volume Number: 41

Requirement Number: BGO.080

OMRSD Reference Title: PR1–3/7–9 SSME Helium regulator function test:

e. OMI. <24> Required only when an OMRSD is not imposed and an OMI is required for verification of hazard control. When an OMI is listed in a document reference section, list by OMI number and title.

f. Launch Commit Criteria. <25> Document all LCCs that are used as a control.

Include (LCC) section number and title:

Subsystem Identification (SSID) Number:

Section Title: 6.2.1

LCC Title: MPS Regulator Helium Outlet Pressure Anomaly

g. Flight Data File. (Crew Procedures) <26> Document all FDFs that are used as a control. Include book and procedure name.

Document Number: JSC 18768

Book Title: Ascent/Entry System Procedures

Procedure Title: MPS Helium Tank Leak Procedure Pre–ET Sep

h. Flight Rules. <27> Document all FRs that are used as a control. Include FR number and title.

Flight Rule Number:

Flight Rule Title: Thermal Windowpane Failure

4.6.4 Part IV of the HR

Part IV of the HR, (see Figure 4–3, page 4 of 4) contains background, status of open work, preparing engineer, and date.

a. Background. <28> Include information which adds understanding to the hazard, changes to the hazard, and supportive documentation, etc. Document

the chronology of major events associated with the hazard, including related flight history, test and check–out failure summaries, etc.

b. Status of open work. <29> Identify open work, responsible agency, action required, and due date. Completion due dates will only be supplied for open work that is a constraint to a mission milestone.

c. Preparing engineer and date. <30> Identify the preparing engineer/analyst and date.

d. Submittal signatures. Each HR must include the following approval signatures prior to submitting an SSP CR.

   1. Originator/Contractor Design Engineer. <31>

   2. Originator/Contractor Safety Engineering Manager. <32>

   3. NASA Subsystem Manager (optional). <33>

   4. NASA Project Safety (optional). <34>

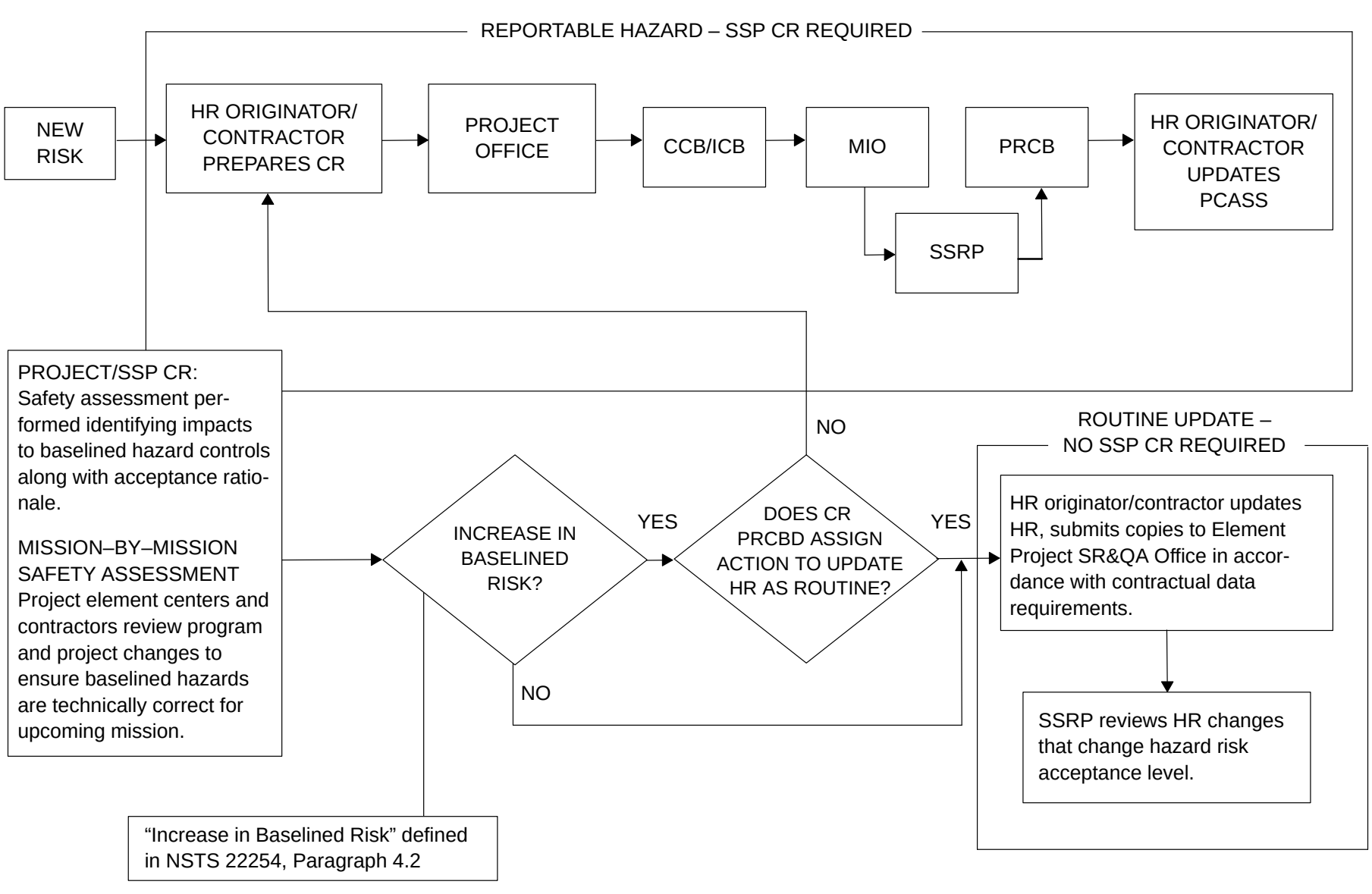
4.7 PROGRAM

These reports will provide current hazards description and disposition for management visibility and action.

Upon approval of the SSP CR baselining the hazard, a PRCB directive will be issued to update the PCASS data base to reflect the current hazard status. These HRs will be approved and updated as specified in Section 4.2.

FIGURE 4–1

HAZARD REPORT APPROVAL PROCESS



THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE 4–2

SSP HAZARD REPORT EXECUTIVE SUMMARY

(Page 1 of 3)

	SSP HAZARD REPORT EXECUTIVE SUMMARY	**NAME:** **DATE:**

SAMPLE SSP HAZARD REPORT EXECUTIVE SUMMARY

CR#: **50414F**

TITLE: **KSC LAUNCH AND LANDING REEVALUATION**

FIGURE 4–2

SSP HAZARD REPORT EXECUTIVE SUMMARY

(Page 2 of 3)

	SSP HAZARD REPORT EXECUTIVE SUMMARY	NAME:
		DATE:

CR#: 50414F KSC LAUNCH AND LANDING REEVALUATION

HR#: SPC–K13019–86 PERSONNEL INJURY AND FLIGHT HARDWARE DAMAGE DUE TO INADEQUATE FIRE DETECTION AND SUPPRESSION IN THE PAYLOAD CHANGEOUT ROOMS (PCRs)

HR CLASSIFICATION:
WAS: CONTROLLED
IS: ACCEPTED RISK

HAZARDOUS CONDITION DESCRIPTION:

THE EXISTING FIRE DETECTION AND SUPPRESSION SYSTEMS IN THE PAYLOAD CHANGEOUT ROOMS (PCRs) WILL NOT PROVIDE EARLY DETECTION AND WARNING OR RAPID FIRE SUPPRESSION IN THE EVENT OF A FIRE DURING PERIODS WHEN THE PCR IS UNATTENDED. DURING PERIODS OF INACTIVITY, SUCH AS THIRD SHIFT, HOLIDAYS, OR WEEKENDS, THE PCR IS LOCKED AND UNATTENDED.

DESCRIPTION OF CHANGE:

- HR UPGRADED FROM CONTROLLED TO ACCEPTED RISK.
- PRESENTED TO SPACE SHUTTLE PRCB 12/06/89.

FIGURE 4–2

SSP HAZARD REPORT EXECUTIVE SUMMARY

(Page 3 of 3)

	SSP HAZARD REPORT EXECUTIVE SUMMARY	NAME:
		DATE:

DESCRIPTION OF CHANGE: (CONTINUED)

- HR REFLECTS THE FOLLOWING DIFFERENCE IN PAD A FROM PAD B.
  - NO REMOTE CONTROL ON PAD A
  - NO LOCAL SINGLE STATION ACTIVATION ON PAD A. (WATER SYSTEM MUST BE ACTIVATED AT EACH LEVEL CONTROL STATION ON PCR.)

- THERE IS A DELAY IN IMPLEMENTING FIRE DETECTION SYSTEM ON PCR ON PAD A AND PAD B.
- SPACE SHUTTLE PRCB ASSIGNED KSC AN ACTION ITEM TO COME BACK IN SIX MONTHS TO ADDRESS THEIR PLAN FOR CORRECTING THE ABOVE ISSUE.
- RISK IS THOUGHT TO BE ACCEPTABLE DUE TO LOW PROBABILITY OF A FIRE AND PERSONNEL ARE IN THE PCR WHENEVER A PAYLOAD IS PRESENT.

THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE 4–3

SSP HAZARD REPORT (Part I)

(Page 1 of 4)

HAZARD REPORT NO: <1> REVISION LETTER DCN NUMBER	DATE: <2> REVISION:	STATUS: <3> OPEN: _____ CLOSED: _____	CLOSURE CLASSIFICATION: <11> ELIMINATED ___ CONTROLLED ___ ACCEPTED RISK ___
TITLE: <4>			RISK MATRIX <12> (HAZARD SEVERITY AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE)
SYSTEM: <5>	SUB–SYSTEM: <5>	COMPONENT: <5>	
VEHICLE EFFECTIVITY: <6>			
MISSION PHASE: <7>			
HAZARDOUS CONDITION DESCRIPTION: <8>			
ACCEPTANCE RATIONALE: <9>			
ACCEPTED RISK CAUSES: <10>			

LIKELIHOOD

	MARGINAL	CRITICAL	CATASTROPHIC
PROBABLE			
INFREQUENT			
REMOTE			
IMPROBABLE			

SEVERITY LEVELS

FIGURE 4–3

SSP HAZARD REPORT (Part II)

(Page 2 of 4)

REPORT NO: <1>	DATE: <2> REVISION:
TITLE: <4>	
A. CAUSE(S): <13> (FAULT TREE REFERENCE) 1. EFFECT(S): <14> 2. CONTROL(S): <15> 3. VERIFICATION(S): <16>	1. SEVERITY: <17> 2. LIKELIHOOD OF OCCURRENCE: <18> 3. CLASSIFICATION: <19>
B. CAUSE: (FAULT TREE REFERENCE) 1. EFFECT(S): 2. CONTROL(S): 3. VERIFICATION(S):	1. SEVERITY: 2. LIKELIHOOD OF OCCURRENCE: 3. CLASSIFICATION:

FIGURE 4–3

SSP HAZARD REPORT (Part III)

(Page 3 of 4)

REPORT NO: <1>	DATE: <2> REVISION:
TITLE: <4>	
SAFETY REQUIREMENTS: <20>	
INTERFACES: <21>	
FMEA/CIL: <22>	
OMRSD: <23>	
OMI: <24>	
LAUNCH COMMIT CRITERIA: <25>	
FLIGHT DATA FILE: <26>	
FLIGHT RULES: <27>	

FIGURE 4–3

SSP HAZARD REPORT (Part IV)

(Page 4 of 4)

REPORT NO: <1>		DATE: <2> REVISION:	
TITLE: <4>			
BACKGROUND: <28>			
STATUS OF OPEN WORK: <29> RESPONSIBLE AGENCY: ACTION REQUIRED: DUE DATE:			
PREPARING ENGINEER: <30>		DATE:	
ORIGINATOR/ CONTRACTOR DESIGN ENGINEER: <31>	ORIGINATOR/ CONTRACTOR SAFETY ENGINEERING MANAGER: <32>	NASA SUBSYSTEM MANAGER: (OPTIONAL) <33>	NASA PROJECT SAFETY: (OPTIONAL) <34>

FIGURE 4–4

RISK MATRIX TEST FOR AGREEMENT BETWEEN CLOSURE CLASSIFICATION AND RISK

(HAZARD SEVERITY LEVEL AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE)

LIKELIHOOD	MARGINAL	CRITICAL	CATASTROPHIC
PROBABLE	ACCEPTED RISKS	ACCEPTED RISKS	UNACCEPTABLE RISK
INFREQUENT	ACCEPTED RISKS	ACCEPTED RISKS	ACCEPTED RISKS
REMOTE	CONTROLLED	ACCEPTED RISKS	ACCEPTED RISKS
IMPROBABLE	CONTROLLED	CONTROLLED	CONTROLLED

SEVERITY LEVELS

FIGURE 4–5

SAMPLE COMPLETED RISK MATRIX

(HAZARD SEVERITY LEVEL AND LIKELIHOOD OF OCCURRENCE WITH CONTROLS IN PLACE)

LIKELIHOOD	MARGINAL	CRITICAL	CATASTROPHIC
PROBABLE			
INFREQUENT			(3) A, C, D
REMOTE			(1) B
IMPROBABLE			

4 HAZARD CAUSES

SEVERITY LEVELS

5.0 MANAGEMENT SAFETY ASSESSMENT (MSA)

NSTS 22973, Management Safety Assessment (MSA) for SSP, identifies selected significant risks to the program in support of the risk reduction program.

