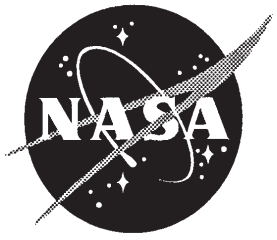
Safety Analysis and Risk Assessment Requirements Document

International Space Station Alpha Program

Revision E

October 28, 1994

National Aeronautics and Space Administration
International Space Station Alpha Program
Johnson Space Center
Houston, Texas
Contract No. NAS15–10000



REVISION AND HISTORY PAGE

REV.	DESCRIPTION	PUB. DATE
	BASELINE ISSUE (REFERENCE SSCBD BB000122 EFF 01-26-87)	01-15-87
A	REVISION A (REFERENCE SSCBD THE ELECTRONIC BASELINE REFORMATTED VERSION)	08-15-88
	CHANGE A1 (REFERENCE SSCBD BB000677 EFF. 01-18-91)	03-30-91
B	REVISION B (REFERENCE SSCBD BB511AR2 EFF. 10-23-91 AND BB000727 EFF. 09-28-90)	10-91
C	REVISION C (REFERENCE SSCBDs BB003134 EFF. 06-02-92 AND BB003135A EFF. 05-06-92)	07-92
	CHANGE C1 (REFERENCE SSCBD BB003206A EFF. 09-09-92)	10-92
D	REVISION D (REFERENCE SSCBD BB003339A EFF. 05-14-93 AND BB003681 EFF. 05-28-93)	06-93
E	REVISION E (REFERENCE SSCD 000123 EFF. 01-11-95)	01–21-95

PREFACE

The purpose of this document is to provide International Space Station Alpha Program Participants (ISSAPP) with consistent methodology for preparation and maintenance of the Safety Analyses, System Description, and Risk Assessment.

This document contains an introduction and paragraphs that discuss hazard identification, hazard classification, the Hazard Report form, and the treatment of safety risk in the Space Station Program.

The contents of this document are intended to be consistent with the tasks and products to be prepared by Program participants. The Safety Analysis and Risk Assessment Requirements Document may be implemented on new ISSA contractual activities and may be implemented on existing contracts by an authorized contract change. This document is under the control of the Safety IPT. Changes shall be approved by the Space Station Control Board.

/s/J. Harold Taylor	10–28–94
Safety and Mission Assurance Manager, International Space Station Alpha	Date

SSCD 000123	01–11–95
Program Manager (or delegated authority) International Space Station Alpha	Date

INTERNATIONAL SPACE STATION ALPHA PROGRAM
SAFETY ANALYSIS REQUIREMENTS DOCUMENT

AUGUST 24, 1994

CONCURRENCE

PREPARED BY:	Amy Hoang	S&MA	
	PRINT NAME	ORGN	
	/s/Amy Hoang	09/29/94	
	SIGNATURE	DATE	
CHECKED BY:	Carol Stewart	S&MA	
	PRINT NAME	ORGN	
	/s/Carol Stewart	10/31/94	
	SIGNATURE	DATE	
SUPERVISED BY (BOEING):	Peter Smoot	S&MA	
	PRINT NAME	ORGN	
	/s/Peter V. Smoot	09/29/94	
	SIGNATURE	DATE	
DQA:	Jeff Prince	2–6640	
	PRINT NAME	ORGN	
	/s/Jeff Prince	09/28/94	
	SIGNATURE	DATE	

INTERNATIONAL SPACE STATION ALPHA PROGRAM

SAFETY ANALYSIS AND RISK ASSESSMENT REQUIREMENTS DOCUMENT

LIST OF CHANGES

SEPTEMBER 29, 1994

All changes to paragraphs, tables, and figures in this document are shown below:

SSCBD	ENTRY DATE	CHANGE	PARAGRAPH(S)
			TABLE(S)
			FIGURE(S)
			APPENDIX(ES)
			ADDENDA

TABLE OF CONTENTS

APPENDIXES

FIGURES

TABLES

1.0 INTRODUCTION

The National Aeronautics and Space Administration (NASA) ISSAP has directed utilization of the requirements contained herein for safety analyses. Consistent application of these requirements will enable the integration of a meaningful safety risk assessment into the overall program risk management process. The integrated safety risk assessment program will include all ISSAPPs, each International Space Station Alpha (ISSA) system/subsystem, International Space Station support equipment, related software, ground operations, and flight operations to identify risk contributors and controls hazardous systems and functions. ISSAPPs include the International Space Station Alpha Program Office, the ISSA Prime Centers, Product Group (PG) contractors and their subcontractors-suppliers, Kennedy Space Center (KSC), and the International Partners (IPs).

1.1 PURPOSE

The purpose of this document is to provide ISSAPPs with consistent methodology for preparation and maintenance of the safety analyses and risk assessment. This document will clarify the relationships between the elements of safety analyses. The document also establishes the reporting requirements to assure commonality for integration of the results from supporting ISSAPPs.

