National Aeronautics and
Space Administration

CXP 70038
Revision: Baseline
EFFECTIVE DATE: June 30, 2006

Constellation Program Office
Lyndon B. Johnson Space Center
Houston, TX 77058

HAZARD ANALYSES METHODOLOGY

Approved for Public Release; Distribution is Unlimited

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline			Baseline Release.

METHODOLOGY FOR CONDUCT OF PROJECT CONSTELLATION HAZARD ANALYSES

Signature Page

SUBMITTED BY:

_____ _____

Name *Date*
Title/Function
Organization

APPROVED BY:

_____ _____

Name *Date*
Title/Function
Organization

_____ _____

Name *Date*
Title/Function
Organization

_____ _____

Name *Date*
Title/Function
Organization

TABLE OF CONTENTS

1.0 INTRODUCTION 8

1.1 Purpose 8

1.2 Scope 8

2.0 APPLICABLE DOCUMENTS AND REFERENCE DOCUMENTS 9

2.1 Applicable Documents 9

2.2 Reference Documents 9

3.0 DEFINITIONS AND ACRONYMS 10

3.1 Definitions 10

3.2 Acronyms and Abbreviations 16

4.0 HAZARD ANALYSES REQUIREMENTS 18

4.1 Hazard Reduction Order of Precedence 18

4.1.1 Design for minimum hazards 18

4.1.2 Incorporate Safety Devices 18

4.1.3 Provide caution and warning devices 18

4.1.4 Develop and implement special procedures 19

4.2 Minimizing Hazards 19

4.2.1 Fault Tolerance 19

4.2.2 Design for Minimum Risk 19

5.0 HAZARD ANALYSES DEVELOPMENT EVOLUTION 20

5.1 Phase Descriptions 20

5.1.1 Concept Development (Phase A) 20

5.1.2 Preliminary Design (Phase B) 21

5.1.3 Final Design (Phase C) 21

5.1.4 Fabrication, Assembly and Test (Phase D) 21

5.1.5 Operational and Sustaining Engineering Phase (Phase E) 22

5.2 Integrated Hazards 22

6.0 HAZARD REPORTS 23

6.1 Purpose 23

6.2 HA Review Process 23

6.3 Standardized Data Elements 23

6.4 Maintaining Hazard Reports 23

7.0 SAFETY ANALYSIS REPORT 26

8.0 MISSION SAFETY ASSESSMENT 27

8.1 Purpose 27

8.2 Content....27

8.3 Timing....28

A APPENDIX A - HAZARD ANALYSIS TYPES AND TECHNIQUES 29

A.1. Preliminary Hazards Analysis (PHA) 29

A.1.1. Purpose....29
A.1.2. Description 29
A.1.3. Project Phase....30
A.1.4. Technique....30

A.2. Subsystem Hazard Analyses (SSHA) 39

A.2.1. Purpose....39
A.2.2. Description 39
A.2.3. Project Phase....39
A.2.4. Technique....39

A.3. System Hazard Analyses (SHA)....41

A.3.1. Purpose....41
A.3.2. Description 41
A.3.3. Project Phase....41
A.3.4. Technique....41

A.4. Operating and Supporting Hazard Analyses (O&SHA) 42

A.4.1. Purpose....42
A.4.2. Description 42
A.4.3. Project Phase....43
A.4.4. Technique....43

A.5. Software Hazard Analyses (SWHA) 45

A.6. Integrated Hazard Analysis (IHA) 46

A.6.1. Purpose....46
A.6.2. Description 46
A.6.3. Project Phase....46
A.6.4. Technique....46

B APPENDIX B – FAULT TREE ANALYSIS 47

B.1. Fault Tree Analysis Process 47

B.1.1. Purpose....47
B.1.2. Description 48
B.1.3. Program Phase....48

B.1.4. Technique *48*

C APPENDIX C - HAZARD REPORT FORMAT 53

D APPENDIX D, XXX 61

LIST OF FIGURES

FIGURE 5. 1 – REVIEW CYCLE
ERROR! BOOKMARK NOT DEFINED.

FIGURE 6.3-1: CONSTELLATION HAZARD MATRIX
ERROR! BOOKMARK NOT DEFINED.

FIGURE 6.3-2: HAZARD LIKELIHOOD AND SEVERITY
ERROR! BOOKMARK NOT DEFINED.

FIGURE A - 1, PHA ANALYSIS FLOW 32

FIGURE A - 2, PRELIMINARY HAZARD LIST WORKSHEET FOR SRR 33

FIGURE A - 3, PRELIMINARY HAZARD LIST WORKSHEET FOR PDR 34

FIGURE A - 4, LIST OF STANDARD HAZARDS 38

FIGURE A - 5, OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA) INSTRUCTIONS 44

FIGURE B-1, FAULT TREE SYMBOLS 50

FIGURE B-2, LOGIC SYMBOLS LEGEND 51

FIGURE B-3, SAMPLE SYSTEM FAULT TREE 52

FIGURE C-1: CONSTELLATION HAZARD REPORT FORM (PAGE 1 OF 4) 53

FIGURE C-1: CONSTELLATION HAZARD REPORT FORM (PAGE 2 OF 4) 54

FIGURE C-1: CONSTELLATION HAZARD REPORT FORM (PAGE 3 OF 4) 55

FIGURE C-1: CONSTELLATION HAZARD REPORT FORM (PAGE 4 OF 4) 56

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to set forth the methodologies and processes required for the Constellation Program and the Constellation Project Elements in implementing a healthy and robust hazard analysis, hazard communication, and hazard approval process.
This document provides a concise methodology and guidance for conducting the various safety analyses for the Constellation Program/Projects. The safety requirements established for the Constellation Program/Projects dictate that aggressive and accurate safety analytical practices be developed and implemented to identify and document all hazards.

Note: This document uses the generic term Safety Review Panel. The official name and responsibilities of that panel will be defined in the CxP charter for the panel.

1.2 Scope

Constellation Program/Projects and contractors will be responsible to identify Hazards created or controlled by their element for each Program/Project lifecycle phase. The Hazards will be identified using the methodology defined in this document, recorded in Hazard Reports and maintained for the life of the Program. Hazard analyses will address design and operational hazards associated with flight and ground hardware, software, operations, and environments. This document provides the hazard analysis methodology; hazard documentation formats and data elements; and data submittal, review and approval process.

2.0 APPLICABLE DOCUMENTS AND REFERENCE DOCUMENTS

2.1 Applicable Documents

CxP 70059 Safety, Reliability, and Quality Assurance Requirements
NASA-STD 8719.13B Software Safety

2.2 Reference Documents

Number	Title
NPR 8705.2	Human-Rating Requirements and Guidelines for Space Flight Systems
CxP 70043	Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL) Methodology

3.0 DEFINITIONS AND ACRONYMS

3.1 Definitions

Abort -- Termination of the nominal mission that allows the crew and passengers to be returned to Earth in the portion of the space system used for nominal entry and touchdown.

Acceptance Rationale -- Logic presented to accept the risk associated with an identified hazard.

Accident -- An unplanned event that results in an unsafe situation or operational mode.

Catastrophic Hazard -- Death or permanently disabling/life-threatening injury, facility destruction on the ground, or loss of crew, major system, or vehicle.

Cause -- Root or symptomatic reason for the occurrence of a hazardous condition.

Component -- A combination of parts, devices, and structures, usually self-contained, which perform a distinctive function in the operation of the overall equipment. A "black box" (which might include, for example, a transmitter, encoder, cryogenic pump, and star tracker).

Contractor Furnished Equipment (CFE) -- Equipment provided to a NASA Center by its' prime contractor.

Contributing Factor (s) -- Factors other than the primary causal factor that must be involved in order for the stated consequence to occur.

Control – Attribute of the design or operational constraints of the hardware/function under analysis which prevent a hazard or reduce the residual risk to an acceptable level. Design controls include those attributes of the robustness of the design as well as inspections and tests to assure the as-built hardware meets the design-to requirements. Operational controls include both operational constraints as well as crew and support personnel training to prevent a hazard or to mitigate its effects once it has occurred.

Critical Hazard -- Severe/lost-time injury or incapacitation, or major loss/damage to facility, system, equipment, or flight hardware which could cause mission abort.

Design for Minimum Risk -- Areas where hazards are not controlled using failure tolerance, but instead are controlled by specified margins of safety, factors of safety, material properties, or any other properties inherent to the design of the part, component, subassembly, or assembly. Examples include structures, pressure vessels, pressurized lines and fittings, pyrotechnic devices, mechanisms in critical applications, material compatibility, and flammability. These areas are

certified safe based upon their inherent properties to withstand their required usage as verified by analysis, qualification, and acceptance testing. Designing for minimum risk is done where failure tolerance is not technically feasible or when adding redundancy actually reduces the overall reliability. Areas proposed for "Design for Minimum Risk", as well as the associated standards for design, manufacturing, and test, must be approved by Constellation and the Technical Authority.

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

Design Reference Mission --A planning mission or a reference mission is a tool used to compare and evaluate approaches to mission and system concepts. The DRM identifies and clarifies system drivers, or significant sources of cost, performance, risk, and schedule variation but does not represent a final or recommended approach to any of these missions.

Element -- Physical entities that have functional capabilities allocated to them necessary to satisfy system-level mission objectives within the Constellation Architecture. Elements can perform all system functions within a mission phase, or through mated operations with other Constellation elements (e.g. Crew Exploration Vehicle (CEV), Earth Departure Stage and Lunar Surface Access Module.)

Element Cause – A cause in an integrated system hazard analysis/report that requires controls within the responsibility of a single element.

Element Hazard Analysis -- A Hazard Analysis provided by an Element as defined above.