5.1 PURPOSE

The purpose of the MSA document is to identify selected SSP risks in support of the risk reduction program. This safety assessment is performed and documented to focus management attention on selected risks which were chosen from the group of risks that could result in loss of vehicle or crew, and to enhance communication of these risks to all management and technical personnel.

5.2 SCOPE

The MSA addresses the safety assessment of the SSP mission, including Space Shuttle integration, Space Shuttle elements, GFE, CFE, launch and landing, facilities/operations, OEX, and payloads. The safety assessment identifies selected risks that could cause loss of vehicle or crew. The risks are selected based on results of the hazard reevaluation effort, review of Top 20 FMEA/CILs, flight anomalies from past missions, significant risk items presented by each element contractor and NASA center through the SSRP, and the MSA fault tree analysis. The SSRP represents the focal point for identifying significant program risks. Only selected significant risks that can be reduced by incorporating recommended hardware or procedure modifications will be included in the MSA.

As additional risks are identified and evaluated, selected risk reports will be incorporated into future MSA documents. This approach results in an evolving MSA document wherein management and technical personnel can track the status of selected risks to the program and make plans for future actions.

Risks associated with noncatastrophic vehicle damage and crew injury are not included in the MSA. These risks are identified and resolved as an integral part of the mission operations activity and are included in the FRs and FDF.

5.3 APPROACH

The MSA approach is to present selected risks to the program which are based on results of NASA–wide safety analyses, assessments, and HR evaluations. The documentation of selected risks will be in a graphical presentation format using fault trees when appropriate to permit highlighting of selected risks and to recommend future improvements.

5.4 RESPONSIBILITIES

The JSC SR&QA Office will be responsible for NSTS 22973. The risk issues will be coordinated through the element project offices and/or the Space Shuttle Systems Integration Office prior to publishing this document. The MSA will be published annually.

6.0 SAFETY ANALYSIS REPORT (SAR)

The SAR will be prepared and processed as directed by the project manager. A sample SAR is included in Appendix E of this document. If desired, it can be adapted as a guideline for preparation and contents of a SAR.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

FAULT TREE ANALYSIS

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 PURPOSE

The Fault Tree Analysis (FTA) is a deductive analytical technique which lends itself to:

a. Detailed systems analyses

b. Decision making

c. Communications

When used as a system safety analysis tool, the fault tree results in a graphic and logical representation of the various combinations of possible events, both fault and normal, which can occur within a system and which can cause a pre–defined undesired event. An undesired event is any event which is identified as objectionable and unwanted, such as a potential accident, hazardous condition, or undesired failure mode. This graphic presentation exposes the interrelationships of system events and their dependence upon each other, which may result in the occurrence of the undesired event.

When the fault tree structure is completed, the fault tree is evaluated to determine the results or significance of the analysis. Two types of evaluations are possible: (1) qualitative and (2) quantitative. The qualitative evaluation is an engineering judgment assessment of the fault tree. The quantitative evaluation is a numerical evaluation. Failure rates of the system elements are inserted into the fault tree structure and mathematically combined to yield probabilities. The validity of action taken to eliminate or control events can be enhanced in certain circumstances by quantifying the fault tree and performing such a numerical evaluation. The quantification and numerical evaluation may provide three basic measurements for decision making relative to risk acceptability and required preventive measures. They are (1) the probability of occurrence of the undesired event; (2) the significance or importance of the undesired event or the various paths leading to the undesired event; and (3) the baseline measure of the level of safety, which can be used to determine the effects of design changes.

As recommended preventive measures are incorporated into the design, their adequacy involving the safety problem may be verified. This is done by making the appropriate changes in the fault tree structure and then reevaluating the fault tree. The effects of the change, or the relative measure of improvement, should be apparent from the reevaluation.

2.0 DESCRIPTION

FTA is a technique by which the system safety engineer can rigorously evaluate specific hazardous events. It is a type of logic tree which is developed by deductive logic from a top undesired event to all sub–events which must occur to cause it. It is primarily used

as a qualitative technique for studying hazardous events in systems, subsystems, components, or operations involving command paths. It can also be used for quantitatively evaluating the probability of the top event and all sub–event occurrences when sufficient and accurate data are available. Quantitative analyses shall be performed only when it is reasonably certain that the data of part/component failures and human errors for the operational environment exist.

A fault tree consists of the segments shown in Figure A–1. The tree should only be developed to the lowest segment required to identify and resolve the hazard.

The top structure may be developed as the project Preliminary Hazard Analysis (PHA) to identify the project safety requirements and obvious hazards. The tree can be quantified with actual data, developed data, or simulation. There are computer programs available for plotting the tree and performing a qualitative or quantitative analysis.

3.0 PROGRAM PHASE

The FTA can be performed at any time in the life of a system as long as the required level of detail is available. The top structure can be used to support the PHA during project planning. The lower levels can then be developed in parallel and consistent with system development. FTAs can be very effective tools for accident or mishap investigation. FTAs can be used in the most complex situations and need only be developed to the lowest level required. The structure must be developed by hand, but computer programs are available for all other efforts. Quantitative applications are difficult to perform because of the lack of appropriate failure rate data.

4.0 TECHNIQUE

Only the basic FTA symbols (Figures A–3 and A–4) and tree development are described in the following paragraphs. A detailed description of this FTA technique is found in the “Fault Tree Handbook”, NUREG–0492, Nuclear Regulatory Commission, January 1981, “GPO” Sales Program Division of Technical Information and Document Control, U. S. Nuclear Regulatory Commission, Washington, DC 20555. Failure rate data may be obtained from DOD–HDBK–217, Reliability Prediction for Electronic Parts, or through the Government–Industry Data Exchange Program. Figure A–3 provides an example of logic symbols expanded to provide more detail.

Suitable mathematical expressions representing the fault tree entries may be developed using Boolean algebra. When more than one event on a chart can contribute to the same effect, the chart and the Boolean expression indicate whether the input events must all act in combination (AND relationship) to produce the effect or whether they may act singly (OR relationship). The probability of failure of each component or of the occurrence of each condition or listed event is then determined. These probabilities

may be from failure rates obtained by experience; vendors' test data; comparison with similar equipment, events, or conditions; or experimental data obtained specifically for the system. The probabilities are then entered into the simplified Boolean expressions. The probability of occurrence of the undesirable event being investigated may then be determined by calculation.

Figure A–4, Sample System Fault Tree, is an example of a tree for the explosion of a compressor pressure vessel with the various levels and symbols. The top level shows the final results of potential faults, and each level lower provides more specific details of the faults and causes.

5.0 COMPUTERIZATION

The Nuclear Safety Analysis Computer Program fault tree program may be used for fault tree input, printout, data transfer, and automated analyses. It may be obtained free of charge from the Air Force Weapons Laboratory, Kirkland Air Force Base, New Mexico.

THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE A–1

SUGGESTED FAULT TREE SEGMENTS

TOP UNDESIRED EVENT

PROGRAM OPERATIONS

- MANUFACTURING
- TEST
- TRANSPORTATION
- LAUNCH PROCESSING
- MISSION

PROCESS FLOW

- OPF PROCESSING
- OPF ROLLOVER PROCESSING
- ELEMENT PROCESSING
- VAB PROCESSING
- PAD ROLLOUT PROCESSING
- PAD LAUNCH PROCESSING
- MISSION PROCESSING
- POST–LANDING PROCESSING
- FERRY FLIGHT PROCESSING
- LSF PROCESSING
- OPF ROLLOVER PROCESSING

PAD LAUNCH PROCESSING

- PROPELLANT LOADING TO CREW INGRESS (PHASE A)
- CREW INGRESS TO SSME IGNITION SEQUENCE COMMAND (PHASE B)

MISSION PROCESSING

- SSME IGNITION SEQUENCE COMMAND TO SRB IGNITION COMMAND (PHASE C)
- SRB IGNITION COMMAND TO TOWER CLEAR (PHASE D)
- TOWER CLEAR THROUGH SRB SEPARATION COMPLETE (PHASE E)
- SRB SEPARATION COMPLETE TO ET SEPARATION COMPLETE (PHASE F)
- ET SEPARATION COMPLETE TO ORBIT INSERTION (PHASE G)
- ON–ORBIT OPERATIONS (PHASE H)
- DEORBIT BURN COMMAND TO TOUCHDOWN (PHASE I)
- TOUCHDOWN TO WHEEL STOP (PHASE J)
- WHEEL STOP TO CREW EGRESS (PHASE K)

FIGURE A–2

FAULT TREE SYMBOLS

	PRIMARY EVENT SYMBOLS	
	BASIC EVENT	A basic initiating fault requiring no further development
	CONDITIONING EVENT	Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)
	UNDEVELOPED EVENT	An event which is not further developed either because it is of insufficient consequence or because information is unavailable
	EXTERNAL EVENT	An event which is normally expected to occur
	INTERMEDIATE EVENT SYMBOLS	
	INTERMEDIATE EVENT	A fault event that occurs because of one or more antecedent causes acting through logic gates
	GATE SYMBOLS	
	AND	Output fault occurs if all of the input faults occur
	OR	Output fault occurs if at least one of the input faults occurs
	INHIBIT	Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)
	TRANSFER SYMBOLS	
	TRANSFER IN	Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page)
	TRANSFER OUT	Indicates that this portion of the tree must be attached at the corresponding TRANSFER IN