The information presented herein clarifies and expands the safety requirements of NHB 1700.1 (V1-B) NASA Safety Policy and Requirements Document.

1.2 SCOPE

The requirements of this document apply to all ISSAPPs. Technical aspects of the hazard resolution process are addressed, but the programmatic resolution process description is left to NASA/Prime Safety & Mission Assurance Directorate. The document also addresses reporting on the results of the hazard analyses and the system description data package.

1.3 APPROACH

This document defines the overall process by which safety hazard analysis and risk assessment is performed and identifies the responsibilities of the participating ISSA activities. Each of the major safety analyses and products are discussed and a clear interpretation of how the safety analyses work together is provided. This document will also identify how the analyst should perform the analyses and produce the required safety documentation for distribution to all ISSAPPs. This approach to hazard analyses will also provide sufficient information on hazards to NASA/Prime for the performance of the Integrated Hazard Analysis and Risk Assessment.

The Safety Analysis Process is initiated by Hazard Analyses (HAs) which shall be performed by each contractor's safety organization and the International Partners as specified in section 3.0. Each represents an evaluation of the hazards associated with particular systems, subsystems, operations or equipment. The HA is the building block for the other safety analyses. The hazard identification process is augmented through specified cross-check of Critical Items List (CIL) results from the Failure Mode Effect Analysis (FMEA). The preliminary evaluation/classification process is described in terms of hazard characteristics and consequences

The Prime Contractor is responsible for the development of a comprehensive ISSA qualitative Logic Tree. The methodology and approach to the Logic Tree will be documented in the Integrated Risk Assessment section 4.0.

Qualitative Logic Trees shall be developed as a step in overall safety risk management. These Logic Trees shall differ from traditional fault trees in their utility in the verification of all hazard causes. Specifically, each bottom event of a qualitative Logic Tree should be referenced as a cause on a hazard report. The qualitative Logic Tree shall be used as a verification tool for the identification of new hazards and hazard causes.

Section 4.0 addresses the Integrated Risk Assessment to be conducted by NASA/Prime.

Section 5.0 addresses hazard resolution.

Section 6.0 addresses the hazard report and system description requirements.

Appendixes A and B provide the glossary and abbreviations and acronym list utilized by this document, SSP 30309.

Appendix C is reserved for future updates.

2.0 DOCUMENTS

The following documents include specifications, standards, guidelines, handbooks, and other special publications. The term “Current Issue” is shown in place of the specific date and issue when the document is under Space Station Control Board control. The documents have been grouped into two categories: applicable documents and reference documents.

2.1 APPLICABLE DOCUMENTS

2.1.1 NASA HANDBOOKS

The documents in this paragraph are applicable to the extent specified herein.

DOCUMENT NO.	TITLE
NHB 1700.1 (V1.B)	NASA Safety Policy and Requirements Document

2.1.2 MILITARY STANDARDS

MIL-STD-882B	System Safety Program Requirements

2.2 REFERENCE DOCUMENTS

The documents in this paragraph are provided as reference material for background information only. In case of conflict, this document shall take precedence.

DOCUMENT NO.	TITLE
NHB 5300.4 (1D-2)	Safety, Reliability, Maintainability, and Quality Provisions for the Space Shuttle Program
NMI 8070.4	NASA Management Instruction, Risk Management 1988 Policy for Manned Flight Systems
SSP 30234 (TBD)	Instructions for Preparation of Failure Modes and Effects Analysis and Critical Items List for Space Station
SSP 30599 (TBD)	Safety Review Process
SSP 50021 (TBD)	Space Station Safety Requirement

3.0 HAZARD ANALYSIS

Hazard analyses are performed by identifying, evaluating, and classifying a hazard. This information is used to guide technical resolution development. Hazard identification is accomplished by application of individually developed and applied analysis techniques against each system, subsystem, or operation (including software), with keyed tracking through documentation of each analytical step. The following hazard analyses will be performed: Preliminary Hazard Analysis (PHA), System Hazard Analysis (SHA), Subsystem Hazard Analysis (SSHA), and Operating and Support Hazard Analysis (O&SHA). In conjunction with each of the above analyses, the applicable software will be evaluated by the techniques described in section 3.4, Software Safety Analysis. For each HA, a CIL cross-check will be performed. These primary analyses are described in the paragraphs which follow.

The evaluation/classification process is approached in terms of ratings of hazard characteristics and consequences. The classification of hazards are applied in accordance with requirements provided in this section. Subsequently, safety risk assessment addressed in section 4.0 are used to methodolocially, relatively rank, and explore significant hazards that are identified by the hazard analysis process.

3.1 HAZARD IDENTIFICATION

A hazard is the presence of a potential risk situation caused by an unsafe act or condition. Hazard identification is a process for determining and characterizing information relating to a hazard and documenting in a manner for management to review and understand.