Emergency Systems -- Removal of crew and passengers from the portion of the space system normally used for reentry, due to rapidly deteriorating and hazardous conditions, thus placing them in a safe situation suitable for survivable return or recovery. Escape includes, but is not limited to, those modes that utilize a portion of the original space system for the removal (e.g., pods, modules, or fore bodies).

Failure – Inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions, for a specified duration.

Fault Tree Analysis (FTA) -- A deductive logic tool that schematically depicts events, or possible combinations of events that may lead to an undesired top event.

Failure History -- A record of related component or system failures or anomalous events that have occurred in the past and are associated with a given hazard cause.

Flight Hardware -- Hardware designed and fabricated for ultimate use in a vehicle intended to fly.

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 -- Non-flight systems, equipment, or devices necessary to support such operations as transporting, receiving, handling, assembly, inspection, test, checkout, servicing, launch, and recovery of space systems, including spacecraft, launch vehicles, and payloads at launch, landing, or retrieval sites.

Hazard -- The presence of an existing or potential risk caused by an unsafe act, situation or condition that can result in or contribute to a mishap.

Hazard Analysis (HA) -- The determination of sources of potentially dangerous events, and mitigation methods prior to the occurrence of a mishap or event for those conditions found in hardware, software systems, the person–machine relationship, or both, that cause loss of personnel capability, loss of system, or loss of life or injury to the public.

Hazard Report (HR) -- The document recording a Hazard Analysis for a specific event or mishap, which states the hazard title, description, acceptance rationale, cause(s), control(s), verification(s), and status.

Hazard Report Closure Classification -- One of three classifications which define the basis for closure and acceptance of Hazard Reports.

Classification	Definition
Eliminated Hazard	A hazard that has been eliminated by removing the hazard causal factors.
Controlled Risk Hazard	A hazard for which the likelihood and/or severity level have been reduced by implementing the appropriate hazard reduction precedence sequence (as specified in section 4.1).
Accepted Risk Hazard	A hazard for which the strength of the controls has significant limitations or uncertainties, or which has not been adequately controlled through the application of the hazard reduction precedence sequence (as specified in section 4.1), 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 that 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 -- Constellation Hazard Reports status should be either closed or open.

Status	Definition
Closed	Action(s) to eliminate or control the hazard have been implemented or scheduled for implementation. Program management accepts the risk pending completion of corrective action and verification. Baselining by the Program is required to approve a HR as closed.
Open	Actions(s) to eliminate or control the hazard have not been completed and are not scheduled to be performed.

Initiating Event -- An event could initiate an accident or mishap.

Integrated Hazard -- An integrated hazard is an event which could impact another element or an event that is caused by or controlled by multiple systems, segments or elements. Systems that cross projects or elements are considered integrated systems and they are addressed by an integrated hazard analysis.

Likelihood -- Likelihood is the probability that an identified hazard will result in a mishap.

Description	Hazard Likelihood Definitions
Very Low	Extremely remote possibility that it will happen in the life of the program, strength of the controls reduce the safety risk to negligible level.
Low	Unlikely but possible to occur in the life of the program, strong controls in place.
Moderate	Could occur sometime in the life of the program, controls have minor limitations and/or uncertainties.
High	Likely to occur sometime in the life of the program, controls have significant limitations and/or uncertainties.
Very High	Expected to happen in the life of the program, any controls in place have severe limitations and/or uncertainties.

Loss of Crew (LOC) -- An event that results in loss of life during pre-mission, mission, and post-mission activities.

Loss of Mission (LOM) -- Loss of or inability to complete significant/primary mission objectives.

Loss of Vehicle (LOV) – Loss of the capability to provide the level of system performance required for normal or emergency operations.

Mishap -- An unplanned event that results in injury to non-NASA personnel or occupational injury or illness to NASA personnel or damage to public or private property caused by NASA operations.

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, salt spray, sand, dust, clouds, and fungus, etc.

Operating and Support Hazard Analysis (O&SHA) – An analysis that identifies hazards and recommends risk reduction alternatives in procedurally controlled activities during all phases of intended use.

Preliminary Hazard Analysis (PHA) -- An analysis that identifies safety–critical areas, identifies and evaluates hazards, and identifies the safety design and operation requirements needed in the Project concept phase.

Residual Risk -- A portion of the risk that remains after all mitigation has been applied (hazard reduction precedence sequence) and is above that risk level that has already been identified to and accepted by Program Management. Also described as hazard reports that are accepted risk and hazards above the risk baseline.

Risk -- The combination of 1) the probability (qualitative or quantitative) that a Project or Project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, compromise of security, or failure to achieve a needed technological breakthrough; and 2) the consequences, impact or severity of the undesired event were it to occur.

Risk Baseline -- That portion of risk that has been accepted and baselined by Program Management through establishment of the technical baseline (performance requirements, design and construction standards) or through acceptance and baseline of risk reports describing controls and verifications.

Safety -- The minimization of risk from damage or harm to hardware, software, facilities, or humans.

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

Safety Critical -- An event, system, subsystem or process that, if lost or degraded, would result in a critical or catastrophic hazard.

Severity Levels -- Assessment of the most severe effect(s) of a hazard.

Description	Hazard Severity Definitions
Negligible	No injury, illness or crew discomfort; minor damage to secondary or non-essential flight or ground equipment.
Minor	The need for minor first aid treatment (though would not adversely affect personal safety or health. Minor loss/damage to facility, system, equipment, or flight hardware greater than normal wear and tear.
Marginal	Medical treatment for a minor injury or minor loss/damage to facility, system, equipment, or flight hardware.
Critical	Severe/lost time injury or incapacitation, or major loss/damage to facility, system, equipment, or flight hardware.
Catastrophic	Death or permanently disabling/life-threatening injury, facility destruction on the ground, or loss of crew, major system, or vehicle.

Single Failure Point (SFP) -- The failure of an item which would result in critical or catastrophic hazard because the item is not compensated for by redundancy or an alternative operational procedure.

Sneak Analysis – 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.

Standard 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/implosion, vibration/shock/acoustic effects, thermal effects, contamination, radiation, electrical discharge, biological/physiological/psychological impact, toxicity and other general items.

Subsystem Hazard Analysis (SSHA) -- The SSHA identifies 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 -- The aggregate of the ground segment, flight segments, and workforce required to accomplish the Constellation mission.

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) -- The SHA is identical to the SSHA but at the system level. Once the subsystem levels have been established, a combination of subsystems comprises a system. In turn, a group of systems may comprise another system until the top system is identified.

System Safety -- Application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

Verification – Method used to confirm identified controls are in place. Methods may include analyses, tests, inspections, and operations and maintenance requirements.

3.2 Acronyms and Abbreviations

CCB	Change Control Board
CDR	Critical Design Review
CEV	Crew Exploration Vehicle
CFE	Contractor Furnished Equipment
CIL	Critical Items List
COTS	Commercial Off The Shelf
CSFP	Critical Single Point Failure
DCR	Design Certification Review
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
HA	Hazard Analysis
HR	Hazard Report
IHA	Integrated Hazard Report
ITA	Independent Technical Authority
MSA	Mission Safety Assessment
NASA	National Aeronautics and Space Administration
NPR	NASA Procedures and Guidelines
O&SHA	Operating and Support Hazard Analysis
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PRA	Probabilistic Risk Assessment
R&M	Reliability and Maintainability
SAR	Systems Assessment Review
SDP	Safety Data Package
SFP	Single Failure Point

SHA	System Hazard Analysis
SRP	Safety Review Panel
SRR	System Requirements Review
SSHA	Subsystem Hazard Analysis
SSWG	System Safety Working Group
SWHA	Software Hazard Analysis
TSE	Test Support Equipment
USAF	United States Air Force

4.0 HAZARD ANALYSES REQUIREMENTS

It is the objective of the Constellation Program/Projects to maintain insight into all safety hazards and issues that are posed by the design, development, manufacturing, construction, facilities and operations. *The Safety, Reliability, and Quality Assurance Requirements* Document, CxP 70059, requires that the Constellation Program/Projects office and element project offices perform or ensure that the contractor performs the required Hazard Analyses (HA) to identify hazards and ensure their appropriate disposition, tracking and resolution. CxP 70059 requires that the Constellation Program/Projects maintain a closed loop system to assure that all hazards identified in the Hazard Analyses are resolved. To that end this document establishes core methodologies for performing Hazard Analyses and the requirements for documenting those analyses for all Project phases and aspects.

Hazard Analyses will address the hazards that arise in the design, development, manufacturing, construction, facilities, transportation, operations and disposal associated with hardware, software, operations and environments. The analyses will also address hazards caused by the Program/Project/Element/etc. that impact others (ISS, public, International Partners, etc.). The Program will perform an integrated hazard analysis and each Project/Element will perform a hazard analyses on their respective system or subsystem. The Constellation Program/Projects will use the Hazard Reduction Precedence and guidelines described in this document in determining risk associated with identified hazards.

4.1 Hazard Reduction Order of Precedence

The actions to eliminate or control hazards will be in accordance with the hazard reduction precedence sequence as follows: *Note 1: Some hazards may require the combination of several of these approaches to mitigation.*

4.1.1 Design for minimum hazards

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

4.1.2 Incorporate Safety Devices

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

4.1.3 Provide caution and warning devices

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

4.1.4 Develop and implement 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 will be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations will be standardized.