FIGURE A–3

LOGIC SYMBOLS LEGEND

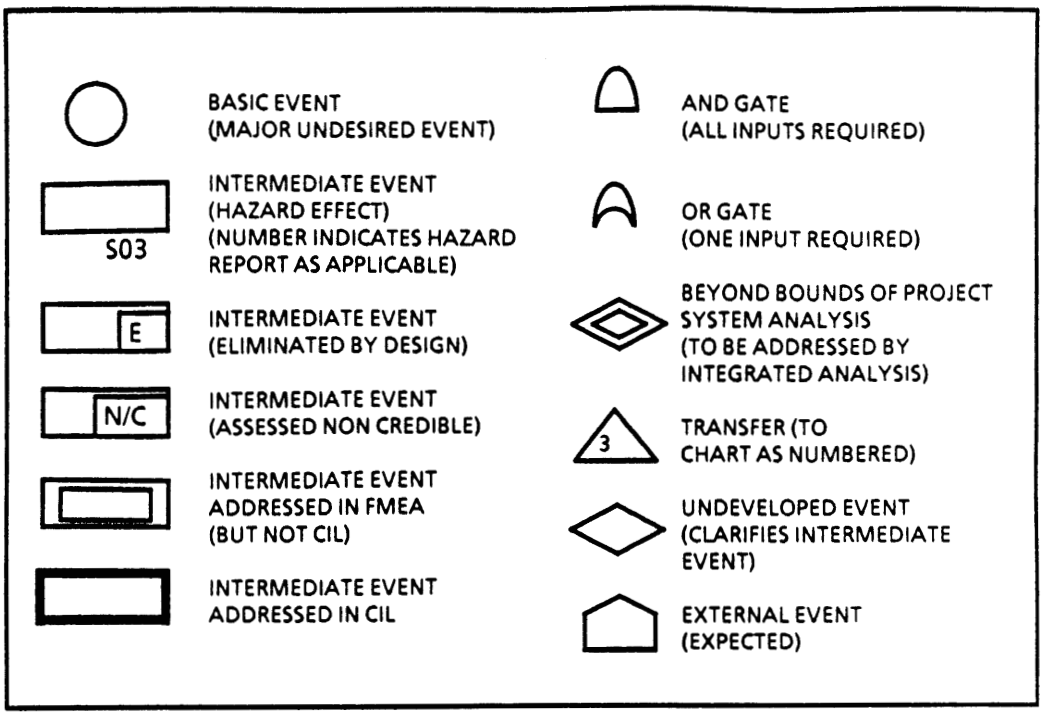
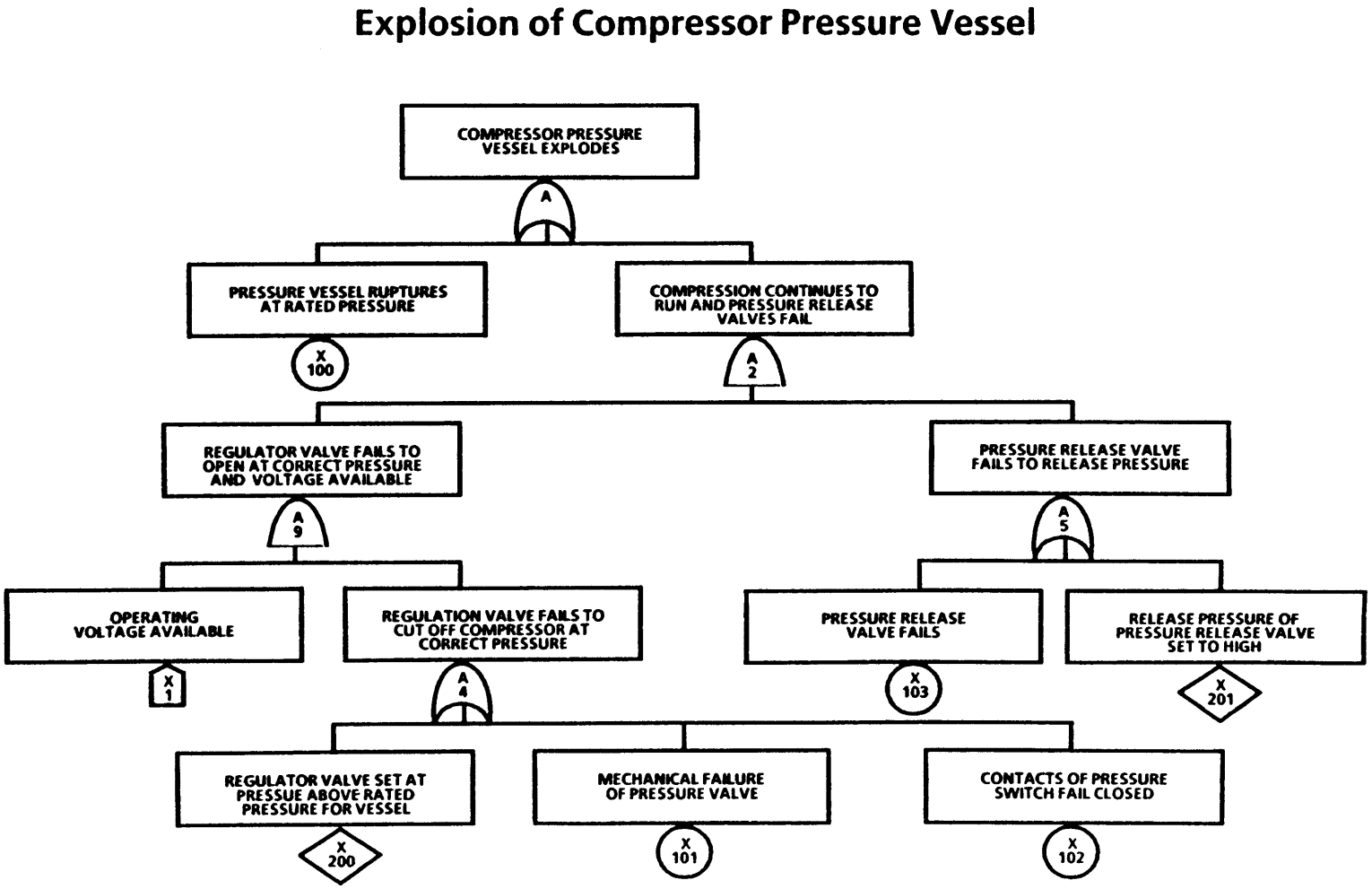


FIGURE A–4

SAMPLE SYSTEM FAULT TREE



APPENDIX B

SNEAK ANALYSIS

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 PURPOSE

A Sneak Analysis (SA) is performed to identify areas in which undesired functions could occur or desired functions could be inhibited during normal or abnormal operations.

2.0 DESCRIPTIONS

SA is a technique for identifying latent conditions not caused by component failures which can inhibit desired functions or cause undesired functions to occur. The SA technique is a formalized, rigorous, and orderly process of assuring that unintended conditions have been excluded from the system.

SA is a computer–aided analysis approach for automated development of network trees developed from circuit diagrams and software source code. Network trees can be easily analyzed for sneak conditions by using a checklist of clues applied at each junction or decision point. The computer also provides cross–references between network trees, which maintain system–level connectivity.

3.0 PROGRAM PHASE

A SA should be initiated when component–level circuit data and software source codes are reasonably well defined. The preferred start time is before the CDR in the full–scale engineering development phase. The SA complements, but does not replace or supersede, testing and the common design analysis techniques such as the FMEA and HA.

A full scale SA may not be feasible depending on project constraints. Therefore, a SA can be done on catastrophic hazards as identified by a system level FMEA or hazard analysis. SAs of subsequent data releases and changes are a cause of sneak conditions which will require SA updating.

4.0 PROCEDURE

SA is performed in five phases: (1) data preparation, (2) computer input, (3) computer processing, (4) network tree construction, and (5) clue application. The first four phases of SA involve restructuring the physical oriented design data to show the system outputs in terms of their inputs. The network trees are constructed from hardware “built from” data and documented software source code.

Once the trees have been produced, the next task of the analyst is to identify sneak clues in each network tree, where a clue is a visual key that directs the analyst to ask specific questions. A clue can be a basic topological pattern. Five basic patterns exist: the single line (no–node) topograph, the ground dome, the power dome, the combination dome, and the “H” pattern. As shown in Figure B–1, “PWR” represents electrical power; “S” indicates a switching element; and “L” an electrical load. Similar topological

patterns exist for software. Although at first glance, a given circuit may appear more complex than these basic patterns, closer inspection reveals that the circuit is actually composed of these basic patterns in combination.

Other visual clues are also available such as interface connections and analog and digital circuitry. These clues are easily identifiable on topological network trees and forests, and the questions will identify if one of the following sneak conditions exists:

a. Sneak paths which cause current, energy, or logic to flow along an unexpected route, resulting in unwanted functions or inhibiting a desired function.

b. Sneak timing which results from incompatible hardware or logic sequences, and can cause inappropriate system response.

c. Sneak indications which cause an ambiguous or false indications of system operating conditions, or lead to erroneous operator actions.

d. Sneak labels which result from a lack of precise nomenclature, instructions on controls, or operating consoles that can lead to erroneous operator actions.

The application of sneak clues is performed without limitations as to the intended sequence of inputs. It is important to note that it is this principle that makes SA unique from simulations and other analysis techniques, since it is the unexpected combinations or sequences of inputs which make sneak conditions difficult to uncover by other means.

The sneak clues are applied at multiple levels during the clue application phase. The first two levels are applied to individual network trees in a forest. The third level is applied to the forest.

First, applicable clues are applied at the electrical current flow level for hardware network trees or at the program flow level for software network trees. This level of clue application results in finding classical conditions such as unintended reverse current flows, unused circuitry, overstressing of components, infinite software program loops, and nonexecutable software codes.

The second level of clue application is also at the individual hardware or software network tree level. This second level application of sneak clues results in location signal/data flow problems, logic design flaws, and timing conflicts on a localized basis.

The third level of clue application occurs at the network forest or system level. Recognition of topological patterns and clue application at this level provides much more than a mere interface check. The forests provide a system level view of the relationships between the various signals and variables which relate to a system output. However, no paths are omitted, since they are in typical system level block diagrams. Therefore,

clue application of the forests provides insight into complex system relationships, including hardware/software interactions which cannot be seen clearly through other means.

When a potential sneak condition is identified, the analyst must verify that it is valid. The network trees are checked against the latest applicable drawings, program listings, and revisions. Operational information may also be reviewed concerning the system in question. If the sneak condition is verified, a sneak condition report is written. This report includes applicable drawings, an explanation of the condition(s), system–level impact, and a recommendation for elimination of the sneak. A sample Sneak Circuit Report is shown in Figure B–2.

During the course of an analysis, unnecessary or undesirable conditions are sometimes encountered. Such conditions as certain Single Failure Points, unsuppressed inductive loads, unnecessary components, unnecessary software code, and inadequate redundancy provisions are reported in design concern reports. Any discrepancies found in the documentation are also reported in document error reports.

The reports are tracked to assure proper closeout action on each reported condition. At the end of the analysis, a final report is issued which details the scope, procedures, results, and conclusions of the analysis. The final report contains all the sneak condition reports, design concern reports, document error reports, and report tracking status sheets.

The network trees and forests are very useful for performing other analyses such as FMEAs and FTA at the component or system level. Computer programs have been developed for extracting from the SA data base the parts data required for performing a detailed FMEA. The network trees provide an easy–to–follow means of tracing cause–and–effect relationships through complex hardware/software systems. The forests can be used to calculate mean time between failures for a system function as opposed to a specific circuit card or black box.

THIS PAGE INTENTIONALLY LEFT BLANK

FIGURE B–1

BASIC TOPOGRAPHS

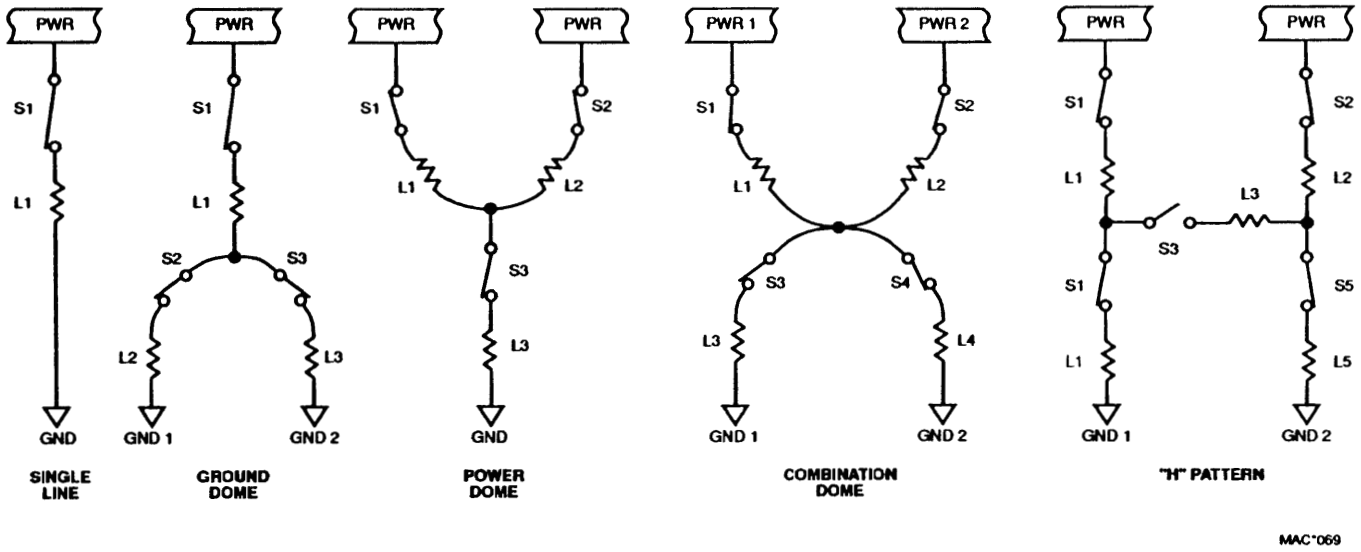


FIGURE B–2

SAMPLE SNEAK CIRCUIT REPORT

SNEAK CIRCUIT REPORT–1

TITLE SNEAK CURRENT PATH RESULTS IN UNINTENTIONAL MASTER ARMING OF WPN RELEASE SQUIB FIRING CIRCUITS

REFERENCES

MODULE/EQUIPMENT

WEAPON CONTROLLER (9431A2)

EXPLANATION

As shown in Figure 1, when the Master Arm switch is off, Emergency Jettison has not been selected, and the Weapon Select switch is left in the Center Station position, a sneak path exists from the +28VDC Weapon Control power through the Weapon Select Switch (9417A3S3) through 9431A2A1R1 to charge capacitor 9431A2A1C1 and then through transistor 9431A2A1Q1 to the firing circuit. This bypasses the Master Arm ‘A’ function. Similar paths exist for Master Arm ‘B’ and the Left and Right Wing Stations.