To begin the hazard identification process, the analyst must become familiar with the item to be analyzed as well as the environment and planned operations to be reviewed. Analytical effort and rationale should be documented progressively and systematically.

The following analyses shall be accomplished during the program phases indicated. NASA/Prime shall be responsible for the development of an integrated ISSAP hazard analysis which utilizes all other ISSAPPs analyses and properly identifies and assesses system level and interface hazards per stage. ISSAPPs shall be responsible, however, to deliver information related to each hazard according to the Statement of Work (SOW). All analyses shall include the data specified in Figure 3.1-1, Hazard Report Legend.

TEAM NAME
International Space Station Alpha

Hazard Report Number

---

1. HAZARD TITLE:

a. Review Level:
b. Revision Date:
c. Scope:

2. HAZARD CONDITION DESCRIPTION:

3. CAUSE SUMMARY:

1. Title:
2. Title:
3. Title:

4. PROGRAM STAGE(S):

5. INTERFACES:

6. STATUS OF OPEN WORK: (PHASE III ONLY)

7. REMARKS:

FIGURE 3.1-1 HAZARD REPORT LEGEND (PAGE 1 OF 6)

8. SUBMITTAL CONCURRENCE:

(a) U.S. Product Groups:

Tier 1 Subcontractor Safety Manager	Date
Tier 1 Integrated Product Team Manager	Date
Tier 1 Program Manager	Date

(b) International Partners

Safety Manager	Date
Program Manager	Date

9. APPROVAL:

(a) Safety Review Panel

Panel Chairman	Date
Panel Chairman	Date

(b) For Phase III (ONLY)

NASA Manager, Space Station Program	Date

FIGURE 3.1-1 HAZARD REPORT LEGEND (PAGE 2 OF 6)

Hazard Report Number

Cause 1

1. HAZARD CAUSE DESCRIPTION:

SEVERITY: **LIKELIHOOD:**

2. CONTROL(S):

Control 1.

Control 2

.

.

Control n

3. METHOD FOR VERIFICATION OF CONTROLS:

Verification for Control 1

Verification for Control 2

.

.

Verification for Control n

4. SAFETY REQUIREMENT(S):

Document: Paragraph:

Title:

Document: Paragraph:

Title:

FIGURE 3.1-1 HAZARD REPORT LEGEND (PAGE 3 OF 6)

5. MISSION PHASE(S):

_____ Launch Processing:
_____ Launch:
_____ Rendezvous/Docking:
_____ Deployment:
_____ Orbital Assembly & Checkout:
_____ On-Orbit Operation:
_____ On-Orbit Maintenance:
_____ Return/Decommissioning:

6. PROGRAM STAGE(S):

7. DETECTION AND WARNING METHOD(S):

8. CAUSE REMARKS:

9. CIL REFERENCE:

10. POINT OF CONTACT:

Name: **Telephone:**

FIGURE 3.1-1 HAZARD REPORT LEGEND (PAGE 4 OF 6)

Hazard Report Number

Cause 2

1. HAZARD CAUSE DESCRIPTION:

SEVERITY: **LIKELIHOOD:**

2. CONTROL(S):

Control 1.

Control 2

.

.

Control n

3. METHOD FOR VERIFICATION OF CONTROLS:

Verification for Control 1

Verification for Control 2

.

.

Verification for Control n

4. SAFETY REQUIREMENT(S):

Document: Paragraph:

Title:

Document: Paragraph:

Title:

FIGURE 3.1-1 HAZARD REPORT LEGEND (PAGE 5 OF 6)

5. MISSION PHASE(S):

——— Launch Processing:
——— Launch:
——— Rendezvous/Docking:
——— Deployment:
——— Orbital Assembly & Checkout:
——— On-Orbit Operation:
——— On-Orbit Maintenance :
——— Return/Decommissioning:

---

6. PROGRAM STAGE(S):

---

7. DETECTION AND WARNING METHOD(S):

---

8. CAUSE REMARKS:

---

9. CIL REFERENCE:

---

10. POINT OF CONTACT:

Name: **Telephone:**

FIGURE 3.1-1 HAZARD REPORT LEGEND (PAGE 6 OF 6)

HAZARD REPORT LEGEND

FOR TOP LEVEL PAGES

HAZARD REPORT NUMBER: AAAA-NNNN-RR

A. Identification of Team originator:

N. Sequential number. The number must be unique to the team originator and identify entries associated with a single category of hazard.

R. Alpha character indicating the revision of the report.

1. TITLE: Enter a brief description of the hazard in terms of hazard initiator, action or consequence.

a. REVIEW LEVEL: Enter the milestone review the hazard report was written for (Phase I, Phase II, Phase III, etc.)

b. REVISION DATE: Enter the date the hazard report was entered or revised.

c. SCOPE: Describe the scope of the hazards being addressed including, as appropriate, the end item, system, subsystem, Orbital Replacement Unit (ORU), and operation.