4.2 Minimizing Hazards

4.2.1 Fault Tolerance

Primarily, hazards should be controlled by designing a robust and reliable system that is fault tolerant. This may include like and unlike redundancy, error checking, inhibits, and other methods incorporated into the design. The level of fault tolerance specified is commensurate with the severity of the hazard. Constellation Architecture systems will be two fault tolerant to catastrophic hazards and single fault tolerant to critical hazards. The Project Manager will provide evidence and rationale that one or more of the following are met when requesting proposing to control hazards through means that do not meet the fault tolerance requirement:

a. Fault tolerance is technically not feasible.
b. Redundancy does not reduce the critical system contribution to cumulative risk or the contribution of common cause failures to that critical system's failure.
c. The system or subsystem, such as but not limited to, structures, pressure vessels, and thermal protection systems, will be designed and certified in accordance with approved standards.

4.2.2 Design for Minimum Risk

Design for minimum risk (DFMR) is a proven approach to controlling hazards where fault tolerance is not technically feasible or when adding redundancy actually reduces overall reliability. The Safety Review Panel will approve areas proposing to use DFMR to control hazards in lieu of fault tolerance.

5.0 HAZARD ANALYSES DEVELOPMENT EVOLUTION

5.1 Phase Descriptions

The safety analysis and review process is a phased process and is described herein. The safety analysis will begin at the Program/Project Concept Development phase and will continue throughout the life of the Program. Data/Analysis packages are required for each Program/Project milestone review. The milestone review data package will be utilized by the Safety Review Panel (SRP) to review the hazard analysis and hazard reports prior to the milestone review. A completed review with the SRP is an entry gate for the Preliminary Design Review, Critical Design Review, and System Acceptance Review milestones. Issues and actions identified during the panel review will be briefed at the milestone review. Other SR&QA disciplines, Reliability & Maintainability (R&M) and Probabilistic Risk Assessment (PRA) will have a review with their respective panels prior to the SRP review. Figure 5.1 shows the timeline for the data drop and review cycle.

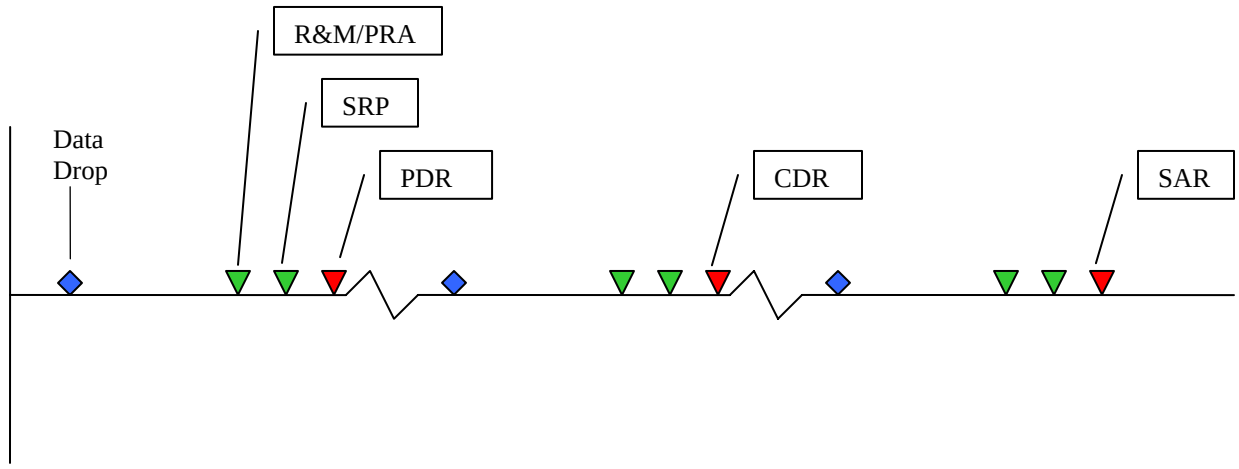

Figure 5. 1 – Review Cycle

5.1.1 Concept Development (Phase A)

The safety analysis process is initiated during the Concept Development phase. The focus of the safety analysis is to identify all potential hazards and hazard causes inherent in the design reference missions (DRM) and concept of operations and determine the necessary safety requirements for eliminating, reducing, or controlling the risk. A Preliminary Hazard Analysis (PHA) is performed during this phase. The process for the PHA and format for the resulting Preliminary Hazard List (PHL) is in Appendix A. Results of the analysis are used to assure that

proper safety requirements are implemented in the Program and Project requirements documents. The document required to capture this analyses is the Preliminary Safety Analysis Report and will include the resulting PHL (see Figure A-2). This report will be included in the System Requirements Review (SRR) data package.

5.1.2 Preliminary Design (Phase B)

The safety analysis process is continued and the safety review process is initiated during the Preliminary Design phase. The preliminary hazard analysis is updated during this phase. The process for the PHA and format for the resulting Preliminary Hazard List (PHL) is in Appendix A. The document required to capture this analyses is the Safety Analysis Report and will include the resulting PHL (see Figure A-3). A Safety Analysis Report is prepared and included in the Preliminary Design Review (PDR) data package. The Phase I Safety Review is the first required Program safety review in which the safety of the system/end-item and associated operations are assessed. The Phase I Safety Review will be conducted prior to the PDR. The focus of the safety review is to identify all potential hazards and hazard causes inherent in the preliminary design, to evaluate the means of eliminating, reducing, or controlling the risk, and to establish the preliminary methods for verification of those controls. After approval, the results of the Phase I Safety Review, including issues and actions, are presented at PDR.

5.1.3 Final Design (Phase C)

The safety analysis and review process is continued during the final design phase. A detailed hazard analysis is performed and completed during this phase. The document required to capture this analyses is the Safety Analysis Report and will include Hazard Reports (see figure C-1). The Safety Analysis Report is prepared and included in the Critical Design Review (CDR) data package. The Phase II Safety Review will be conducted prior to the CDR. The focus of the safety review is to evaluate the updated analysis that reflects the detailed design and operations of the system/end item to assure that all appropriate hazard controls have been defined and implemented in design documentation and that specific methods of verifying each control have been identified in verification plans and procedures. After approval, the results of the Phase II Safety Review, including issues and actions, are presented at CDR.

5.1.4 Fabrication, Assembly and Test (Phase D)

The design safety analysis and review process are completed during the Fabrication, Assembly and Test phase. The Safety Analysis Report, including the Hazard Reports (see figure C-1), is prepared and included in the System Acceptance Review (SAR) data package. The Phase III Safety Review will be conducted prior to the SAR. The focus of the safety review is to:

- Evaluate the effectiveness of the hazard controls,
- Evaluate the results of the verification activity
- Evaluate the results of any failure analysis, and

- Assure that specific methods of verifying each control in flight fabrication, assembly and test process are identified in verification plans and procedures.

After approval, the results of the Phase III Safety Review including open issues and actions are presented at System Acceptance Review.

5.1.5 Operational and Sustaining Engineering Phase (Phase E)

Safety analyses and reviews continue during the Operational and Sustaining Engineering phase to assure Hazard Reports and the associated data elements are maintained and current information is available for real time and near real time risk assessments. The focus in this phase is to:

- Identify new operational risks and creep in risk acceptance rationale
- Ensure operational controls are properly implemented
- Identify and avoid unacceptable risk associated with changes in flight rules, ground checkouts, and/or operational procedures
- Assure safety analysis (Phases A through E) is applied to proposed design changes and modification kits to preclude those changed from adversely affecting risk
- Minimize risk through appropriate design and operation changes
- Identify and analyze adverse trends to assure Program risk does not creep as a result of failures experienced

5.2 Integrated Hazards

During the hazard analysis process, the Project Elements and the Program will identify integrated hazards. An integrated hazard is an event which could impact another element or an event that is caused by or controlled by multiple systems, segments or elements. Systems that cross projects or elements are considered integrated systems and they are addressed by an integrated hazard analysis. When these are identified by the projects, they will create preliminary hazard reports that describe the hazard and forward this information to the Safety Review Panel Coordination Office for further assignment to analyze and control the hazard. When the Program, through the integrated hazard analysis process, identifies hazards that should be included in the Projects hazard analysis, the program will forward, through the Safety Review Panel Coordination Office, to the Projects for further assignment to analyze and control the hazard. The Safety Review Panel Coordination Office will account for the transmittal of this information and assure the appropriate actions have been completed during the review of Project or Program hazard analyses.

6.0 HAZARD REPORTS

6.1 Purpose

Hazard Reports (HRs) are the means of documenting hazards identified in the hazard analyses to allow management acceptance of hazard control and verification.

6.2 HA Review Process

The Constellation Program/Projects are responsible for assuring that all hazards associated with the design, development, manufacturing/construction, testing, transporting and operations are addressed adequately. The Constellation Safety Review Panel reviews and approves all hazards associated with the Constellation Program/Projects.

6.3 Standardized Data Elements

The development of HRs involves the conveyance of basic information about the risk associated with the hazard, how the hazard is controlled, and the verification method for the control in place.

The Hazard Report form with detailed instructions for the Constellation Program/Projects is included in Appendix C. A determination of Hazard Severity and the Likelihood of the hazardous event occurring is included in the Hazard Report (reference Figures 6.3-1 and 6.3-2).

6.4 Maintaining Hazard Reports

The Program/Projects prepare Hazard Reports to document the results of the formal hazard analysis process, and establish management acceptance of the hazard controls and verifications. Once approved during the phase III review, the hazard controls and verifications cannot be changed without review and approval by the Safety Panel. Changes in the design, operations, hazard controls or verifications must be maintained current with the program baseline. Hazard Reports will be reviewed annually by the Program/Projects to assure that the information is current and accurate. All data contained in Hazard Reports will be included in the TBD database.

Anomalies and PRACA reports will be presented and concurred with by the Safety Panel prior to closure to assure hazard acceptance rationale is still acceptable. Also, negative failure history trends in flight hardware or in flight-like hardware will be reviewed by the Safety Panel to ascertain if anomalies and system failures indicate hazard control effectiveness is in question and merit reassessment of the hazard closure classification and/or risk assessment as identified on the Risk Matrix.