POTENTIAL IMPACT

1. Unexpected Master Arm power may contribute to inadvertent weapon release.

2. The function of the Weapon Release ‘A’ and ‘B’ circuit breakers (245EA1C31 and 2456A1C32) may be bypassed.

RECOMMENDATION

Add a blocking diode as shown in Figure 2.

REPORTED BY: _____ DATE October 16, 1980

CUSTOMER ACTION

APPENDIX C

SOFTWARE HAZARD ANALYSIS

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 INTRODUCTION

Software Hazard Analyses (HAs) are accomplished to identify and eliminate requirements and code deficiencies so that the total system operates at an acceptable level of risk. The analysis techniques and procedures described herein are a blend of evaluation of requirements, requirements HAs, and software code versus requirements analyses. Appropriate analysis techniques are applied throughout the total software development process initiating with the concept phase and continuing through the operation and maintenance phases.

2.0 EVALUATION OF SOFTWARE REQUIREMENTS

2.1 SCOPE

Safety Engineering is to evaluate baselined software requirements and subsequent changes to provide assurance that the requirements adequately reflect safety criteria and contain no defects which could adversely impact crew safety or mission success. The evaluation process is applicable to all flight and flight launch support software systems.

2.2 BACKGROUND

The requirements phase of the software development process provides for the definition and documentation of requirements at levels initiating with top level system requirements and progressing to design specifications for the detail design of code at the module and instruction level. Subsequent to the system conceptual phase, documentation of the software system program requirements is normally provided for levels corresponding to the system, functional, and detail requirements. Design specifications, prepared subsequent to the requirements definition, may be documented at both the functional and detail levels. Interface requirements are considered part of the system requirements, although they may be specified in independent documents. Baselining of the various level requirement documentation is established and placed under formal configuration control. Subsequent to baselining, changes to the requirements are processed through applicable CCB.

2.2.1 System Concept Documentation

Software system development begins with system concept definition originating with customer–provided mission and system requirements. The interaction between system hardware and software is established and requirements are allocated to hardware or software. Documentation includes the results of data system analysis and architecture studies, contractor’s submittals of related documentation/data requirements, and preliminary and system requirements review material.

2.2.2 System Level Requirements

System level requirements, referred to as Level A, describe the top level architectural design of the hardware and software components for the design and development of the software system. Documentation of these requirements form the controlling document for all requirements and provides the basis for subsequent levels of requirements. Software engineering requirements, design guidelines, and requirements and constraints are provided for the network and subsystem processors operating systems including software structure and partitioning, process and memory management, and input/output services. Crew, ground, and element interface requirements and operations are specified. Interfacing hardware system specifications are made reference to and programming and user interface languages are defined.

2.2.3 Functional Level Requirements

Functional level requirements, referred to as Level B, describe high level application functions related to major events; hardware subsystems; systems management; downlist/uplink; and assembly and checkout areas. Interfaces, timing and sequences, and other functional characteristics are specified.

2.2.4 Detail Level Requirements

Detail level requirements, referred to as Level C, define equations, algorithms, format conversion, data compensation and transformation, initialization data, and function interface details for areas described in the function requirements. The detail requirements may be contained in several documents, categorized as guidance, navigation, sequencing, redundancy management, display detail, and others.

2.2.5 Functional and Detail Design Specifications

Software design specifications are normally established at two different levels, functional design and detail design. The functional or preliminary design specification as it may be referred to, defines the overall structural design at the software system and computer program levels including the definition of the program structure in terms of function allocation, storage and timing allocation, as well as sequencing control, error detection and recovery, and interfaces between the program functions. Detail design specifications describe the function and organization of each program module with sufficient detail to permit coding of the software.

2.3 EVALUATION OF SYSTEM CONCEPTS AND SOFTWARE REQUIREMENTS

The safety effort identified in Paragraphs 2.3.1 and 2.3.2 below shall provide assurance that software system design concepts and subsequent software requirements including

applicable interface control documents contain no defects which could adversely impact crew safety or mission success. The safety effort objectives are the following:

a. Assure that safety requirements and safeguards have been allocated to software systems.

b. Identify and assess hazards.

c. Assure that all hazards have been eliminated or reduced to an acceptable level.

Identified hazards will be documented and tracked until satisfactory resolution is obtained.

2.3.1 Software System Concepts

An evaluation of the software system conceptual design documentation shall be performed and shall include, as a minimum, the following guideline criteria:

a. Adequacy of design and defined system objectives.

b. Assurance that safety requirements are allocated to hardware and/or software.

c. Interaction between system hardware and software are clearly defined and compatible.

d. Identification of safety–critical functions and compliance to failure criteria.

e. Adequate use of software safety feature to minimize hazard potential.

f. Data system redundancy and backup provisions are adequate.

g. Crew and ground interfaces identified and enhance crew safety.

2.3.2 Software Requirements Documentation Evaluation

An evaluation of the formal software requirements at each level and design specifications shall be performed and shall include, as a minimum, the following guideline criteria:

a. Adequate definition of requirements including objectives, interfaces, guidelines, and constraints.

b. Allocation of safety requirements for critical functions and compliance to failure tolerance.

c. Assurance that higher level requirements are incorporated into lower tiered requirements and specifications.

d. Technical adequacy, completeness, and clarity.

e. Definition of validity checks for all operator inputs.

f. Adequacy of fault detection, annunciation and reconfiguration.

g. Compatibility of software/hardware operations.

2.4 PROCEDURE

Each requirement submitted for formal baselining and subsequent CRs to the requirements are to be evaluated using the guidelines specified in Section 2.3 above. Worksheets are to be developed and used as aids by the analysts during the evaluation process.

2.5 REPORTING

Each identified deficiency is to be documented using the hazard report form and procedures specified in this document. Worksheets are to be submitted in accordance with the requirements of this document.

3.0 SOFTWARE REQUIREMENTS HAZARD ANALYSES

3.1 SCOPE

Requirements HAs are to be performed for all flight and flight launch support software related to safety–critical preflight and flight functions that are commanded, controlled, or monitored by software systems. For the purposes of this procedure, requirements are to include formally approved baselines and subsequent changes to the baselines.

3.2 BACKGROUND

Software requirements HAs are performed to identify and resolve potential requirements–related hazards. The analyses are performed using top–level Fault Tree Analyses (FTAs) and follow–on hardware/software analysis techniques. The major factor in the analyses is to ensure that the entire system is looked at with consideration to integration and operation conditions including the operator’s interfaces. To be effective, the analyses are initiated early in the system development phase where the system allocation process has assigned responsibilities between the hardware and software. The system PHA serves as the entry point into the top–level FTA by identifying critical functions and credible hazards that should be addressed in the software development. The software top–level FTA technique is to identify potential requirement hazards for software system critical functions, to assure that safety requirements are adequately allocated into software systems, and to identify software areas that require

in–depth hardware/software analysis. The hardware/software analysis provides a systematic approach to analyze the hardware and software interaction and interfaces taking human factors into consideration.

3.3 TOP–LEVEL FAULT TREE ANALYSES (FTAs)

A top–level FTA technique is a method for identifying hazardous elements and conditions on a gross level to obtain an initial safety evaluation of a specific system. A FTA is an analytical technique whereby an undesired event of the system is specified (usually a state that is critical from a safety standpoint) and the system is then analyzed in the context of its operation to determine all credible ways in which the undesired event can occur. The fault tree itself can be a qualitative graphic model of the various parallel and sequential combinations of system states or faults that will result in the occurrence of the predefined undesired event which is the top event of the tree. When software is considered along with the hardware and human interfaces, an entire system can be analyzed. The analysis identifies potential hazardous conditions, provides assurance that adequate software safety features are in place, and identifies areas that require further in–depth analysis.

3.4 HARDWARE/SOFTWARE ANALYSIS

The hardware/software analysis technique is a structured integrated approach to identify potential software requirements–related hazards resulting from the operating interaction of the system's hardware and software. Diagrams, forms, and checklists are used as aids by the system analyst to perform a comprehensive evaluation of software stimuli and measurements in order to assess the potential of adverse system operations. The primary goal of this analysis is to uncover inadequate allocation of software requirements.

3.5 PROCEDURES

The following procedures are to be followed in performing the Top–Level Fault Tree and Hardware/Software Analyses.

3.5.1 Top–Level Fault Tree Analysis

A software FTA is to be performed on all software–related critical functions identified from the system level PHAs or critical functions assessments. Hazards associated with each undesired event are to be determined and software functions that could contribute to the occurrence of the undesired event are to be identified. Logic trees are to be drawn to depict the logical interrelationship of major software system functions and events that could lead to top undesired events.

3.5.1.1 Data Acquisition

The following software, data processing, and hardware system related documentation are to be obtained for the defined system critical functions to be analyzed.

a. Preliminary software requirements/software concept document.

b. Software system study reports.

c. Preliminary Contract End Items (CEI) specifications.

d. Operations planning documents.

e. Preliminary Safety Analysis (SA) assessment reports.

f. Preliminary Failure Modes and Effects Analyses (FMEA).

g. System level Preliminary Hazard Analyses (PHAs).

h. System and application software requirements documents.

i. Hardware system functional operational requirements.

j. Interface Control Documents.

3.5.1.2 Critical Functions

This step is to determine the critical system functions to be performed by software systems. This is accomplished by review of the available documentation listed in Section 3.5.1.1 and from participation in software and hardware system development meetings. The preliminary safety analysis assessment reports and the system level PHAs documentation should be the primary source for identifying and compiling a list of software system critical functions.

3.5.1.3 Undesired Events

For each critical function, investigate the possible modes of occurrence of undesired events that could be caused by software systems and result in a potential hazardous condition. Undesired events to be considered that may be caused by software systems fall into four broad categories: (1) Inadvertent event, (2) out–of–sequence event, (3) failure of event to occur, and (4) magnitude or direction of event is incorrect.

3.5.1.4 Fault Tree Analysis (FTA)

A software system FTA is to be performed for each critical function. The fault tree is to be a graphic model of the various parallel and sequential combination of faults or

system states that will result in the occurrence of the predefined undesired event affecting the critical function. The faults or system states are to be events associated with the computer system, the software, or human error. Computer system redundancy techniques and operations are to be considered in the analysis. Each major interacting software principal function is to be identified and noted in the related blocks of the tree. For this analysis, it is to be assumed that any top–level software functions that process critical commands associated with the undesired events could cause the undesired event. Figure C–1 is an example of a software system fault tree. Each fault tree is to be evaluated for potential hazardous conditions based on the fail–operational/fail–safe requirement for critical systems. A summary table worksheet (Figure C–2) is to be prepared for each critical function showing the undesired events, applicable flight phase, the possible causes, and resulting potential hazards. Rationale for non–hazardous conditions will also be included.

3.5.1.5 Reporting

A HR is to be prepared for each identified potential software–related hazard using the HR form and procedures specified in this document. Worksheets are to be submitted in accordance with the requirements of this document.

3.5.2 Hardware/Software Analysis

Hardware/software HAs are to be performed on critical functions. The analysis is to consider the complete operating system in all planned and contingency operations during prelaunch checkouts and flight operations, including maintenance. Analyses are to be performed initially using the software requirements baselined at the software Preliminary Design Review (PDR) and end–item hardware defined at the related hardware system PDR. Software configuration changes to the baseline requirements are also to be analyzed depending on their criticality.

3.5.2.1 Data Acquisition

The following software, data processing system, and hardware system related documentation are to be obtained for the defined systems to be analyzed:

a. Functional and detail level software requirements documentation.

b. Approved copies of software requirements CRs.

c. Data processing system design/procurement specifications, technical descriptions and operation documents.

d. Data processing systems/software Interface Control Documents.

e. System hardware designs/procurement specifications and description documents.

f. Systems hardware functional/schematic diagrams.

g. Systems handbook.

h. Operation and maintenance plans and procedures.

i. PHA documentation.

j. Master Measurement List (MML).

k. Integrated system schematics.