2. HAZARD CONDITION DESCRIPTION: The hazard description should define the risk situation including the unsafe act or conditions and its effect on station, shuttle, or personnel.

3. CAUSE SUMMARY: List the titles of causes associated with this hazard.

4. PROGRAM STAGES: Using the ISSA Assembly Sequence Manifest, identify the Stage(s) in which the hazard manifests itself.

5. INTERFACES: Identify the segments of the Space Station that may be associated with detection or control of the identified hazard.

6. STATUS OF OPEN WORK: Indicate the status of each open verification method. (Phase III only)

7. REMARKS: Entries here should include any information relating to the hazard but not fully covered in any other item field.

8. SUBMITTAL CONCURRENCE: The indicated managers from the applicable End-Item developer shall sign the hazard report prior to release outside of the company. Signature indicates agreement with the content at the current phase or level of program maturity and accuracy.

9. APPROVAL: The indicated Safety Review Panel Chairman shall sign the hazard report. The signature indicates agreement with the content at the current phase or level of program maturity and accuracy.

HAZARD REPORT LEGEND

FOR EACH CAUSE PAGE

1. HAZARD CAUSE DESCRIPTION: Describe the types of phenomena that are of concern, i.e., the key factor to be assessed as leading to the expected outcome/consequence.

> **SEVERITY:** This index quantifies the worst case accident or undesired event resulting from this cause. Severity levels are I (Catastrophic), II (Critical), and III (Marginal) as specified in Table 3.1.1.2-1, Severity Category. Hazard Report with Severity Level of III (Marginal) shall not be brought forth to the Safety Review Panel.
>
> **LIKELIHOOD:** The likelihood (probability of occurrence) of this hazard cause manifesting itself after controls have been implemented. Likelihood levels are A, B, C, and D, with A being the most probable as specified in Table 3.1.1.2-2, Likelihood of Occurrence

2. CONTROL(S): Provide 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 which will be or are used to control or eliminate the hazard cause and thereby satisfy the Safety Requirement. Sufficient detail shall be provided to clearly reflect controls which mitigate/control the hazard. The hazard controls shall be numbered to provide linkages with Method of Verification of Controls.

3. METHOD FOR VERIFICATION OF CONTROL(S): Identify for each control method the method of verification (procedure/processes), including document number if applicable, used to assure the effectiveness of the hazard controls. Each control verification method must link with its corresponding control, and when more than one method of verification is listed for a control, the verification methods will be listed separately (e.g., 1a, 1b, 2, 3a, 3b, 3c). Each verification method description shall include sufficient detail or explanation of the testing, inspection, or analysis which mitigates the hazard to support hazard closure or risk acceptance.

4. SAFETY REQUIREMENT(S): Identify the design requirements used this cause.

5. MISSION PHASE(S): Identify the phase of the mission in which the hazard manifests itself. An (X) indicates that the identified phase is affected by the hazard. An (O) indicates that it has been considered but is not affected.

Launch Processing covers the time period where the hardware arrives at launch site, is processed into the launch vehicle and extends to T-0.

Launch covers the time period from T-0 through orbital insertion.

Rendezvous/Docking covers the time period from orbital insertion until launch vehicle is docked to the Stage.

Deployment covers the time period from launch vehicle docking through detachment of the segment or end item from the launch vehicle .

Orbital Assembly & Checkout covers the time period from detachment from the launch vehicle, mating to the pre-existing stage, checkout and launch vehicle demate.

On-Orbit Operations covers Stage operations from launch vehicle demate until the next launch vehicle mates to the on-orbit stage.

On-Orbit Maintenance covers the maintenance tasks and the tests required for verification of maintenance action completion.

Return/Decommissioning

Return covers the time period from launch vehicle demate, from the on-orbit stage, through element removal from launch vehicle on the ground. Decommissioning covers the time period from element disassembly, form the on-orbit stage, through final disposal of the elements.

6. PROGRAM STAGES: Using the ISSA Assembly Sequence Manifest, identify the Stage(s) in which the hazard manifests itself.

7. DETECTION AND WARNING METHOD(S): When applicable, describe the technique(s) used to detect the hazardous condition.

8. CAUSE REMARKS: Entries here should include any information relating to the hazard cause but not fully covered in any other item field.

9. CIL REFERENCE: Provide the CIL numbers used in this analysis broken out by cause.

TABLE 3.1.1.2-1 SEVERITY CATEGORY

Description	**Category**	**Mishap Definition**
Catastrophic	I	Any condition which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the orbiter, ISSA or major ground facility. Loss of ISSA: Loss of the ISSA is to be limited to those conditions resulting from failures or damages to elements in the critical path of the ISSA that render the ISSA unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISSA in a condition which prevents further rendezvous and docking operations with ISSA launch elements.
Critical	II	Any condition which may cause a non–disabling personnel injury, severe occuptational illness; loss of a ISSA element, on–orbit life sustaining function or emergency system; or involves damage to the orbiter or a major ground facility. For safety failure tolerance considerations, critical hazards include loss of ISSA elements that are not in the critical path for station survival or damage to an element in the critical path which can be restored through contingency repair.
Marginal	III	Any condition which may cause major damage to an emergency system, damage to an element in a non–critical path, minor personnel injury, or minor occupational illness.