Constellation HAZARD MATRIX

SEVERITY

LIKELIHOOD

	Category 1: NEGLIGIBLE	Category 2: MINOR	Category 3: MARGINAL	Category 4: CRITICAL	Category 5: CATASTROPHIC
5 VERY HIGH	Controlled	Controlled	Accepted Risk	Accepted Risk	Unacceptable
4 HIGH	Controlled	Controlled	Accepted Risk	Accepted Risk	Accepted Risk
3 MODERATE	Controlled	Controlled	Controlled	Accepted Risk	Accepted Risk
2 LOW	Controlled	Controlled	Controlled	Controlled	Accepted Risk
1 VERY LOW	Controlled	Controlled	Controlled	Controlled	Controlled

Figure 6.3-1: Constellation Hazard Matrix

Description	Level	Hazard Likelihood Definitions
Very Low	1	Extremely remote possibility that it will happen in the life of the program, strength of the controls reduce the safety risk to negligible level.
Low	2	Unlikely but possible to occur in the life of the program, strong controls in place.
Moderate	3	Could occur sometime in the life of the program, controls have minor limitations and/or uncertainties.
High	4	Likely to occur sometime in the life of the program, controls have significant limitations and/or uncertainties.
Very High	5	Expected to happen in the life of the program, any controls in place have severe limitations and/or uncertainties.

Description	Level	Hazard Severity Definitions
Negligible	1	No injury, illness or crew discomfort; minor damage to secondary or non-essential flight or ground equipment.
Minor	2	The need for minor first aid treatment (though would not adversely affect personal safety or health). Minor loss/damage to facility, system, equipment, or flight hardware greater than normal wear and tear.
Marginal	3	Medical treatment for a minor injury or minor loss/damage to facility, system, equipment, or flight hardware.
Critical	4	Severe/lost time injury or incapacitation, or major loss/damage to facility, system, equipment, or flight hardware.
Catastrophic	5	Death or permanently disabling/life-threatening injury, facility destruction on the ground, or loss of crew, major system, or vehicle.

Figure 6.3-2: Hazard Likelihood and Severity

7.0 SAFETY ANALYSIS REPORT

The Safety Analysis Report contains the relevant information on the system being analyzed, descriptions and background data necessary to understand the system and analysis, reference to milestone review data necessary to understand the analyzed system, the ground rules for the analysis, hazards evaluated and excluded from further detail in hazard reports, and the hazard reports.

8.0 MISSION SAFETY ASSESSMENT

8.1 Purpose

Mission Safety Assessments (MSAs) should provide evaluations for each specific mission to ensure that the public, flight and ground crews, facilities, environment and assets are adequately protected from hazards. These evaluations review the risks of each anticipated event and determine the best course of action to ensure the consequences are acceptable by preventing a condition or event from occurring, mitigating the event or situation, and/or containing the hazard to preclude further dispersion. Mission Safety Assessments should evaluate each mission (including payloads) to determine if additional hazards (in addition to those documented in the Hazard Analysis and reviewed and approved at the Constellation Safety Review Panel) are present.

Each MSA should also review any changes in hardware, operations, or mission profile against accepted HRs to ensure that there are no safety impacts. The scope of the MSA encompasses all on-board equipment, Constellation On-Orbit replaceable units, and medical equipment to achieve the defined missions; any cargo exceeding the basic Constellation mission requirements is beyond the scope of the MSA. Any excluded cargo carried by the Constellation System must be evaluated by the appropriate established board and/or panels prior to flight. The MSA should include an updated summary of all verifications associated with the Start of Mission Processing and the Flight Readiness Review (FRR) that reflects the current integrated system status.

8.2 Content

The MSA is an integrated assessment of the hazards associated with a specific mission. The content of the MSA report should include the following:

a) Description of the Mission complement and objectives. This will include a reference to the specific vehicles involved.

b) Listing of all applicable hazards for this mission.

c) Summary of the integrated hazard analysis for the mission

d) Listing of all new or uniquely performed verifications associated with baseline HR that will be opened and specifically re-verified for this mission. Any verifications or hardware that is approaching a limited life should be detailed.

e) A listing of all related anomalies that have occurred since the Constellation Design Certification Review (DCR), during the previous missions, or during the preparation of the system for the current. The MSA should contain closure information and rationale for

closing anomalies experienced during the preparation for the current mission. Documentation, including reference material should require CCB approval of anomaly closure.

f) Any new and unique hazards associated with this Mission.

8.3 Timing

The initial MSA should be prepared and submitted to the Constellation Safety Review Panel starting with the equivalent of the DCR. Later MSAs should be initiated by approval of flight schedules and the commencement of mission planning activities for the subject Constellation mission and continue to final approval at the Flight Readiness Review.

A APPENDIX A - HAZARD ANALYSIS TYPES AND TECHNIQUES

A.1. Preliminary Hazards Analysis (PHA)

A.1.1. Purpose

The PHA is begun early in the concept phase of the Program/Project to identify potentially hazardous conditions of the conceptual design. The PHA provides the Program/Projects with knowledge of the potential hazard causes and candidate controls.

A.1.2. Description

The PHA documents an initial risk assessment of a concept or system. It is based on the best available data, starting with the Functional Flow Block Diagram (FFBD), including mishap data from similar systems, and lessons learned from other projects. It identifies and evaluates the hazards associated with the proposed design or functions for potential hazard severity, probability, time of exposure, and hazard classification. Design controls, software controls, operational controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level should be considered and documented. Output of the PHA is used in (1) further developing system safety requirements, (2) preparing performance/design specifications, and (3) initiating the hazard tracking and risk resolution process.

The PHA provides consideration of the following, as a minimum, for identification and evaluation of hazards:

a. As complete a description as possible of the system or systems and how it will be used.

b. Hazard sources inherent to the design (e.g., propellants, lasers, explosives, toxic substances, corrosives, hazardous construction materials, pressure systems, and other energy sources).

c. 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).

d. Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, humidity, corrosive environments, hurricane winds, seismic activity, noise, exposure to toxic substances, confined spaces, fire, electrostatic

discharge, lightning, electromagnetic environmental effects, and ionizing and non-ionizing radiation).

e. 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).

f. Facilities, support equipment (e.g., provisions for storage, disposal, assembly, checkout, proof-testing of hazardous systems and 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).

g. 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).

h. A review of historical safety experience (lessons learned on similar systems)

A.1.3. Project Phase

The Project should begin its PHA effort during the concept development phase through the preliminary design phase so that it can use safety considerations to evaluate design alternatives and trade studies. The PHA should be used as the baseline for performing future analyses, such as the SSHA, SHA, IHA and O&SHA. To ensure that safety considerations are fully examined and included in the concept definition of the system, an initial PHA report is required as part of the System Requirements Review (SRR) and updated for the Preliminary Design Review. The PHA should include an initial analysis of all identified major systems, sub-systems, flight phases and high risk ground support activities at a minimum.

A.1.4. Technique

The PHA information should be recorded in the form and content of the columnar matrix shown in Figure A-2 for SRR and Figure A-3 for PDR. The Preliminary Hazard List (PHL) format provides a systematic and consistent method for documenting the analysis, has wide applicability, and provides evidence of the analytical procedure. Other aids, such as top-level fault trees, Sneak Analysis (SAs), SHAs, FMEA/CILs, and safety checklists, may be used to identify hazardous conditions and causes. The following steps are provided as a guide to assist the analyst and ensure the performance of a comprehensive PHA.

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 descriptions, design reference mission descriptions, functional flow block diagrams, design drawings, operational concepts/plans, related failure and flight anomaly reports, and other available technical data. To populate the PHL the analyst will first assess the Functional Flow Block Diagram (FFDB). The analyst will then identify the appropriate FFBD block to begin a Fault Tree Analysis (see appendix B). The fault tree will be developed far enough down to identify hazardous conditions and causes that may be controlled or eliminated by design. Figure A-1 shows the analysis flow.

b. *Hazard Analysis*. Having accumulated the necessary information, the safety analyst can make entries in the columnar matrix HA worksheet. The format provides space to describe hazardous conditions, hazard causes, hazard effect, severity level, safety requirements, hazard elimination and control provisions, verifications (for PDR), and likelihood of occurrence (for PDR). HA worksheet instructions are provided in Figure A-2 for SRR and Figure A-3 for PDR. Checklists are also provided in Figure A-4, which will be helpful as a guide throughout the analysis. Using the Hazard Matrix (see Figure 6.3-1), assign the highest credible likelihood associated with the residual risk of this hazard after mitigations are completed. The HA should include justification, based on the worst credible severity, for the assessment of risks. Supporting data, either quantitative or qualitative should be attached to support both severity and likelihood. The safety requirements may be identified by using the mapping table from the FFBD to the applicable requirement document (CARD, SRD, etc). If requirements are not in the appropriate document, the analyst will record what requirement needs to be added and report to the Program/Project.