3.5.2.2 Documentation Familiarization

This step is to gather the available hardware and software documentation as listed in Section 3.5.2.1 for the related subsystem/system. The analyst is to familiarize himself with all documentation that will be used to develop the analysis. Applicable documentation is to be listed on the system/subsystem definition form (Figure C–3).

3.5.2.3 Subsystem/System Block Diagram

A block diagram of the designated subsystem/system is to be obtained or drawn by the analyst and is to include the related data processing system and data bus structure and interfaces. Redundant and backup provisions are to be shown along with all crew controls and display devices.

3.5.2.4 Software Functional Flow Diagram

Using primarily the software requirements documentation, the analyst is to obtain or draw a software functional flow diagram that is to include the data management system software, application software, interfaces, data bus interface with hardware, crew controls, displays, alarm annunciation, and telemetry provisions.

3.5.2.5 Stimuli Analysis

A software stimuli analysis, keyed to an inventory of all command or control signals for the subsystem/system, is to be performed using the stimuli worksheet form (Figure C–4). Stimuli as used for this analysis are signals which are generated by the flight computers, flight crew (manual controls), launch processing system, or uplink for the purpose of stimulating or initiating an action by a hardware or software element. All stimuli for the designated subsystem are to be listed on the form and related data is to

be entered for appropriate columns. The stimuli identification numbers are contained in the MML document and also in related software requirement documentation. Hardware functional schematics also normally show these numbers for related signals.

3.5.2.5.1 Analysis Question

Pertinent information regarding adverse hardware/software interaction is to be noted in the remarks column. Questions to be considered for stimuli functions shall include:

a. Is the software compatible with hardware constraints and required hardware redundancy level?

b. Does software perform all necessary sequencing prior to generating stimulus?

c. Does software support capability for performing critical functions at a nominal level with any single component failed or with a portion of the subsystem inactivated and with any combination of two component failures or inactivated subsystems?

d. Is adequate redundant processing provided?

e. Can command signals be commandable to a known state independent of the current state?

f. Are keyboard controls adequate?

g. Is data bus and Interface Device (ID) redundancy adequate?

h. Is execution rate adequate?

i. Is Telemetry (TLM) provision adequate?

j. Is uplink processing provided and is it sufficient?

k. Is hardware safing required and provided by software?

3.5.2.6 Measurement Analysis

Software measurement analysis, keyed to an inventory of all measurements produced by subsystem/system hardware, is to be performed using the measurement worksheet form (Figure C–5).

Measurements as used for this analysis are signals which are needed directly or indirectly to provide data to the flight crew, the ground crew, or flight computers regarding a parameter pertaining to the state, performance, or condition of hardware elements or software computation. All measurements for the designated subsystem are to be listed

on the form and related data is to be entered for appropriate columns. Identification numbers for measurement are contained in the same documentation type and hardware drawings as for stimuli.

3.5.2.6.1 Analysis Questions

Pertinent information regarding adverse hardware/software interaction is to be noted in the remarks column. Questions to be considered for measurement functions shall include:

a. Is software redundancy management provided and is it adequate for fault detection, identification, and reconfiguration?

b. Is sampling rate of measurement adequate?

c. Is transient protection for measurement provided for?

d. Is computer, data bus, and ID redundancy adequate?

e. Is dedicated and Cathode–Ray Tube (CRT) display support adequate?

f. Is Fault Detection and Annunciation (FDA) and Caution and Warning (C/W) alarms adequate?

g. Is hardware Built–In Test Equipment (BITE) provided?

h. Is prelaunch and launch monitoring adequate?

i. Is TLM provision adequate?

j. Is sufficient scheme and data provided to support hardware checkout?

3.5.2.7 Reporting

A HR is to be prepared for each identified potential software–related hazard using the HR form and procedures specified in this document. Worksheets are to be submitted in accordance with the requirements of this document.

4.0 SOFTWARE CODE VERSUS REQUIREMENTS ANALYSIS

4.1 SCOPE

Software code versus requirements analysis is to be performed for all safety–critical flight and flight launch support software code. For the purposes of this procedure, software code is to include baseline versions, partial baseline versions, and configuration changes to these versions.

4.2 BACKGROUND

Software code versus requirements analyses performed to identify and resolve potential hazardous conditions resulting from software program errors. Using an analysis tool, a comparison is made between the documented software requirements and specification to the software code. The analysis technique converts software code into computer–plotted topological network trees depicting program logic flow and execution sequence. Clues are applied to the network trees to aid in determining inconsistencies between the software requirements/specifications and the code, and also to identify improper instruction sequences. Error conditions determined to have a potential safety impact are formally documented.

4.3 PROCEDURE

The analysis is to be performed on defined baselined software systems, portions of the baselined systems, and approved software changes. The procedure in general consists of acquiring the required data on the defined system, assuring correct correlation of documentation to code version, developing network trees, and identifying and documenting problem conditions. Specific tasks outlined in Paragraph 4.3.1 below are to be followed.

4.3.1 Data Acquisition

The following software deliverables and related documentation are to be obtained for the defined software system to be analyzed.

a. Software code on magnetic tape.

b. Functional and detail level software requirements documentation.

c. Approved software changes.

d. Software detail design specification.

e. Other software program documentation including module descriptions, flow diagrams, data structure definition.

f. Discrepancy reports, waivers, user notes.

g. Users guide, reference manuals for data processor and software language.

This task is to include assurance that the requirements and design documentation are of the correct issue/revision for the related version/release of the software code to be analyzed.

4.3.2 Network Tree Generation

The software code instructions are to be processed for entry into computerized algorithms which reduce the software program into topological network trees that identify all data and logic continuity paths. Hard–copy plots of network trees are to be produced.

4.3.3 Analysis

The analyst is to apply clues to the topographs (software patterns) identified in the network trees. The network trees are to be compared to the requirements/specifications and all miscomparisons are to be noted and categorized as problem or documentation error conditions.

4.3.4 Reporting

Problem conditions identified other than verified documentation errors are to be documented using the HR form and procedures specified in the document. The analyst identifying the problem is to complete the applicable portions/blocks of the hazard form including sufficient data that locates the problem area. Each identified problem condition is to be clearly described and recorded on a separate hazard form. Upon completion of the analysis on a software system, all observed documentation errors are to be summarized on a single hazard form for information with indication that they are not potential hazard–related conditions.

4.3.5 Software Change Analysis

Approved safety–critical software changes implemented in the code are also to be analyzed. The data acquisition and other tasks as previously described are to be followed. All network trees changed or affected by the changed network trees will be analyzed against the related changed requirements/design specifications.

FIGURE C–1

INADVERTANT RCS JET FIRING SOFTWARE FAULT TREE

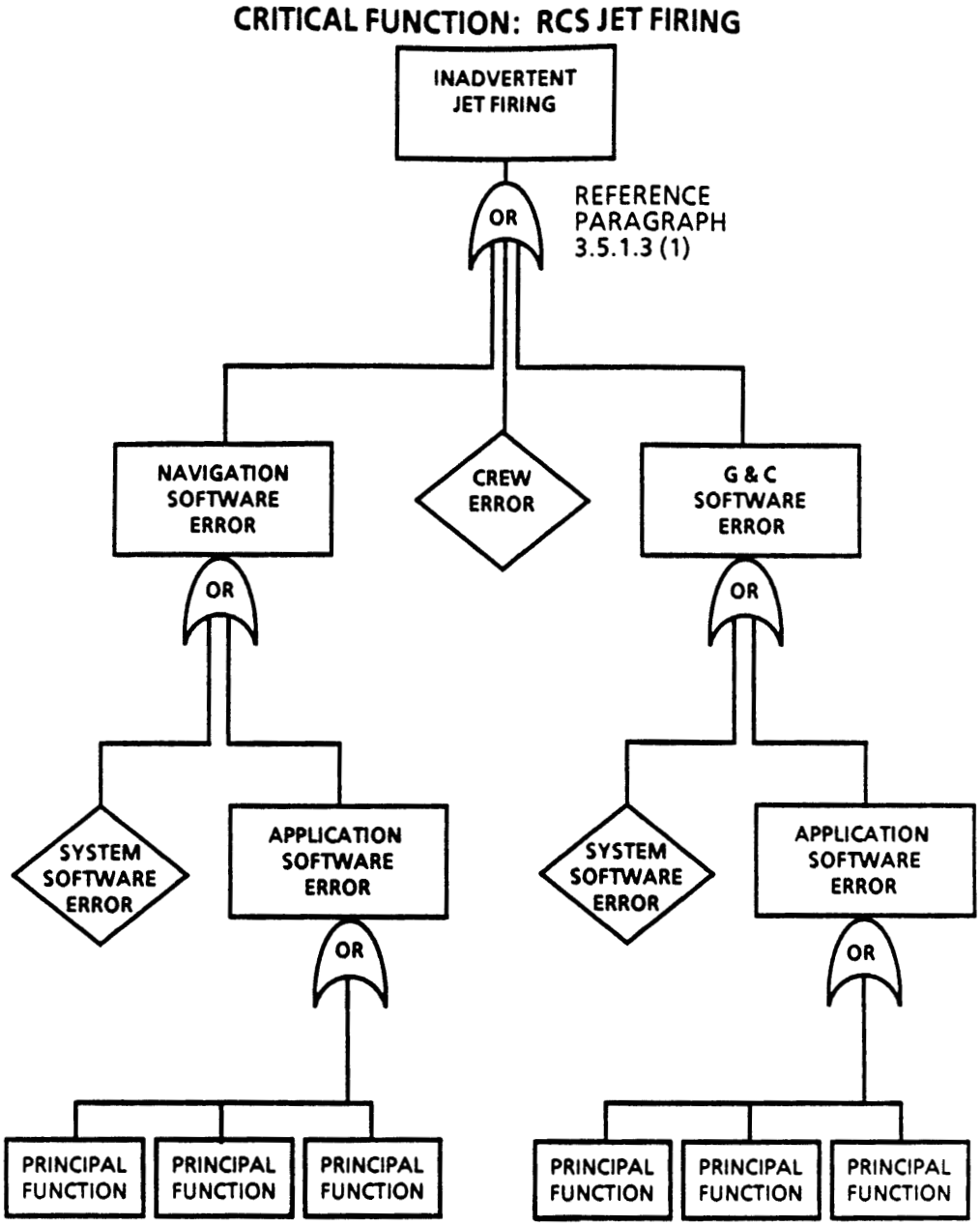


FIGURE C–2

CRITICAL FUNCTION TABLE

UNDESIRED EVENT	FLIGHT PHASE	POSSIBLE CAUSES	POTENTIAL HAZARD

FIGURE C–3

SYSTEM/SUBSYSTEM DEFINITION

SYSTEM/SUBSYSTEM DEFINITION

SYSTEM/SUBSYSTEM: Reaction Control System

CONFIGURATION DESCRIPTION

FUNCTIONAL DESCRIPTION

APPLICABLE DOCUMENTATION

FIGURE C–4

SOFTWARE STIMULI WORKSHEET

SYSTEM/SUBSYSTEM REACTION CONTROL SYSTEM

STIMULI	TITLE	REQUIREMENTS NUMBER & ABSTRACT	ID	TLM	MANUAL OVERRIDE	HARDWARE RESPONSE	REMARKS

FIGURE C–5

SOFTWARE MEASUREMENTS WORKSHEET

SYSTEM/SUBSYSTEM REACTION CONTROL SYSTEM

MEASUREMENT	TITLE	REQUIREMENTS NUMBER & ABSTRACT	ID	DED. DISPLAY	CRT	FDA	C & W/ ALARM	TLM	REMARKS

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

COMMON CAUSE FAILURE ANALYSIS

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 PURPOSE

A Common Cause Failure Analysis (CCFA) is used to determine if there are combined multiple failures of components and operator errors which result in degradation or disablement of a system and are set up by a common event or causative mechanism.

Common cause failures can affect redundant and interlocked design features in the system. When redundancy is provided by identical components, locations, or channels, susceptibility to common cause failures may be increased. For example, susceptibility of redundant systems to a failure with the same cause is seen when fire can burn away insulation of collocated wire bundles such that the wires short together and render inoperative a primary system and its backup.