TABLE 3.1.1.2-2 LIKELIHOOD OF OCCURRENCE

Description	Category	Mishap Definition
Probable	A	Expected to happen in the life of the program.
Infrequent	B	Could happen in the life of the program. Controls have significant limitations or uncertainties.
Remote	C	Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties.
Improbable	D	Extremely remote possibility that it will happen in the life of the program. Strong controls are in place.

10. POINT OF CONTACT: Provide the name and telephone number of the individual to be used as a point of contact for this cause.

3.1.1 PRELIMINARY HAZARD ANALYSIS

3.1.1.1 PURPOSE

The PHA is used to:

3.1.1.1.1 Identify hazards.

3.1.1.1.2 Determine their significance.

3.1.1.1.3 Establish safety requirements to eliminate or control them in accordance with the Hazard Reduction Precedence Sequence in section 5.3.

In addition, the data and information derived from this analysis will help to:

3.1.1.1.4 Foresee hardware, procedural, and system interface problems.

3.1.1.1.5 Provide visibility to management for program resource allocations.

3.1.1.1.6 Establish priority for safety efforts.

3.1.1.1.7 Identify areas for testing.

3.1.1.1.8 Identify areas for trade studies and further analysis.

3.1.1.2 DESCRIPTION

The PHA is performed to identify generic hazards, basic technical safety requirements, hazard controls, allow evaluation of alternative concepts, and to document an initial safety risk assessment of the concept or system.

Based on the best available data, including mishap data from similar systems and other lessons learned, hazards associated with the proposed design or function shall be identified and evaluated for potential hazard severity. (See Table 3.1.1.2-1). Proposed design requirements and other actions needed to eliminate hazards or to reduce the risk to an acceptable level shall be submitted to management as changes to the baseline technical requirements, and documented in the PHA.

3.1.1.3 PROGRAM PHASE

The PHA should be performed during the conceptual stage. Scheduled updates may be performed as design development progresses to provide a basis for establishment of design safety requirements early in the program. Ideally, this also would eliminate the possibility of costly design changes later in the program.

A PHA may be accomplished during any stage of product development with satisfactory usefulness. If the safety program begins at the conceptual phase of product development, initial safety requirements may be established from the PHA. If the safety program begins at some other stage of product development (e.g., production manufacturing), safety requirements which may impose possible design changes will be more difficult and costly.

3.1.1.4 APPLICATION OF PRELIMINARY HAZARD ANALYSIS RESULTS

The PHA documents recognized and anticipated design safety pitfalls, and provides requirements by which these pitfalls may be avoided. The methods of avoiding such pitfalls generally include:

3.1.1.4.1 Establishing preventive measures:

3.1.1.4.1.1 Initial safety requirements for design and procedures.

3.1.1.4.1.2 Design changes for hazard elimination.

3.1.1.4.2 Identifying areas that require further investigation:

3.1.1.4.2.1 Areas for further safety analysis and type of analysis.

3.1.1.4.2.2 Areas requiring testing.

3.1.1.4.2.3 Areas requiring trade studies.

3.1.1.4.3 Identifying applicable documents and standards.

In many areas of safety concern, design safety data already exist. The data are contained in applicable documents such as standards, criteria, specifications, requirements, and guidelines. Safety design data documents should be researched by the safety analyst. All applicable documents should be identified and specified to avoid guesswork as to which documents are applicable. All applicable safety portions should be specified so that the designer knows exactly what is required. However, only the specific requirements that are truly necessary to preclude the anticipated mishap(s) should be selected. Blanket application of general requirements wastes program resources. If a mission requirement prevents the use of established safety design data, the PHA should reveal why the data cannot be used. The PHA should show what design data will be applied to accomplish the intent of the established design data.

The results of the PHA are used by both design engineering and system safety engineering. Design engineering uses the results in their decision-making process to ensure an optimum design specification. In effect, safety requirements serve as constraints for the designer. Safety engineering uses the requirements from prior projects as a baseline to compare the safety of current or future designs. In addition, the results provide a road map for follow-on safety studies, analyses, and testing.

3.1.1.5 APPROACH

The particular approach used to accomplish the PHA depends on available resources such as funding, available time, and on the complexity and experience with the same or similar

products. The documentary format of each approach is, in itself, a method of performing the analysis.

Although each approach differs from the other, their basic formats are very similar. Each approach results in the identification of hazardous conditions and potential mishaps, with their related probable causes and potential effects. The major differences between approaches are the rigor of the method, the amount of information generated, and the overall usefulness of that information.