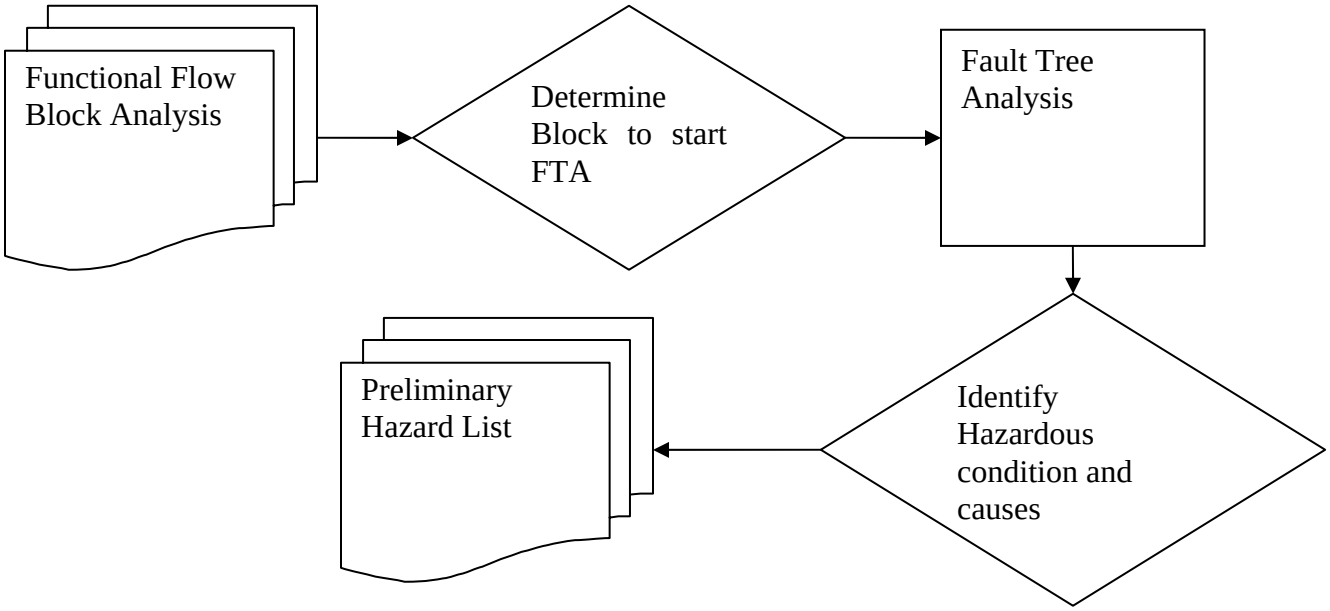

Figure A - 1, PHA Analysis Flow

CxP Preliminary Hazard List for SRR

Hazard Analysis Title:	Revision:	DRM:
Worksheet No:		Engineer:
FFBD Version:	FFBD Block No:	Date:
Project/Element/Subsystem:		Sheet: **33 of 61**

Hazardous Condition	**Cause(s)**	**Effect and Applicable Project, Element, or Subsystem**	**Initiating/ Affected Element**	**Severity**	**Requirements**	**Hazard Elimination / Control Provisions**	**Failure Tolerance**	**Recommendation**
Use the checklist Below to identify potentially hazardous conditions. 1. Can the system fail to operate as intended? 2. Can the system operate inadvertently (untimely)? 3. Are there standard hazards? (See Figure A-4) Record the identified hazards.	Enter brief Description of how each hazardous condition is created, i.e., rupture of the O2 tank; wiring insulation overheating and igniting; human error 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 Project/ Element/ Subsystem that initiates the event or is affected	Identify the worst case severity level as one of the Following for each hazardous condition: Catastrophic, Critical, or Other. Reference Severity Definitions in Figure 6.3-1.	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 hazards. For Level II – Identify transfer to Level III Project if applicable.	Identify the level of failure tolerance required. How many levels of failure tolerance are currently in place? Does it meet the requirement?	Provide recommendations for additional requirements, trade studies, or other options which may be needed to control or eliminate the hazardous condition.

Figure A - 2, Preliminary Hazard List Worksheet for SRR

CxP Preliminary Hazard List for PDR

Hazard Analysis Title:	Revision:	DRM:
Worksheet No:		Engineer:
FFBD Version:	FFBD Block No:	Date:
Project/Element/Subsystem:		Sheet: **34 of 61**

Hazardous Condition	**Cause(s)**	**Effect and Applicable Project, Element, or Subsystem**	**Initiating / Affected Element**	**Severity / Likelihood of Occurrence**	**Require-ments**	**Hazard Eliminatio n/ Control Provisions**	**Verification**	**Failure Tolerance**	**Recom-mendation**
Use the checklist Below to identify potentially hazardous conditions. 1. Can the system fail to operate as intended? 2. Can the system operate inadvertently (untimely)? 3. Are there standard hazards? (See Figure A-4). Record the identi-fied hazards.	Enter brief Description of how each hazardous condition is created, i.e., rupture of the O2 tank; wiring insulation overheating and igniting; human error 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 Project/ Element/ Subsystem that is affected	Identify the Project/ Element/ Subsystem that initiates the event or is affected	Identify the worst case severity level Assess the controls that are in place and determine the residual risk after the controls are applied. Specify the Likelihood that the hazard cause could occur as a result of the residual risk. Reference Severity and Likelihood Definitions in Section Figure 6.3-2.	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 hazards. For Level II – Identify transfer to Level III Project if applicable.	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 level of failure tolerance required. How many levels of failure tolerance are currently in place? Does it meet the requirement?	Provide recommendation s for additional requirements including those that belong in the verification plan, trade studies, or other options which may be needed to control or eliminate the hazardous condition.

Figure A - 3, Preliminary Hazard List Worksheet for PDR

The Generic Hazards listed are predicated on the following top-level events, or consequences; Loss of Life, Loss of Vehicle, or Loss of Mission.

GENERIC HAZARD	STANDARD CAUSE
I. CONTAMINATION	A. CHEMICAL DISASSOCIATION B. CHEMICAL REPLACEMENT/COMBINATION C. MOISTURE D. OXIDATION E. ORGANIC (FUNGUS/BACTERIAL, GROWTH MEDIA, ETC) F. PARTICULATE G. PLANET/MOON EXPOSED TO EARTH CONTAMINATION H.BIOHAZARDS I. CHEMICAL REACTIONS J. WASTE MANAGEMENT (INCLUDING PACKING MATERIAL, TRASH, RECYCLING, REUSE, BIOLOGICAL, AND SOLID WASTE)
II. CORROSION	A. CHEMICAL DISASSOCIATION B. CHEMICAL REPLACEMENT/COMBINATION C. MOISTURE D. OXIDATION E. ORGANIC (FUNGUS/BACTERIAL, GROWTH MEDIA, ETC) F. PARTICULATE
III. ELECTRICAL DISCHARGE/SHOCK	A. EXTERNAL SHOCK B. INTERNAL SHOCK C. STATIC DISCHARGE D. CORONA E. SHORT
IV. ENVIRONMENTAL/ WEATHER	A. FOG B. FUNGUS/BACTERIAL/VIRAL C. LIGHTNING (IN HABITAT, DARK SIDE OF MOON) D. PRECIPITATION (RAIN/SNOW/SLEET/HAIL) E. METEOROIDS/METEORS F. SOLAR/COSMIC RADIATION G. SAND/DUST H. VACUUM I. WIND J. TEMPERATURE EXTREMES K. TERRAIN CHANGES
V. FIRE/OVERHEAT	A. CHEMICAL CHANGE (EXOTHERMIC/ENDOTHERMIC) B. FUEL AND OXIDIZER IN PRESENCE OF PRESSURE AND IGNITION SOURCE C. PYROLYSIS/CHEMICAL DECOMPOSITION UNDER THE ACTION OF HEAT D. PRESSURE RELEASE E. HIGH HEAT SOURCE
VI. COLLISION	A. ACCELERATION (INCLUDING GRAVITY) B. DETACHED EQUIPMENT C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL D. METEOROIDS E. MOVING/ROTATING EQUIPMENT

GENERIC HAZARD	STANDARD CAUSE
	F. LOSS OF CONTROL DURING PROXIMITY OPERATIONS G. LOSS OF POSITIONAL AWARENESS DURING PROXIMITY OPERATIONS H. ATTITUSE CONTROL FAILURE DURING PROXIMITY OPERATIONS I. RECONTACT FOLLOWING PLANNED SEPARATION J. FAILURE TO DECELERATE OR ACTIVATE LANDING ATTENUATION SYSTEMS K. TRANSPORTATION (MOTORIZED VEHICLES) L. CONSTRUCTION
VII. PATHOLOGICAL/ PHYSIOLOGICAL/ PSYCHOLOGICAL	A. ACCELERATIONS/SHOCK/IMPACT/VIBRATION B. PRESSURE (HIGH, LOW, RAPID CHANGE) C. HUMIDITY D. ILLNESS/ILLNESS E. NOISE F. SHARP EDGES G. SLEEP, LACK OF VISIBILITY (GLARE, WINDOW/HELMET FOGGING, SUSPENDED PARTICULATES) H. HOUSEKEEPING I. TEMPERATURE J. WORKLOAD, EXCESSIVE K. DEHYDRATION L. STARVATION M. LOSS OF CLEANLINESS N. PROLONGED PHYSICAL CONSTRAINT O. LONLINESS/DEPRESSION P. TRIPPING HAZARDS Q. STRESS R. LASER S. UNSTABLE OBJECTS/LOADS T. PINCH POINTS/CRUSHING U. STRESS
VIII. TEMPERATURE EXTREMES	A. OVERHEAT B. INSUFFICIENT/DAMGED INSULATION C. VENTING GASES D. FIRE E. HEAT SHIELD FAILURE
IX. LOSS OF CONTROL	A. ATTITUDE CONTROL B. DIRECTIONAL CONTROL C. LOSS OF COMMAND
X. LOSS OF SAFE RETURN CAPABILITY	A. DEORBIT B. REENTRY C. LANDING AND RECOVERY
XI. IMPLOSION/LOSS OF PRESSURE (HARDWARE)	A. CHEMICAL CHANGE (ENDOTHERMIC) B. PRESSURE RELEASE/LEAK C. TRANSPORTATION (MOTORIZED VEHICLES)