Common cause failures need not occur simultaneously. Generally, they should be considered to coexist prior to maintenance checks or other procedures which might reasonably be expected to discover any part of the failure.

2.0 DESCRIPTION

The CCFA is directed toward the identification of multiple failures that may result from a single cause or event. These single secondary cause/events may result from a common process, manufacturing defect, an operator error, or external event. The analysis will identify the possible interaction of failures in independent redundant systems. Experience has shown that there is a finite list of common causes or events which should be checked. These typically deal with physical location and manufacturing characteristics such as common subjected environments, wire routing through a common connector or tray, common design processes which introduce a generic defect during manufacture, or susceptibility to common calibration errors because a defective instrument (or procedure) was used during installation or maintenance.

3.0 PROGRAM PHASE

Functional level CCFAs should be performed early in the project phase to identify critical items for design consideration. Detailed or component level CCFAs can be performed only after the detailed design is completed.

4.0 PROCEDURE

The CCFA begins with the development of a detailed system fault tree, and the identification of the minimum cut sets which will be analyzed. These cut sets are selected because they include critical components which may be susceptible to failure caused by some common element or condition such as collocation, environmental factors, common manufacturer, etc.

In the SSP, the identification of critical components to be evaluated by CCFA has already been accomplished. These components have been identified by FMEAs, and are classified as Criticality 1R and Criticality 2R.

The CCFA is prepared using three or four checklists in a three–step process. The first check made on a group of interdependent/redundant parts is to identify commonalities. The checklist for commonality identification can be tailored according to project, application boundaries, or experience. Generally, it appears as follows:

a. Commonality checklist

1. Location and environment

(a) Chassis

(b) Packaging/containment

(c) Elevation

2. Manufacture

(a) Part numbers

(b) Equipment name/item

(c) Process

(d) Calibration/test

3. Maintenance

(a) Period

(b) Calibration equipment

(c) Personnel

(d) Materials

4. Operations

(a) Status displays

(b) Inputs

Other entries such as TRANSPORTATION and INSTALLATION can be made. Subentries can be expanded, such as by adding THERMAL (COLD/HEAT), EXPOSURE, HUMIDITY, and VIBRATION to the ENVIRONMENT checks. Likewise, the subentries

can be expanded where necessary. For example, the ELEVATION item can involve checks for ATMOSPHERIC PRESSURE/CORONA or FLOODING.

b. For each commonality found, a second checklist is used to correlate possible critical conditions within the area of commonality. The critical condition checklist is of the following form:

   1. Electrical

      (a) Short

      (b) Open

      (c) Clocking

   2. Mechanical

      (a) Separation/shock

      (b) Welding

      (c) Obstruction

   3. Chemical, corrosives

   4. Biological

c. The next step in the process is to apply a third checklist to suggest credible accident–initiating events, mechanisms, or causes. At this point it should be realized that not every possible cause of a critical accident need be predetermined. There is no need to identify all contributing scenarios if a single credible cause of a critical accident can be foreseen. Corrective action should be instituted to prohibit design susceptibility for the whole class of conditions due to any trigger event. Therefore, the third checklist represents a search for a credible trigger event scenario:

   1. Conductive contaminant

   2. Mechanical shearing

   3. Fire/Explosion

   4. Flood

   5. Loss of cooling

   6. Dust/grit

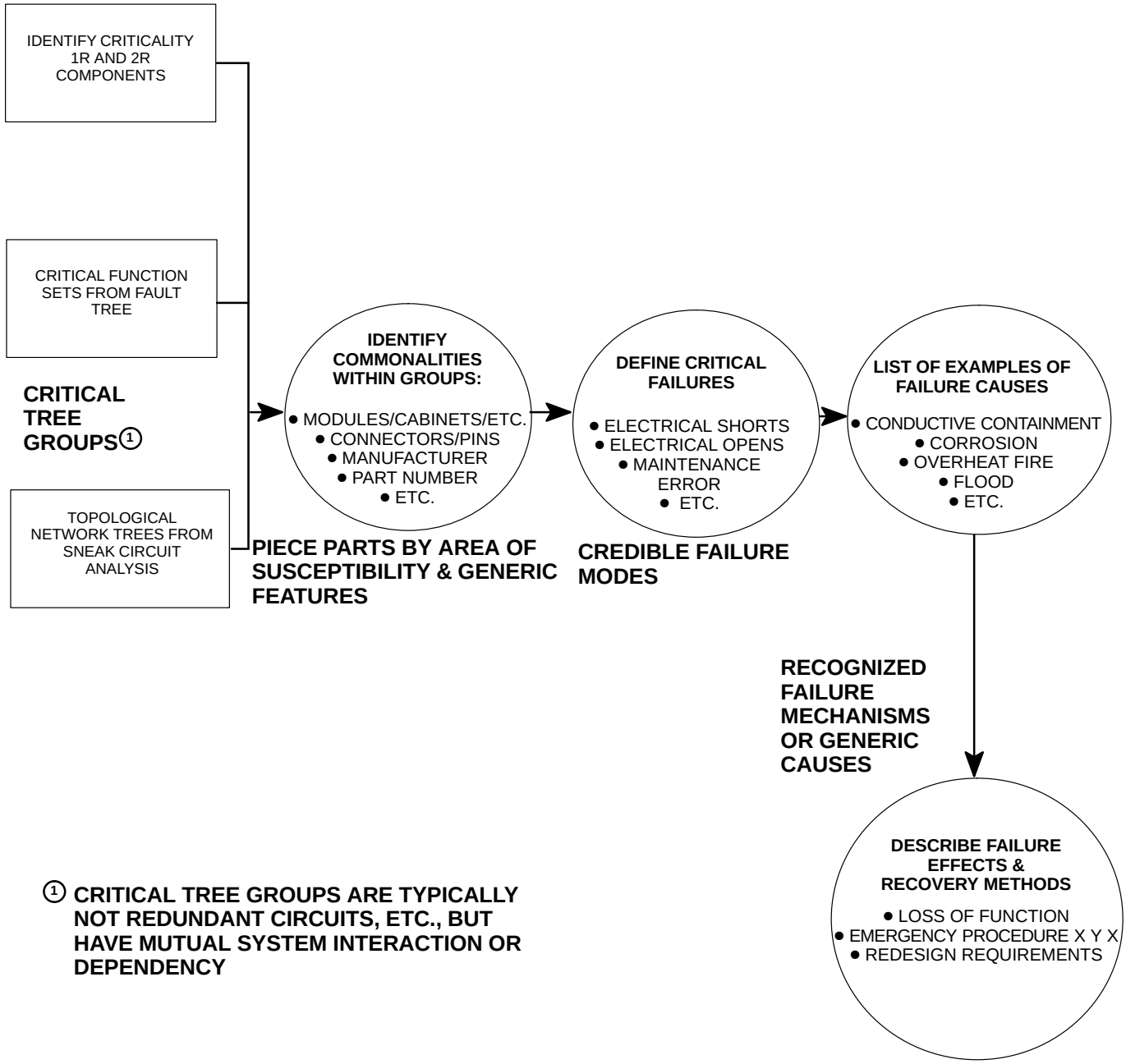
d. Again, each entry can be broken down. For example, CONDUCTIVE CONTAMINANT can represent FLUIDS (saltwater and acid) and METAL TRIMMINGS. Sources for each trigger event can also be postulated with a fourth checklist, if desired, but this is usually unnecessary.

As with any analytical effort, no useful result is produced unless each significant activity is documented. Results must be recorded and tracked through appropriate resolution; otherwise, something may be overlooked or the corrective action may introduce a worse situation. Any kind of tracking form can be used to document the coverage of the effort, but significant hazards with their associated accident scenarios generally should be separately reported, illustrated, numbered, and tracked as high–risk items.

The approach to CCFA is shown in Figure D–1. The effort is performed in four steps. First, all commonalities between the trees/components are identified and listed. These commonalities may be shared connectors; common locations in terms of modules, cabinets, or wire bundles; or more generic features, such as common manufacturer or other characteristics. The second step is to determine the credible failure modes or piece parts within each tree or component. Examples of failure modes might be electrical shorts, electrical opens, maintenance errors or calibration errors. The third step requires documentation of at least one credible cause of each failure mode identified in the second step. It is not productive to try to list all possible causes of such failure modes, but listing at least one credible initiating event should suffice to show the need for design improvement. Comprehensive risk assessment may vary widely with each particular trigger mechanism that is suggested. Any resulting design modification should obviate the functional susceptibility to similar causes. Examples of the causes to be listed in the third step would be conductive contaminants, overheat, fire, floods, or other mechanisms which could cause the electrical shorts, opens, maintenance errors and calibration errors. The last step of this procedure is to describe the failure effects and recovery methods for the items listed in the second step. This is documented on a form for subsequent tracking, risk assessment, and resolution as illustrated in Figure D–2.

FIGURE D–1

COMMON CAUSE FAILURE ANALYSIS FLOW



① CRITICAL TREE GROUPS ARE TYPICALLY NOT REDUNDANT CIRCUITS, ETC., BUT HAVE MUTUAL SYSTEM INTERACTION OR DEPENDENCY

FIGURE D–2

CCFA TRACKING AND RESOLUTION FORMAT

(PROJECT) COMMON CAUSE FAILURE ANALYSIS

CRITICAL FUNCTION SET	COMMONALITY	CRITICAL EVENT	POTENTIAL CAUSE	EFFECT	REMARKS
DOOR & SPEED CONTROL					
2–A) T_{38}–LEFT SIDE DOOR	CONNECTOR DJ2	ELECTRICAL SHORTS:	1) CONDUCTIVE CONTAINMENT	LEFT SIDE DOORS DRIVEN OPEN AND EMERGENCY BRAKES INHIBITED.	VIOLATION OF DESIGN CRITERIA REDESIGN RECOMMENDED.
3–B) T_{102}– EMERGENCY BRAKES		PINS H–J–K	2) METALLIC SHEARING OF WIRE BUNDLE	DOORS 1 & 3 DRIVEN OPEN.	ADJACENT PINS CREDIBLE.
		PINS C–J–Y		DOORS 3 & 7 DRIVEN OPEN.	PINS NOT ADJACENT.

APPENDIX E

SAFETY ANALYSIS REPORT (EXAMPLE)

THIS PAGE INTENTIONALLY LEFT BLANK

SAFETY ANALYSIS REPORT

FOR

Enter Name of Item Report is Being Written On

Enter Current Date

Prepared By:

Enter Name of Preparer and Organization

Approved By:

Enter name and organization of safety representative approving Safety Analysis Report and provide signature block (include date)	Enter name of hardware manager responsible for hardware and provide signature block (include date)

PREFACE

Provide background data on the hardware, software, environment or operation being analyzed. State how this analysis fits into other analyses.

NOTE: When preparing the SAR, start each section on a separate page.

1.0 INTRODUCTION.

1.1 BACKGROUND.

Provide background data on the hardware, software, environment or operation being analyzed. State how this analysis fits into other analyses.

1.2 PURPOSE.

Give the purpose of the analysis.

1.3 SCOPE.

Define the scope of the analysis.

1.4 DEFINITIONS.

Provide any definitions that will be helpful in clarifying the report and are peculiar to Safety.

2.0 SUMMARY OF SAFETY ANALYSIS (SA).

2.1 SUMMARY OF SA METHODOLOGY.

2.2 GROUNDRULES AND ASSUMPTIONS USED DURING THE ANALYSIS.

2.3 SUMMARIZE SIGNIFICANT FINDINGS.

3.0 HAZARD DISCUSSIONS/STATUS.

Record how many hazards identified and how many are eliminated, open, controlled and accepted risk candidates.

3.1 OPEN HAZARD STATUS SUMMARY.

Record open number, title, description and status. Include the following data under status:

a. Action item description

b. Action organization, persons name/phone number

c. Date action is due

3.2 CANDIDATE ACCEPTED RISK SUMMARY.

Record accepted risk ID number, title, description, acceptance rationale, and reference Hazard Report by number.

NOTE: When preparing the SAR, start each appendix on a separate page.

APPENDIX A Abbreviations

Provide a list of abbreviations used in the report.

APPENDIX B Acronyms

Provide a list of acronyms used in the report.

APPENDIX C Waivers/Deviations

Include summary of waivers and deviations associated with this Hazard Analysis.