3.1.1.6 DATA REQUIRED

As is the case with most analyses, the PHA is performed by using the level of data available. At the conceptual phase, the following data are essential: requirements and specifications, conceptual drawings, block diagrams, conceptual procedures, and conceptual trade studies. As design development progresses, the PHA incorporates the more detailed data that become available as it transitions into the detail analyses of the subsystem, system, and operating and support hazard analysis formats.

3.1.2 SUBSYSTEM HAZARD ANALYSIS AND SYSTEM HAZARD ANALYSIS

3.1.2.1 PURPOSE

The purpose of the SSHA and SHA is to identify hazards existing within a system/subsystem. Through designed-in features, this technique is used to anticipate and prevent subsystem hazardous circumstances that may potentially result in mishaps. In addition to achieving a “before the fact” safe design, this technique lends itself to verifying system/subsystem design compliance to specified safety requirements.

In providing a method to analyze system/subsystem hazards, the SSHA accomplishes the following:

3.1.2.1.1 Identifies hazardous conditions and hazardous elements in subsystem designs.

3.1.2.1.2 Assesses the significance of the identified hazardous condition’s effects.

3.1.2.1.3 Provides a basis for establishing system safety preventive measures.

3.1.2.1.4 Provides verification of system/subsystem design compliance to specified safety requirements.

3.1.2.1.5 Examines the safety impact of failures.

3.1.2.1.6 Examines the hazard interface.

3.1.2.1.7 Identifies areas for ancillary analysis.

3.1.2.1.8 Provides specific detailed design information for ancillary analyses.

3.1.2.2 DESCRIPTION

The SSHA is an expansion of the PHA to the subsystem level for hazards within subsystems. The SHA accomplishes the same purpose, but at a higher level, dealing with interactions among the various subsystems and systems and with the environment. In general, the previous analyses are extended to encompass the total system and environment. The unique aspect of the SHA is its view of interfaces between the subsystems that comprise a system. Hence, it is an integrated analysis.

3.1.2.3 PROGRAM PHASE

The SSHA effort begins with detail design development. As the preliminary design definitions are established and preliminary/initial hardware drawings become available, the SSHA continues through the detailed design of components, equipment, and software.

The SHA effort should begin as system and subsystem design and interfaces (including software) are defined. The SHA should be upgraded for each succeeding milestone review and/or as a result of any system design and interface change.

3.1.2.4 APPLICATION OF SUBSYSTEM HAZARD ANALYSIS/SYSTEM HAZARD ANALYSIS RESULTS

The results of the SSHA/SHA provide information that accomplishes the following:

3.1.2.4.1 Identifies hazardous circumstances and potential mishaps inherent to the subsystem design.

3.1.2.4.2 Identifies the mishap agents required to create the problem.

3.1.2.4.3 Identifies areas that require further investigation.

3.1.2.4.4 Stores design data (for future use) pertaining to the system/subsystem.

Following the identification of hazardous circumstances and their relationships to the design, preventive measures may be established to eliminate or control the occurrence of these circumstances. Preventive measures will be specified as safety requirements and criteria measurement for design, processes, operators, and safety devices.

One distinct advantage of the SSHA is its ease of integration into an SHA. In this program involving multiple tiers of contractors, this is an invaluable aid. Each of the contractors may apply the SSHA to their particular subsystem(s) as design data and identification of safety-critical areas, and both will be in a form consistent and usable to the Prime Contractor in production of the system-level analysis.

3.1.2.5 APPROACH

The SSHA is simply an expansion of the PHA done on each subsystem to greater levels of design detail as the system matures. The SSHA looks inward, examining pieces of the subsystem for hazards posed to the system itself. The SHA looks outward, examining system-to-system interactions and system-to-environment effects of mishaps within the system under analysis.

3.1.2.6 DATA REQUIRED

As is the case with most analyses, the SSHA is performed using all available design data and information. At a minimum, the following data sources are required:

3.1.2.6.1 Preliminary design drawings.

3.1.2.6.2 Functional diagrams and descriptions.

3.1.2.6.3 Interface control drawings.

3.1.2.6.4 Failure reports.

3.1.2.6.5 Failure Mode Effects Analysis/Critical Item List.

3.1.3 OPERATING AND SUPPORT HAZARD ANALYSIS

3.1.3.1 PURPOSE

The purpose of an O&SHA is to ensure the safety of system elements (personnel, equipment, software, and hardware) during and from the performance of operations. Consideration must

be given to both automatic unmanned operations and manned or personnel operations. Human operations are often accompanied by the use of specific equipment in addition to their interface with system hardware, software, and environmental conditions. Thus, the task of analyzing operations becomes a complex problem, involving operational procedures, human engineering, equipment design, software design, hardware design, and environment, with mission objectives and parameters. Automatic unmanned operations are as complex, except that the human operator element has been eliminated.