GENERIC HAZARD	STANDARD CAUSE
	D. CONSTRUCTION
XII. EXPLOSION	A. CHEMICAL CHANGE (EXOTHERMIC) B. CHEMICAL MIXING (HYPERGOLICS) C. PYROLYSIS/CHEMICAL DECOMPOSITION UNDER THE ACTION OF HEAT D. CRACKS IN SOLID PROPELLANTS E. BLOCKAGE OF ROCKET NOZZLES F. OVERPRESSURE G. IGNITION OF EXPLOSIVE MATERIALS
XIII. LOSS OF CRITICAL FUNCTION	A. FAILURE TO SEPARATE B. FAILURE TO OPERATE C. UNCOMMANDED OPERATION
XIV. IMPACT FROM DEBIS	A. ACCELERATION (INCLUDING GRAVITY) B. DETACHED EQUIPMENT C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL D. METEOROIDS E. MOVING/ROTATING EQUIPMENT F. LOSS OF CONTROL DURING PROXIMITY OPERATIONS G. ATTITUSE CONTROL FAILURE DURING PROXIMITY OPERATIONS H. RECONTACT FOLLOWING PLANNED SEPARATION I. TRANSPORTATION (MOTORIZED VEHICLES)
XV. IMPACT FROM STRUCTURAL FAILURE	A. ACCELERATION (INCLUDING GRAVITY) C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL E. MOVING/ROTATING EQUIPMENT F. LOSS OF CONTROL DURING PROXIMITY OPERATIONS G. LOSS OF POSITIONAL AWARENESS DURING PROXIMITY OPERATIONS H. ATTITUDE CONTROL FAILURE DURING PROXIMITY OPERATIONS J. FAILURE TO DECELERATE OR ACTIVATE LANDING ATTENUATION SYSTEMS K. TRANSPORTATION (MOTORIZED VEHICLES)
XVI. LOSS OF STRUCTURAL INTEGRITY	A. ACCELERATION (INCLUDING GRAVITY) B. DETACHED EQUIPMENT C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL D. MOVING/ROTATING EQUIPMENT E. LOSS OF CONTROL DURING PROXIMITY OPERATIONS

GENERIC HAZARD	STANDARD CAUSE
	F. ATTITUDE CONTROL FAILURE DURING PROXIMITY OPERATIONS G. FAILURE TO DECELERATE OR ACTIVATE LANDING ATTENUATION SYSTEMS H. RECONTACT FOLLOWING PLANNED SEPARATION I. FAILURE TO DECELERATE OR ACTIVATE LANDING ATTENUATION SYSTEMS J. TRANSPORTATION (MOTORIZED VEHICLES)
XVII. LOSS OF HABITABLE ENVIRONMENT (PPE/PVS (PERSONNEL VACUUM SHELL) AND BREATHABLE AIR)	A. OXYGEN FAILURE B. NITROGEN CONTENT C. LOW PRESSURE D. LOW TEMPERAZTURE E. HIGH TEMPERATURE F. LOW PRESSURE G. HIGH TEMPERATURE H. SUIT/BARRIER LEAKAGE I. FIRE
XVIII. LOSS OF HABITABLE ENVIRONMENT FROM TOXINS	A. BACTERIAL B. ORGANIC C. INORGANIC D. FIRE
XIX. LOSS OF HABITABLE ENVIRONMENT FROM COMTAMINATION	A. BACTERIAL B. ORGANIC C. INORGANIC D. FIRE
XX. IONIZING RADIATION	A. RADIOACTIVE ELEMENT/SOURCE B. INTERNAL C. EXTERNAL
XXI. EMI	A. RF B. CONDUCTED C. NON-CONDUCTED D. MAGNETIC
XXII. LASERS	A. VISIBLE B. INFRARED D. ULTRAVIOLET

This list should not be considered to be all inclusive of possible hazards.

Figure A - 4, List of Standard Hazards

A.2. Subsystem Hazard Analyses (SSHA)

A.2.1. Purpose

The general purpose of the Subsystem Hazard Analysis (SSA) is to perform a safety risk assessment of a system's subsystems at a greater level than that provided in a PHA.

The SSHA verifies subsystem compliance with system/safety requirements, identifies previously unidentified hazards associate with the subsystem, assesses the risk of the subsystem design, considers human factors, functional and component failures, and functional relationships between components in the subsystem including software, and recommends actions to control the hazard. .

A.2.2. Description

The SSHA identifies specific, detailed 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, incompatible materials; and environmental conditions such as dust, radiation, and sand.

The SSHA defines the safety-critical functions, operations, possible component fault conditions, standard hazards, safety-critical operations and environments associated with the subsystem under the column heading "Hazardous Condition Description" (Appendix D, HR Instructions data item #9).

A.2.3. Project Phase

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

A.2.4. Technique

The same data fields are required for the SSHA as are used for the PHA. The following steps are provided as a guide to assist the analyst and ensure the performance of a comprehensive SSHA:

a. Identify the hazardous conditions. Use the list of standard hazards in Figure A-4 as a guide. – There may be peculiar hazardous conditions associated with the subsystem being analyzed that are not listed in the figure.

b. Use a fault tree or similar logic diagram to identify all of the potential causes of the hypothetical hazardous condition. The causes will usually 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. For an integrated hazard, also determine the organizational elements responsible for the causes, and note the responsible organizations along with the cause descriptions in the hazard analysis instructions form.

c. The hazard effect, severity level, safety requirements, hazard elimination and control provisions, verifications, and likelihood of occurrence columns should be completed as described in Figure A-2 and A-3, Preliminary Hazard List (PHL) Instructions.

A.3. System Hazard Analyses (SHA)

A.3.1. Purpose

The general purpose of the SHA is to perform a detailed safety risk assessment of a system; in particular the interfaces of that system with other systems and the interfaces between the subsystems that compose the system itself.

The SHA verifies system compliance with safety requirements, identifies previously unidentified hazards associated with the system interfaces, system functional faults and system operation in the specified environment. The SHA considers human factors, system/functional failures and functional relationships between subsystems comprising the system including software. The SHA identifies existing controls and recommends additional controls.

A.3.2. Description

The SHA is identical to the SSHA, but at the system 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. *Note*: Once the subsystem levels have been established, a combination of subsystems makes 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.

A.3.3. Project Phase

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

A.3.4. Technique

The SHA uses the same technique as previously described in Paragraph A.2.4, technique for the SSHA, except at a higher level. Test information such as failure history or other anomalous conditions encountered during test and development should be a major consideration when judging the effectiveness of hazard controls and assessing risk.

A.4. Operating and Supporting Hazard Analyses (O&SHA)

A.4.1. Purpose

The general purpose of the Operating & Support Hazard Analysis (O&SHA) is to perform a detailed safety risk assessment of a system's operational and support procedures.

The O&SHA identifies hazards and recommends risk reduction alternatives in procedurally controlled activities during all phases of intended system/hardware/facility use.

A.4.2. Description

The O&SHA examines human induced hazards to hardware, software, equipment, facilities, and the environment – it describes what a human can do to create hazards and how the hardware, software, equipment, facilities, and environment can create hazards for humans. Generally, the O&SHA examines those operations that are 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 should 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, should be identified.

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

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

f.) Potentially hazardous conditions that may be induced into flight hardware during manufacturing, test, inspections, ground operations, etc., and then show up later during flight hardware/software end use. These conditions should 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.

A.4.3. Project Phase

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

A.4.4. Technique

An O&SHA format and recommended content are to follow the format in Figure A-5, Operating and Support Hazard Analysis (O&SHA) Instructions. This O&SHA is developed with the intent of establishing a systematic review and documentation where the operations are broken down into incremental parts and consistently analyzed for hazards.

O&SHA NO.			ENGINEER:	
OPERATION:			DATE:	
TASK:				
SUBTASK:				
STEP				
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, batteries.)	SHEET	1 of 1

HAZARDOUS CONDITIONS	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 instructions)	Potential effects of impact on personnel or equipment	Identify the worst case severity level as one of the Following for each hazardous condition: Catastrophic, Critical, Minor, Marginal, or Negligible.	Describe recommended measures for preventing eliminating, or controlling the hazardous condition. Include guidelines recommended design or operational requirements, and recommended further analyses or actions	Identify proposed hazard reduction methods for open hazards and implemented reductions 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 determine the residual risk after the controls are applied. Specify the Likelihood that the hazard cause could occur as a result of the residual risk. State likelihood in one of the following terms: Very Low, Low, Moderate, High, or Very High.

Figure A - 5, Operating and Support Hazard Analysis (O&SHA) Instructions

A.5. Software Hazard Analyses (SWHA)

The SWHA provides a detailed hazard evaluation of the system software and firmware to identify hazards incident to safety critical functions. Software safety analyses will assure that procedural errors and malfunctions of any software or firmware modules will not cause or contribute to a failure condition.

The application of software safety is documented in NASA-STD-8719.13, “Software Safety”. The implementation of software safety and the associated HA is an integral part of the overall system safety and software development efforts. The objective of the software safety effort is to ensure that safety is considered throughout the software life cycle. Therefore software safety activities take place during all phases of hazard analyses and systems development and testing. The result of these analyses should be incorporated at the appropriate HA level.

A.6. Integrated Hazard Analysis (IHA)

Integrated hazard reports (HRs) should document inter-element hazards and ensure that the controls necessary for safe integrated operation are properly addressed and controlled in element HRs. Proper conduct of this analysis should identify hazardous conditions to personnel and the system through all ground and flight phases, due to nominal flight operation of the system from pre-launch through landing and crew recovery.

A.6.1. Purpose

Integrated Hazard Analysis should identify hazard causes and controls that cross system and element boundaries and should identify the organizations responsible for assuring mitigation for the hazard causes.