APPENDIX D Hazard Reports and Hazard Report Worksheets

Copies of Hazard Reports or Hazard Analysis Worksheets with actions required for closure.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F

GLOSSARY OF TERMS

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F

GLOSSARY OF TERMS

Accident . As defined in NHB 5300.4(1D–2), "An unplanned event which results in an unsafe situation or operational mode."

Component. As defined in NHB 5300.4(1D–2), "A combination of parts, devices, and structures, usually self–contained, which performs a distinctive function in the operation of the overall equipment. A 'black box' (e.g., transmitter, encoder, cryogenic pump, star tracker)."

Contractor Furnished Equipment (CFE). CFE is that equipment provided to a NASA center by its prime contractor.

Contributing Factor(s). Other factors that must be involved in order for the consequence to be provided.

Corrective Action. As defined in NHB 5300.4(1D–2), "Action taken to preclude occurrence of an identified hazard or to prevent recurrence of a problem."

Critical Item. A single failure point and/or a redundant element in a life or mission–essential application where:

a. Redundant elements cannot be checked out during the normal ground turnaround sequence.

b. Loss of a redundant element is not readily detectable in flight.

c. All redundant elements can be lost by a single credible cause or event such as contamination or explosion.

Critical Items List (CIL). A listing comprised of all critical items identified as a result of performing the Failure Modes and Effects Analysis (FMEA). (See definition for critical item.)

Criticality. The categorization of a hardware item by the worst case potential direct effect of failure of that item. In assigning hardware criticality, the availability of redundancy modes of operation is considered. Assignment of functional criticality, however, assumes the loss of all redundant hardware elements.

Criticality Categories.

Category	Definition
1	Loss of life or vehicle.

1R	Redundant hardware element the failure which could cause loss of life or vehicle.
1S	Potential loss of life or vehicle due to failure of a safety or hazard monitoring system to detect, combat, or operate when required.
2	Loss of mission; for GSE, loss of vehicle system.
2R	Redundant hardware elements the failure of which could cause loss of mission.
3	All others.

Design Safety. Safety achieved by integration of safety features into a system or subsystem to prevent operation except in the manner intended by the designer.

Failure. As defined in NHB 5300.4(1D–2), “The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.”

Failure Modes and Effects Analysis (FMEA). A systematic, methodical analysis performed to identify and document all identifiable failure modes at a prescribed level and to specify the resultant effect of the failure mode at various levels of assembly.

Fault Tree Analysis (FTA). A graphic representation of a logical thought process used to analyze an undesired event. Using inductive logic, all causes that can lead to the undesired, or top event are listed on an inverted “tree”. These causes then become events for which causes are listed. This analysis is continued to determine all the events and combinations of events that can lead to the top event.

Generic Hazards. Those hazard groups that may be present in the design or use of equipment, generally including hazard causes from the environment, collision, fire/explosion (explosion/implosion), vibration/shock/acoustic effects, thermal effects, contamination, radiation, electrical discharge, biological/physiological/psychological impact, toxicity and other general items.

Government Furnished Equipment (GFE). Equipment in the possession of or acquired directly by the Government and delivered or otherwise made available to a non–Government organization.

Ground Support Equipment (GSE). Equipment and associated software required to provide ground support, such as monitoring or controlling a specific activity or phase of vehicle assembly, test, checkout, or launch.

Hazard. The presence of a potential risk situation caused by an unsafe act or condition.

Hazard Analysis (HA). The determination of potential sources of danger and recommended resolutions in a timely manner for those conditions found in either the

hardware/software systems, the person–machine relationship, or both, which cause loss of personnel capability, loss of system, or loss of life or injury to the public.

Hazard Report (HR). The output of a Hazard Analysis for a specific hazard which documents the hazard title, description causes, control, verification, and status.

Hazard Report Closure Classification.

a. Eliminated Hazard – A hazard that has been eliminated by completely removing the hazard causal factors.

b. Controlled Hazard – A hazard for which the frequency of occurrence and/or severity level have been reduced by implementing the appropriate hazard reduction precedence sequence to comply with program requirements.

c. Accepted Risk – A hazard for which the controls for one or more hazard causes fail to meet the hazard reduction precedence sequence and therefore, have limitations or uncertainties such that the hazard could occur during the life of the program. The following are examples of conditions that could be considered accepted risk hazards:

    1. Critical Single Failure Point.

    2. Limited controls, or controls that are subject to human error or interpretation.

    3. System designs or operations that do not meet industry or Government standards.

    4. Complex fluid system leaks.

    5. Safety detection and suppression devices which are not adequate.

    6. Uncontrollable random events which could occur even with established precautions and controls in place, such as weather or fires.

Hazard Report Status.

a. Closed – Corrective action to eliminate or control the hazard has been implemented or scheduled for implementation. Program management accepts the risk pending completion of corrective action and verification. Baselining by the PRCB is required to approve a HR as closed.

b. Open – A HR status is open when corrective action to eliminate or control the hazard has not been completed and the corrective action is not scheduled to be performed.

Loss of Personnel Capability. As defined in NHB 5300.4(1D–2), “Loss of personnel function resulting in inability to perform normal or emergency operations. Also includes loss or injury to the public.”

Loss of Vehicle System. As defined in NHB 5300.4(1D–2), “Loss of the capability to provide the level of system performance required for normal or emergency operations.”

Mission Events. Time–oriented flight operations defined in flight checklists.

Natural Environment. Element of nature that can affect an element/system event, process, or activity such as temperature, pressure, wind, solar radiation, lightning, fog, humidity, ice, dew, rain, hail, icing, sleet, snow, frost, saltspray, sand, dust, clouds, and fungus.

Operating and Support Hazard Analysis (O&SHA). As described in NHB 1700.1(V1–A) and this document, the O&SHA is to identify hazards and recommend risk reduction alternatives in procedurally controlled activities during all phases of intended use.

Preliminary Hazard Analysis (PHA). As described in NHB 1700.1(V1–A) and this document, the PHA is to identify safety–critical areas, to identify and evaluate hazards, and to identify the safety design and operation requirements needed in the program concept phase.

Residual Risk. Risk that remains after all mitigation has been applied (hazard reduction precedence sequence). Procedurally controlled hazards contain residual risks.

Risk. As defined in NHB 5300.4(1D–2), “The chance (qualitative) of loss of personnel capability, loss of system, or damage to or loss of equipment or property.”

Risk Assessment. The process of qualitative risk categorization or quantitative risk elimination, followed by evaluation of risk significance.

Risk Visibility. The documentation of a risk related to hardware, operations, procedures, software, and environment that provides safety, project offices, and program management with the ability to evaluate accepted risks associated with planned operations.

Safety. As defined in NHB 5300.4(1D–2), “Freedom from chance of injury or loss of personnel, equipment or property.”

Safety Analysis (SA). A systematic and orderly process for the acquisition and evaluation of specific information pertaining to the safety of a system.

Safety Analysis Report (SAR). A SAR is a document prepared to document the results of a hazard analysis performed on a system, subsystem or operation. The specific minimum data elements for a SAR will be defined by data deliverable requirements for the program or project.

Safety Critical. As defined in NHB 5300.4(1D–2), “Facility, support, test, and flight systems containing:

a. Pressurized vessels, lines, and components.

b. Propellants, including cryogenics.

c. Hydraulics and pneumatics.

d. High voltages.

e. Radiation sources.

f. Ordnance and explosive devices or devices used for ordnance and explosive checkout.

g. Flammable, toxic, cryogenic, or reactive elements or compounds.

h. High temperatures.

i. Electrical equipment that operates in the area where flammable fluids or solids are located.

j. Equipment used for handling program hardware.

k. Equipment used for personnel walking and work platforms.”

Severity Levels. The severity level is an assessment of the most severe effect(s) of a hazard. Severity level will be categorized as follows:

a. Catastrophic – Hazard could result in a mishap causing fatal injury to personnel, and/or loss of one or more major elements of the flight vehicle or ground facility.

b. Critical – Hazard could result in serious injury to personnel and/or damage to flight or ground equipment which would cause mission abort or a significant program delay.

c. Marginal – Hazard could result in a mishap of minor nature inflicting first–aid injury to personnel, and/or damage to flight or ground equipment which can be tolerated without abort or repairing without significant program delay.

Single Failure Point (SFP). As defined in NHB 5300.4(1D–2), “A single item of hardware, the failure of which would lead directly to loss of life, vehicle or mission. Where safety considerations dictate that abort be initiated when a redundant item fails, that element is also considered a single failure point.”

Sneak Analysis (SA). An analysis technique for discovering unplanned modes of operations or latent conditions that cause unexplained problems, unwanted functions to

occur, unrepeatable glitches or anomalies, or inhibits a desire function without regard to component failure in electrical hardware and software systems.

Space Shuttle Program (SSP). An integrated system consisting of the Space Shuttle (Orbiter, External Tank, Solid Rocket Booster, and flight kits, upper stages, Spacelab, and any associated flight hardware and software.)

Subsystem Hazard Analysis (SSHA). As described in NHB 1700.1(V1–A) and this document. The SSHA is to identify hazards to personnel, vehicle and other systems caused by loss of function, energy source, hardware failures, personnel action or inactions, software deficiencies, interactions of components within the subsystem, inherent design characteristics such as sharp edges, and incompatible materials, and environmental conditions such as radiation and sand.

System Engineering. The process of applying science and technology to the study and planning of a system so that the relationships of various parts of the system and the use of various subsystems are fully established before designs are committed.

System Hazard Analysis (SHA). As described in NHB 1700.1(V1–A) and this document. The SHA is identical to the SSHA but at the system level. Once the subsystem levels have been established, a combination of subsystems comprise a system. In turn, a group of systems may comprise another system until the top system is identified.

System Safety. As defined in NHB 5300.4(1D–2), “The optimum degree of risk management within the constraints of operational effectiveness, time and cost attained through the application of management and engineering principles throughout all phases of a program.”

User. Identified and authorized NASA, element contractor, or integration contractor personnel; flight crew equipment analyst; Orbiter experiments analyst; payload accommodations analyst; detailed secondary objective analyst; or RMS analyst (not inclusive) that have necessary access to the intercenter hazard data base system.

APPENDIX G

ACRONYMS AND ABBREVIATIONS

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G

ACRONYMS AND ABBREVIATIONS

CAR	Change Action Request
CCB	Configuration Control Board
CCFA	Common Cause Failure Analysis
CDR	Critical Design Review
CFE	Contractor Furnished Equipment
CIL	Critical Items List
CR	Change Request
DSO	Detailed Secondary Objectives
DTO	Detailed Test Objectives
ECP	Engineering Change Proposal
FDF	Flight Data File
FMEA	Failure Modes and Effects Analysis
FR	Flight Rules
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GSE	Ground Support Equipment
HA	Hazard Analysis
HR	Hazard Report
ICB	Integration Control Board
ICHA	Integrated Cargo Hazard Analysis
ID	Interface Device
IFA	In–flight Anomaly
IPR	Interim Problem Report
LCC	Launch Commit Criteria
MSA	Management Safety Assessment
MUSA	Mission Unique Safety Assessment

OEX	Orbiter Experiments
OMI	Operations and Maintenance Instruction
OMRSD	Operational Maintenance Requirements and Specifications Document
O&SHA	Operating and Support Hazard Analysis
PCASS	Program Compliance Assurance and Status System
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PIRN	Preliminary Interface Revision Notice
PMMT	Program Mission Management Team
PR	Problem Report
PRCB	Program Requirements Control Board
RCN	Requirements Change Notice
SA	Safety Analysis
	Sneak Analysis
SAR	Safety Assessment Report
	Safety Analysis Report
SCN	Specification Change Notice
SFP	Single Failure Point
SHA	System Hazard Analysis
SR	System Review
SR&QA	Safety, Reliability and Quality Assurance
SSHA	Subsystem Hazard Analysis
SSID	Subsystem Identification
SSP	Space Shuttle Program
SSPO	Space Shuttle Program Office
SSRP	System Safety Review Panel