The O&SHA is a tool of System Safety Engineering for analyzing proposed operations and identifying:

3.1.3.1.1 Hazards involved with operations, tasks, and procedures, including support operations (assembly, maintenance, resupply, refurbishment, etc.).

3.1.3.1.2 Mechanisms of mishap development associated with operations and support tasks.

3.1.3.1.3 Preventive procedures which can be used to avoid hazardous circumstances or reduce mishap effects.

The O&SHA as used in a system safety program will: provide guidelines and requirements for developing safe procedures from initial concepts; identify or develop safety requirements for input into operations and procedures; and guide the resolution of potential problems to assure a safe operating system. The O&SHA results are applicable to all system phases for the ISSAP.

3.1.3.2 DESCRIPTION

The O&SHA is performed to examine procedurally controlled activities. The O&SHA states objectives to be achieved and evaluates hazards resulting from the implementation of operations, tasks, and procedures to be performed by persons and equipment. The process also considers: planned system configurations at each phase of activity; facility interfaces; environments; supporting tools or other equipment specified for use; operations or task sequences, concurrent or parallel task effects, and limitations; biotechnological factors; regulatory or contractually specified personnel safety and health requirements; and potential for unplanned events, including hazards introduced by human error. The O&SHA also identifies the safety requirements and controls needed to eliminate identified hazards, or to reduce the associated risk to an acceptable level. The analysis should identify as a minimum:

3.1.3.2.1 Operations/activities that occur under, lead to, or create hazardous circumstances and their associated time periods plus the actions required to minimize risks during these activities and time periods.

3.1.3.2.2 Changes needed to support functional or design requirements to eliminate or control hazards in system hardware and software, facilities, tooling, or support/test equipment to eliminate or control hazards.

3.1.3.2.3 Requirements for safety devices and equipment, including personnel safety and life-support equipment.

3.1.3.2.4 Requirements and timelines for warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render-safe, and back-out).

3.1.3.2.5 Requirements for handling, storage, transportation, maintenance, and disposal of hazardous material.

3.1.3.2.6 Potentially hazardous conditions that may be induced into flight hardware during manufacturing, test, inspections, etc., and show up later during flight hardware/software use (including, for example, poor welding, unidentified hardware failures, X-ray effects on electronics, and contaminated fuel).

3.1.3.2.7 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.

3.1.3.3 PROGRAM PHASE

The O&SHA effort shall begin at the onset of the development of the manufacturing, processing, assembly, and operating procedures. The analysis is completed after all operating procedures have been written and verified. The O&SHA shall be updated, as needed, concurrent with any system, design, procedure, or operational change, including contingency operations planning.

3.1.3.4 APPLICATION OF OPERATING AND SUPPORT HAZARD ANALYSIS RESULTS

The results of the O&SHA are the identification and documentation of hazardous circumstances associated with the performance of operations. The O&SHA is also used to document recommended methods for eliminating or controlling the hazardous circumstances.

Methods for eliminating or controlling identified hazardous circumstances are specified in the Hazard Reduction Precedence Sequence. Procedural constraints resulting from the O&SHA will become part of the operational procedure.

3.1.3.5 APPROACH

The approach to the O&SHA depends upon two aspects: when, in the product life cycle, the analysis is being performed; and the intended purpose of the O&SHA, or where and how the results will be used.

If the analysis results are intended to solve specific problems or to ensure that suspected problems are alleviated, the analysis may be conducted as a part of a special trade study at any time of the program life cycle.

An optimal approach involves two phases: perform a generalized analysis during the conceptual phase; and subsequently perform a specific and detailed analysis during the procedure development phase. The general analysis would not be rigorous and would provide preliminary requirements and guidelines for design and procedural development. The identification of safety-related problem areas would require further detailed effort. The detailed analysis would begin with previously identified areas and would provide specific procedural safety requirements and caution and safety inputs to the developed procedures.

3.1.3.6 DATA REQUIRED

Data required for an O&SHA are: operation/system configuration information; information on safety critical areas; hazard checklists; and existing applicable safety requirements. These data packages are available from two major sources of information: concurrent program data and historical data.

Concurrent program data, such as drawings, schematics, flow diagrams, timelines, engineering analyses, previously performed safety analyses, trade studies, Program Evaluation Review Techniques diagrams, and narrative descriptions provide the configuration information. The data also provide information on safety-critical areas.

Safety analyses that may have been performed prior to or in conjunction with the O&SHA include: (1) PHA, may include encompose all hazards and (2) a Logic Tree Analyses. These analyses may provide varying amounts of the stated data, which may be used in performing the O&SHA.

3.1.4 CRITICAL ITEM LIST CROSS-CHECK

The CIL will be used to supplement the hazard analyses. Safety personnel will use the CIL to verify that each of the critical item has been addressed in the hazard analysis. To

cross-check the CIL, each of the CIL's failure mode will be checked for use as a hazard cause factor in the hazard analyses. The failure mode is then evaluated for coverage of its effect in the development of hazard mechanisms. If the cross check reveals new information, appropriate revisions or entries will be made to the hazard analysis.