A.6.2. Description

An integrated hazard is an event which could impact another element or an event that is caused by or controlled by multiple systems, segments or elements. Systems that cross projects or elements are considered integrated systems and they are addressed by an integrated hazard analysis. Integrated Hazard Analysis should document inter-element hazards and ensure that the controls necessary for safe integrated operation are properly addressed and documented in system HRs.

A.6.3. Project Phase

The IHA effort should begin as system Interface Control Documents (ICD) are developed and should be updated as required throughout the Program/Projects life cycle.

A.6.4. Technique

The IHA should address hazards to the integrated system, and should use the Functional Flow Block Diagram, the SHA, and other data for each system or element and the appropriate detailed analysis to identify hazards to the entire system or hazards caused by these interactions Proper conduct of this analysis should identify hazardous conditions to personnel and the system through all ground and flight phases, due to nominal flight operation of the system from pre-launch through landing and crew recovery. The IHA uses all applicable HAs, FMEA/CILs, FTA, operational concepts and planning as prime inputs.

B APPENDIX B – FAULT TREE ANALYSIS

B.1. Fault Tree Analysis Process

B.1.1. 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.

B.1.2. 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.
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.

B.1.3. 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.

B.1.4. Technique

Only the basic FTA symbols (Figures B-1 and B-2) 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 B-2 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 B-3, 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.