APPENDIX H

DATA FIELD DESCRIPTIONS

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H

DATA FIELD DESCRIPTIONS

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<1a>	HAZARD REPORT NUMBER	25	YES	CHAR	
<1b>	REVISION LETTER	2	YES	CHAR	AA–ZZ
<1c>	DCN NUMBER	5	NO	CHAR	Blank is acceptable
<2>	PREP/REVISION DATE	10	NO	DATE	yyyy/mm/dd
<3>	HAZARD REPORT STATUS	1	YES	CHAR	"O" or "C"
<4>	TITLE	148	YES	TEXT	
<5a>	SYSTEM	20	YES	CHAR	(See acronym list)
<5b>	SUB–SYSTEM	20	NO	CHAR	
<5c>	COMPONENT	20	NO	CHAR	
<6>	VEHICLE EFFECTIVITY	14	YES	CHAR	Format OV–10n,n,n,n,n or "ALL" or "NONE" ET–XXX, BIO XXX
<7>	MISSION PHASE	25	YES	CHAR	Prelaunch, Engine Start, Pad Abort, Launch Boost Separation, MECO, ET SEP, ON–Orbit, TAL, RTLS, AOA, etc.
<8>	HAZARDOUS CONDITION DESCRIPTION	60,840 (780 lines X 78 chars/line)	YES	TEXT	
<9>	ACCEPTANCE RATIONALE	45,240 (580 lines X 78 chars/line)	YES	TEXT	
<10>	ACCEPTED RISK CAUSES	15,600 (200 lines X 78 chars/line)	NO	TEXT	
<13>	CAUSE(S)	60,840	YES	TEXT	
<13a>	CAUSE PARAGRAPH #	20	NO	TEXT	
<14>	EFFECT(S)	60,840	YES	TEXT	
<14a>	EFFECT PARAGRAPH #	20	NO	TEXT	
<15>	CONTROL(S)	60,840	YES	TEXT	
<15a>	CONTROL PARAGRAPH #	20	NO	TEXT	
<16>	VERIFICATION(S)	60,840	YES	TEXT	
<16a>	VERIFICATION PARAGRAPH #	20	NO	TEXT	

DATA FIELD DESCRIPTIONS – (Continued)

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<17>	SEVERITY LEVEL	12	YES	CHAR	"Marginal", "Critical", or "Catastrophic"
<18>	LIKELIHOOD OF OCCURRENCE	10	YES	CHAR	"Improbable", "Remote", "Infrequent", or "Probable"
<19>	CLASSIFICATION	4	YES	CHAR	"Elm", "Cont", or "A/R"
<11>	HAZARD REPORT CLOSURE CLASSIFICATION	N/A	N/A	N/A	Generated by PCASS, worst case from Risk Matrix
<12a>	HAZARD REPORT SEVERITY	N/A	N/A	N/A	Generated by PCASS, worst case from cause severities, one dimension of Risk Matrix
<12b>	HAZARD REPORT LIKELIHOOD OR OCCURRENCE	N/A	N/A	N/A	Generated by PCASS, worst case from cause likelihoods, one dimension of Risk Matrix
<20>	SAFETY REQUIREMENTS	60,840	YES	TEXT	
<21>	INTERFACES	30	NO	CHAR	Primary System
<21a>	SYSTEM INTERFACES	30	NO	CHAR	
<21b>	RESPONSIBLE AGENCY 1 SRB	18	NO	CHAR	
<21c>	RESPONSIBLE AGENCY 2 SRM	18	NO	CHAR	
<21d>	RESPONSIBLE AGENCY 3 ET	18	NO	CHAR	
<21e>	RESPONSIBLE AGENCY 4 ORB	18	NO	CHAR	
<21f>	RESPONSIBLE AGENCY 5 SSME	18	NO	CHAR	
<21g>	RESPONSIBLE AGENCY 6 L&L	18	NO	CHAR	
<22>	CIL	—	—	—	Cross reference to related CIL items
<22a>	CIL NUMBER	20	NO	CHAR	
<22b>	CIL PROJECT ELEMENT	8	N0	CHAR	
<22c>	CIL REVISION DATE	10	NO	DATE	
<22d>	CRITICALLY	Per CIL Table	NO	CHAR	

DATA FIELD DESCRIPTIONS – (Continued)

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<22e>	ITEM	Per CIL Table	NO	CHAR	
<22f>	FAILURE MODE	Per CIL Table	NO	CHAR	
<23>	OMRSD	25	NO	CHAR	
<23a>	OMRSD FILE	2	NO	CHAR	
<23b>	OMRSD VOLUME	1	NO	CHAR	
<23c>	OMRSD REQ NUMBER	25	YES	CHAR	
<23d>	OMRSD TITLE	144	NO	CHAR	PCASS Name DESCRIPTION COL
<24>	OMI	18	NO	CHAR	Required when OMRSD not imposed and OMI required for hazard control verification
<24a>	OMI NUMBER	18	YES	CHAR	
<24b>	OMI TITLE	150	NO	CHAR	PCASS Name OMI_COMMENTS_COL
<25>	LAUNCH COMMIT CRITERIA	—	—	—	Mandatory for all LCCs used as controls
<25a>	SUBSYSTEM IDENTIFICATION (SSID) NUMBER	9	NO	CHAR	
<25b>	LCC REVISION	2	N0	CHAR	
<25c>	LCC MISSION INDEX	2	NO	CHAR	
<25d>	LCC SECTION NUMBER	2	NO	CHAR	
<25e>	LCC TITLE	108	NO	CHAR	PCASS Name: LCC_VIOLATION_CALL
<25f>	LCC SECTION TITLE	55	NO	CHAR	
<26>	CREW PROCEDURES DOCUMENT	18	NO	CHAR	
<26a>	FLT_DATA_FILE BOOK	18	NO	CHAR	
<26b>	FDF PROCEDURES NAME	25	NO	CHAR	
<27>	FLIGHT RULES	—	—	—	All FRs used as controls
<27a>	FLIGHT RULE NUMBER	18	NO	CHAR	

DATA FIELD DESCRIPTIONS – (Continued)

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<27b>	FLIGHT RULE TITLE		NO	CHAR	
<28>	BACKGROUND	60,840	YES	TEXT	Support documentation hazard history
<none>	NSTS_ELEMENT_ COD	4	YES	CHAR	ORB, SSME, ET, SRB, RSRM, L&L, INTG
<none>	LOAD_DATE	10	YES	DATE	Date Hazard Report was entered via data entry screens
<none>	LOAD_TIME	8	YES	TIME	Time Hazard Report was entered via data entry screens
<none>	EXTRACT_DATE	10	YES	DATE	Date Hazard Report was extracted from MSFC PCASS data base
<none>	EXTRACT_TIME	8	YES	TIME	Time Hazard Report was extracted from MSFC PCASS data base
<none>	ORGANIZATION	14	YES	CHAR	Center responsible for hardware (e.g., KSC, VAFB, NRUP, etc.)
<none>	PROGRAM MODEL NUMBER 1	15	NO	CHAR	Model number of equipment related to hazard
<none>	PROGRAM MODEL NUMBER 2	15	NO	CHAR	
<none>	PROGRAM MODEL NUMBER 3	15	NO	CHAR	
<none>	PART_NUMBER	30	NO	CHAR	Part number impacted by the hazard
<none>	LRU	30	NO	CHAR	
<none>	SOW_COMP_DATE	10	NO	DATE	Date work was completed for each of the actions required to close the hazard
<none>	PRIMARY_SYSTEM	30	NO	CHAR	Name of system that may be impacted by hazard or cause of hazard
<none>	CHRONOLOGY_ DATE	10	NO	DATE	Date updates were made and logged for Hazard Report
<none>	CHRONOLOGY_ SUMMA	936	NO	CHAR	Description of updates made to hazard
<none>	KEYWORD	25	NO	CHAR	Keywords which describe key elements of hazard (e.g., rupture, fire, explosion, tank, etc.)
<none>	CONTRACTOR_ DATE 1	10	NO	DATE	Date Hazard Report was approved by 1st contractor

DATA FIELD DESCRIPTIONS – (Continued)

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<29>	STATUS OF OPEN WORK	—	—	—	—
<29a>	IDENTIFICATION OF OPEN WORK	2	NO	CHAR	
<29b>	RESPONSIBLE AGENCY	18	NO	CHAR	
<29c>	ACTION REQUIRED	702	NO	CHAR	
<29d>	DUE DATE	10	NO	DATE	yyyy/mm/dd; required if open work is constraints to mission milestone
<30>	PREPARING ENGINEER	20	YES	CHAR	
<30a>	PREP_ENG_DATE	10	YES	DATE	
<31>	ORIGINATOR/CON-TRACTOR DESIGN ENGINEER	24	YES	CHAR	
<32>	ORIGINATOR/CON-TRACTOR SAFETY ENGINEERING MAN-AGER	24	YES	CHAR	
<33>	NASA SUBSYSTEM MANAGER	24	NO	CHAR	
<34>	NASA PROJECT SAFETY	24	NO	CHAR	
<none>	PROJECT APPROVE DATE	10	YES	DATE	yyyy/mm/dd
<none>	SSRP DATE	10	NO	DATE	yyyy/mm/dd
<none>	PRCBD CR/SR NO. OR ROUTINE NO.	15	YES	CHAR	PRCBD approving directive number or SR number if appli-cable; otherwise, for routine updates enter rxyy/mm/dd where r = Routine; x = Element Project alpha (B = Booster, E = Engine, G = GFE, I = Integration, L = Launch & Landing, M = Motor, O = Orbiter, S = Shuttle/Mir, T = Tank); followed by the eight–digit report date assigned by HR originator/ contractor in the following order: year/month/day.
<none>	DATE	10	NO	DATE	PRCB CR/SR or routine date (yyyy/mm/dd).

DATA FIELD DESCRIPTIONS – (Continued)

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<none>	PCIN	15	NO	CHAR	Program Change ID Number
	EXCEPTION(S)	—	—	—	
<none>	EXCEPTION NUMBER	10	NO	CHAR	
<none>	PRCBD NUMBER	15	NO	CHAR	PRCBD number of exception
	WAIVER(S)	—	—	—	—
<none>	WAIVER NUMBER	10	NO	CHAR	
<none>	PRCBD NUMBER	15	NO	CHAR	PRCBD number of waiver
	DEVIATION(S)	—	—	—	—
<none>	DEVIATIONS NUMBER	10	NO	CHAR	
<none>	PRCBD NUMBER	15	NO	CHAR	PRCBD number of deviation
<none>	RELATED_HR_ NUMBER	25	NO	CHAR	
<none>	CONTRACTOR_ DATE 2	10	NO	DATE	Date Hazard Report was approved by 2nd contractor
<none>	CONTRACTOR_ DATE 3	10	NO	DATE	Date Hazard Report was approved by 3rd contractor
<none>	SAFETY_DATE	10	NO	DATE	Date Hazard Report was approved by Safety Office
<none>	CCB_SIGN	24	NO	CHAR	Name of reviewer for CCB
<none>	ICB_SIGN	24	NO	CHAR	Name of reviewer for ICB
<none>	ICB_DATE	10	NO	DATE	Date approved by ICB
<none>	SSRP_ACTION_REQ	1	NO	CHAR	Indicates if SSRP action is required, "x" = yes, blank = no
<none>	SSRP_MIN_NUM	10	NO	CHAR	Control number of SSRP minutes which document SSRP approval
<none>	SSRP DATE	10	NO	DATE	SSRP DATE when Hazard Report was approved by SSRP
<none>	PRCB_ACTION_ REQ	1	NO	CHAR	Indicates if PRCB is required, "x" = yes, blank = no
<none>	PRCB_DOC_RPT_ DATE	10	NO	DATE	Hazard Report date in effect when Hazard Report was approved by PRCB
<none>	OTHER_DOCUMENTS	936	NO	CHAR	Description of other documentation available for this hazard
	IMAGES (FAULT TREES, DRAWINGS, ETC.)	—	—	—	Loading into PCASS is currently a manual process

APPENDIX H

DATA FIELD DESCRIPTIONS – (Concluded)

REF #	COLUMN NAME	SIZE	REQ'D	PRE–FERRED TYPE	COMMENTS
<none>	IMAGE NAME	8	NO	CHAR	Must be unique when combined with Hazard Report Number, Revision Letter, and DCN Number
<none>	SCANNED IMAGE	N/A	NO	TIFF (TAG IMAGE FILE FORMAT)	

PREFERRED TYPE:

CHAR: Means alphanumeric with any letters stored as upper case

TEXT: Means mixed upper/lower case alphanumerics

DATE: Means a date field with yy/mm/dd format

TIME: Is HH:MM:SS expressed as Eastern Time zone (either EST or EDT)

THIS PAGE INTENTIONALLY LEFT BLANK