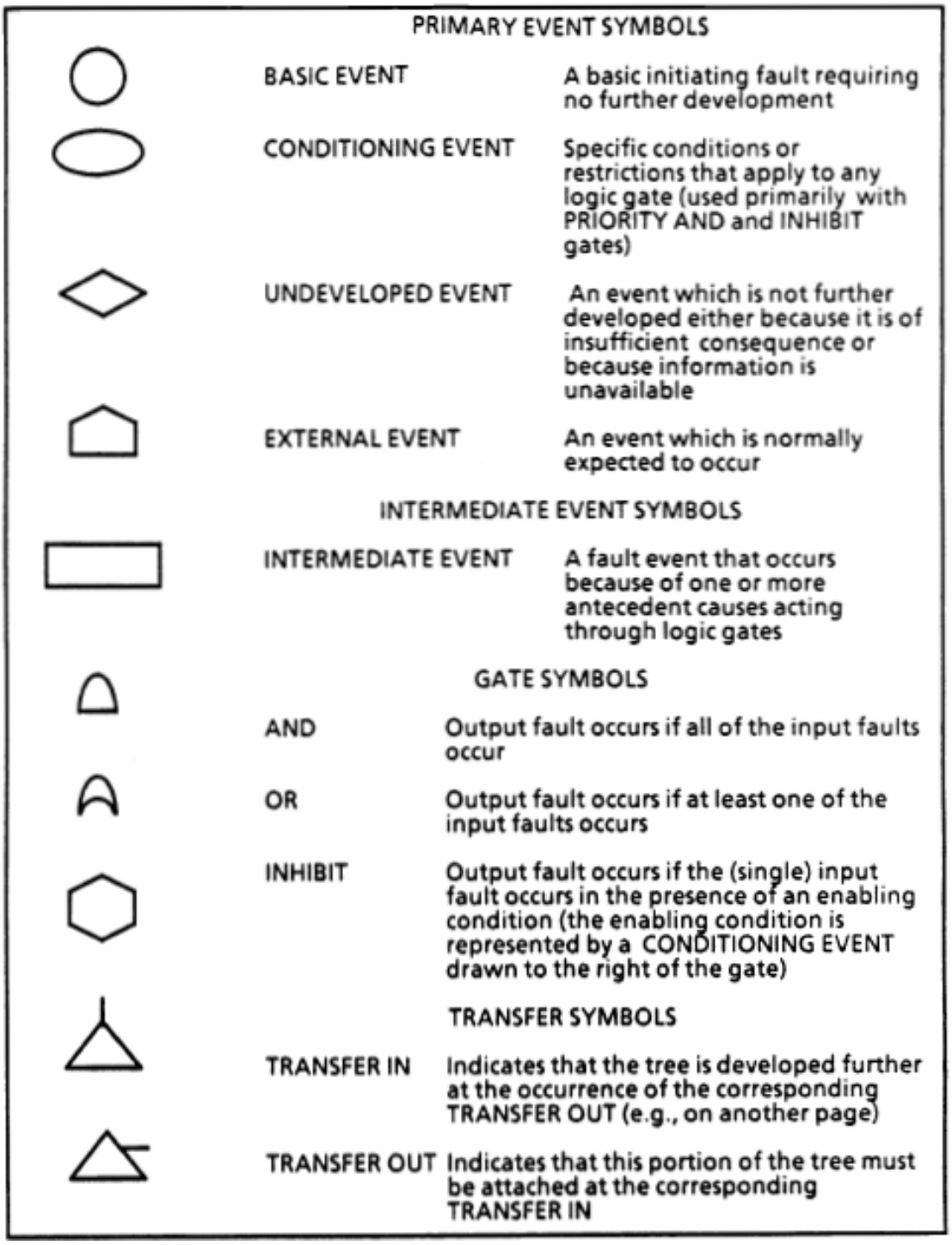

Figure B-1, Fault Tree Symbols

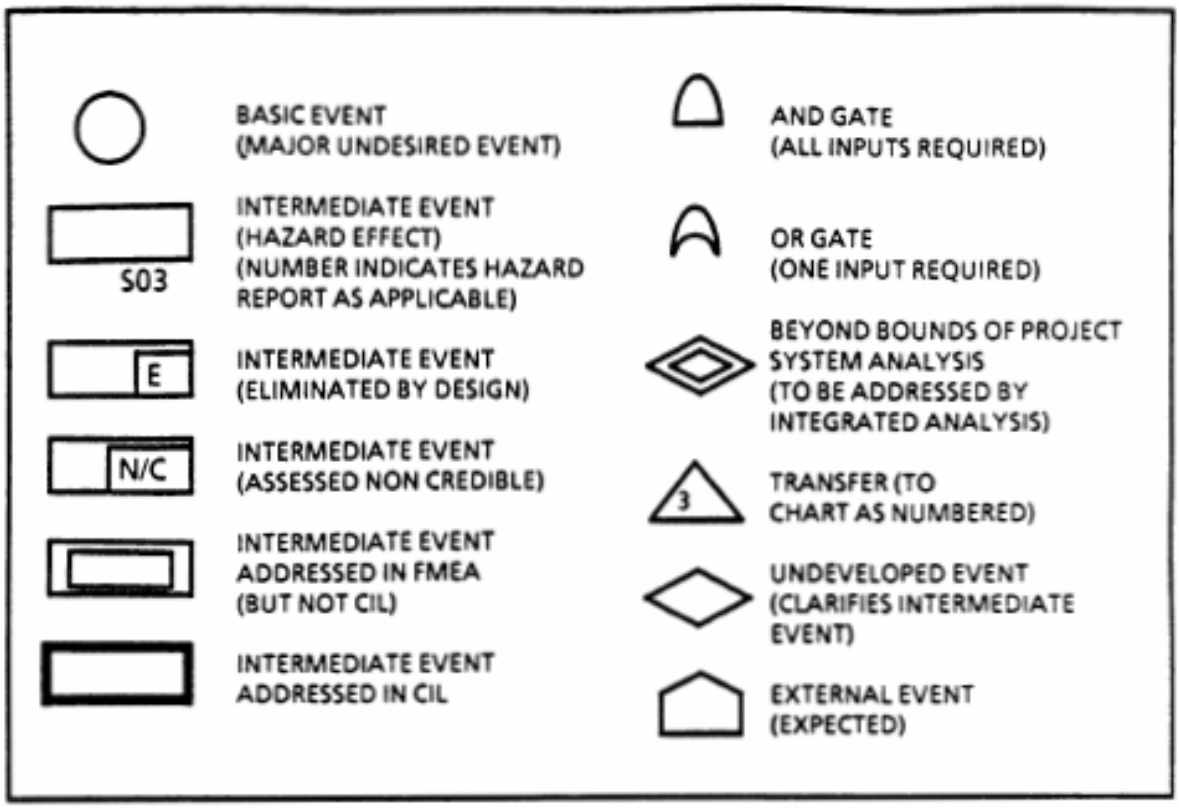

Figure B-2, Logic Symbols Legend

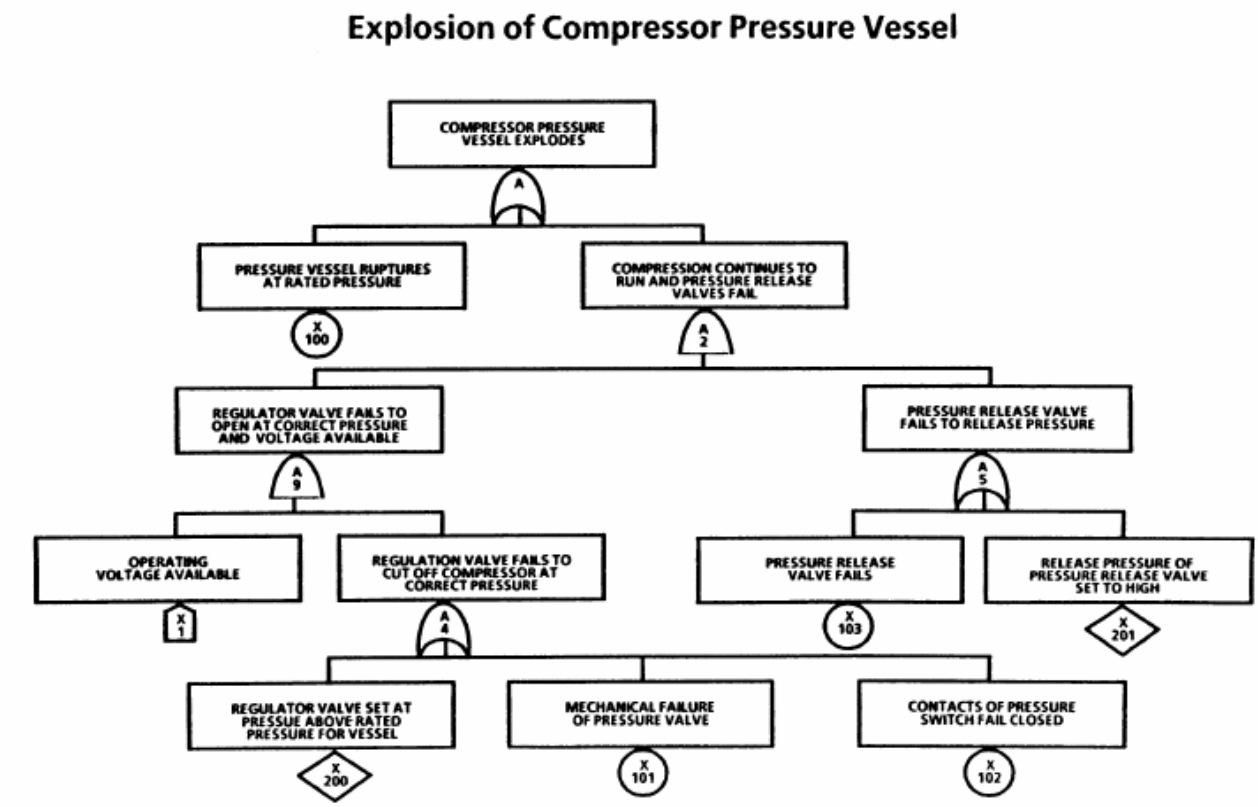

Figure B-3, Sample System Fault Tree

C APPENDIX C - HAZARD REPORT FORMAT

Hazard Report Identifier: <1>	**Date: <2>** **Revision:**	**Review Level: <2a>**
Title: <3>	Status: <4> ___Open ___Closed	
Closure Classification: <5> ___Eliminated	___Controlled	___Accepted Risk

System: <6>	Subsystem: <6>	Component: <6>
Affected Element: <7>		
Mission Phase: <8>		
Hazardous Condition Description: <9>		

Risk Matrix <13>
(Hazard Severity and Likelihood of Occurrence with controls in place)

Likelihood	Negl	Minor	Marg	Crit	Cat
Very High					
High					
Mod					
Low					
Very Low					

Severity

Acceptance Rationale: <10>
Likelihood Justification: <11>
Accepted Risk Cause(s): <12>

Figure C-1: Constellation Hazard Report Form (page 1 of 4)

Hazard Report Identifier: <1> **- Continued -**	**Date Baselined: <2>** **Revision:**	**Review Level: <2a>**
Title: <3>		
A. Cause <14> (Fault Tree Reference) 1. Effect(s) <15> 1a. Integrated System Hazard(s) <15a>	Severity: <19> Likelihood of Occurrence: <20> Classification: <21>	
Control(s): <16>	Verification(s): <17>	Status: <18>
B. Cause <14> (Fault Tree Reference) 2. Effect(s) <15> 1a. Integrated System Hazard(s) <15a>	Severity: <19> Likelihood of Occurrence: <20> Classification: <21>	
Control(s): <16>	Verification(s): <17>	Status: <18>

Figure C-1: Constellation Hazard Report Form (page 2 of 4)

Hazard Report Identifier: <1> **- Continued -**	**Date Baselined: <2>** **Revision:**	**Review Level: <2a>**
Title: <3>		
Safety Requirements: <22>		
Interfaces: <23>		
FMEA/CIL Reference: <24>		
Operations Related Documentation: <25>		
Detection and Warning Methods: <26>		
Background: <27>		
Logic Diagrams: <28>		
Attached Supporting Data: <29>		
Preparing Engineer: Org/ E-mail/ Phone:		Date:
Hazard Report Point of Contact: Name Org/ E-mail/ Phone:		

Figure C-1: Constellation Hazard Report Form (page 3 of 4)

Hazard Report Identifier: <1> **- Continued -**	**Date Baselined: <2>** **Revision:**	**Review Level: <2a>**
Title: <3>		

HAZARD REPORT SIGNATURES PAGE

Name/Function/Organization	Concurrence/Approval:	Date
Project Manager	Concurrence: _____	Date _____
SR&QA Project Lead	Concurrence: _____	_____
Safety Review Panel Chair	Approval: _____	_____
	_____	_____
	_____	_____
	_____	_____

Figure C-1: Constellation Hazard Report Form (page 4 of 4)

References <#> are provided that correlate the data element to the HR.

<1> Hazard Report Identifier – Identification of the Hazard Report 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. Often referred to as the HR Number, this unique identification is assigned to a specific hazard report and is never reassigned or reused. This identifier is used to track the HR.

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

<2a>Review Level – The Program/Project milestone review phase that the Hazard Report is generated/updated for, such as Phase I, II, III, etc.)

<3> Title – Provide a descriptive title of the hazard to give insight to the coverage of the HR.

<4> Status – Report status is classified as *open* or *closed*.

<5> Closure Classification - The hazard closure classification is based on the most severe consequence as shown for each hazard cause. The closure classification will be controlled, accepted risk or eliminated.

a. Eliminated Hazard: A hazard that has been eliminated by completely removing the hazard causal factors. 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 operation.
b. Controlled Hazard: The probability 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.

<6> System/Subsystem/Component – Identify the system/subsystem/component within the element.

<7> Affected Element – Identifies the major element and flights to which the hazard is applicable.

<8> Mission Phase – (As appropriate) Prelaunch Engine Start, Pad Abort, Launch, ET Separation, On-Orbit, etc.

<9> Hazardous Condition Description – The description of the hazard defines the unsafe act or condition and the mission effect (worst case results of the hazard causes). Include a description in terms of one or more generic hazards, (i.e., fire/explosion, impact, toxicity, etc.). The description should be made explicit to specify the equipment involved

<10> Acceptance Rationale - Provide a summary rationale for accepting the HR classification. Also identify flight effectivity if HR is prepared for a specific flight

<11> Likelihood Justification: Provide a summary of the rationale for classification of the likelihood. Include assumptions, any experiential data, and a qualitative summary of the failure history, limitations, or uncertainties in the controls that provide the basis for establishing the likelihood or probability of the hazardous event occurring.

<12> Accepted Risk Cause(s) - Provide a management summary listing of each hazard cause that is classified as accepted risk

<13> Risk Matrix - The risk matrix will be completed by documenting each hazard cause severity, and likelihood of occurrence. The controls are considered to be in place when performing this severity and likelihood of occurrence assessment.

<14> Cause(s) – 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.

<15> Effect(s) – The effect(s) is/are the potential worst case results of` the hazard cause.

<15a> Integrated System Hazard(s) – Reference the associated integrated hazard when there are documented integrated effects. This data element can be satisfied by inclusion as a separate line item in the effects section. This data element is only required if there is an associated integrated HR.

<16> Control(s) – A description of all the necessary design/operational controls needed to mitigate this hazard cause, including documentation references, if applicable. The control methods identify techniques, specific design and operational features which control or eliminate the hazard cause and satisfy the Safety Requirement. Sufficient detail shall be provided to clearly reflect controls which mitigate/control the hazard. The hazard controls shall be numbered (indexed) to provide direct linkages with the appropriate Cause and Verification

<17> Verification(s) – The specific method of verification (test/analysis/inspection/procedure/ processes), applicable to each hazard control, referencing planned activities during phase II, and closure document number (if applicable) during phase III, used to assure the effectiveness of each hazard control. Details will include specific attributes to allow inclusion in appropriate engineering or procedures during development and audit of the verification data during certification and acceptance. 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, procedures, and flight processing/operations and maintenance requirements. Each verification method shall be indexed with its corresponding hazard control. When more than one method of verification is listed for a control, the verification methods and status will be sequentially listed with a unique identifier suffix (e.g. a, b, c, or ".1", ".2", ".3"). Traceability to the specific control information is required.

<18> Status – The status of each verification method (Open, Estimated Completion Date (ECD) if known, Closed).

<19> Severity – 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, marginal, minor, or negligible

<20> Likelihood of Occurrence – The likelihood is classified for each cause by assessing the controls that are in place and documenting them as very high, high, moderate, low, or very low

<21> Classification – Assign a classification to each hazard cause: controlled, accepted or eliminated risk.

<22> Safety Requirements – 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.

<23> Interfaces - Identify system interface(s) that are affected by and cause hazard conditions within the report, including facilities, GSE, and other elements.

<24> FMEA/CIL Reference – 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:
Criticality:

Item:
Failure Mode:

<25> Operations Related Documentation: Reference all Operational Maintenance Requirements and Specifications Documents (OMRSD), Operations and Maintenance Instructions (OMI), Launch Commit Criteria, and/or Flight Rules that are used as a control.

<26> Detection and Warning Method(s) – The techniques used to detect the hazardous condition, any critical threshold values, and timeliness of the Detection and Warning Method.

<27> Background –Include information which adds understanding to the hazard, changes to the hazard, and supporting documentation, etc. Document the chronology of major events associated with the hazard, including related flight history, test and significant failure summaries that drove design/operation changes, etc. Include a summary of the failure history or other anomalous events associated with the hazard cause as appropriate.

<28> Logic Diagrams – Fault trees or other diagrams that were used to derive the listed causes

<29> Attached Supporting Data – Description of the supporting data that must be attached to the HR to complete the presentation of hazard control(s) and to demonstrate complete compliance with requirements.

D APPENDIX D, XXX