3.1.5 OTHER IDENTIFICATION SOURCES

Any person or organization may perceive a hazard through random observation, intuition, common sense, or other methods of analysis or activity not described herein. Any ISSA hazard so identified must be reported, recorded, evaluated, and entered into the hazard analysis. Documented disclosure shall be made to the associated safety organization of the affected NASA Center, PGs, Prime Contractor, and the International Partners. The Prime Contractor will then ascertain whether or not the hazard is adequately treated by existing hazard information. If the hazard is not covered, then a new hazard analysis will be performed. If the hazard is covered, the prime contractor shall issue a letter stating the rationale of coverage, and no new hazard number is assigned.

3.2 HAZARD CLASSIFICATION

Hazards are classified by severity and likelihood of occurrence (see Tables 3.1.1.2-1 and 3.1.1.2-2).

3.3 HAZARD REPORT FORM

A Hazard Report Form will be used to bring issues to management. The report will contain the information in Figure 3.1-1, Hazard Report Legend.

3.4 SOFTWARE ANALYSIS

3.4.1 PURPOSE

As part of the total system safety analysis process the software is evaluated as a cause of hazards, as an active control to hazards, and as part of the detection and warning system. If the software is determined to be a contributing cause or control to a hazard, it requires specific detailed analysis that is then integrated into the total hazard analysis process.

3.4.2 DESCRIPTION

The objective of software analysis is to ensure that any system that involves software has an acceptable level of risk. The software analysis will be an integrated part of the system safety

analysis. The exact analysis techniques to be used depend on the application and function of the software, and the level of responsibility of the provider of the software. ISSA software safety analysis is done in accordance with MIL-STD-882B, Tasks 301, 302, 303, 305 and 306.

Safety-related hazards identified throughout the software development life-cycle process are tracked and documented through the hazard reporting system.

3.4.3 PROGRAM RESPONSIBILITIES

The activities and responsibilities necessary to perform the software analysis are documented in MIL-STD-882B. This details the approach for various analyses prescribed throughout the life of the station.

3.4.3.1 SOFTWARE REQUIREMENTS ANALYSIS

Software Hazard Requirements Analysis evaluates program and interface requirements, and identifies errors and deficiencies in the program requirements that could result in violation of safety objectives. Requirements analysis is defined by Task 301 in MIL-STD–882B and is a prime responsibility.

3.4.3.2 TOP-LEVEL DESIGN HAZARD ANALYSIS

Design analysis verifies that the program design correctly implements the safety requirements. Top-level design analysis is defined by Task 302 in MIL-STD–882B and is a Product Group responsibility.

3.4.3.3 DETAILED DESIGN HAZARD ANALYSIS

Detailed design hazard analysis is defined by Task 303 in MIL-STD-882B and is a Product Group responsibility.

3.4.3.4 SOFTWARE SAFETY TESTING

Software safety testing verifies analysis results, investigates program behavior, and confirms that the program complies with requirements. Software safety exercises program functions under both nominal and extreme conditions and includes nominal, stress, and performance testing. Software Safety Testing is defined by Task 305 in MIL-STD-882B and is a Product Group responsibility.

3.4.3.5 SOFTWARE/USER INTERFACE ANALYSIS

Software/user Interface Analysis ensures that the ISSA software system will be controlled in a safe manner. Software/user Interface Analysis is defined by Task 306 in MIL-STD-882B and is a Product Group responsibility.

3.5 PHASE HAZARD ANALYSIS REPORT

The content of the hazard analysis reports are a function of the system maturity and its proximity to the initial flight of the ISSA system.

Hazard reports shall be submitted with a level of maturity commensurate with the hardware, software, and operations that are being reviewed.

TABLE 3.5-1 LEVELS OF MATURITY

Product Maturity	Review Phase	Report Content
PDR	I	Hazard and Controls Identified
CDR	II	Controls Documented and Verification Identified
Launch - 1 year	III	Verification Complete*

*All verifications that are not complete at the Phase III level review shall be documented in a verification matrix to be provided in block 6 “Status of open work” of the hazard report.

The safety review phases and the content of the hazard analysis reports and data requirements for the phases (I, II, III) are identified in SSP 30599.

4.0 INTEGRATED SAFETY AND MISSION ASSURANCE (S&MA) RISK MANAGEMENT

This paragraph describes the methodologies which will be employed by the International Space Station Alpha Program (ISSAP) to perform integrated safety, reliability, maintainability, and quality technical risk assessments used for risk management decisions. The ISSAP will employ a qualitative assessment approach. The qualitative techniques are described in paragraph 4.4. Risk items which meet the criteria specified in paragraph 4.6 may be further assessed by quantitative methods as described in paragraph 4.4.9 on an exception as needed basis determined by NASA/Prime. The need for any quantitative analysis, as determined by the S&MA IPT/SSAIT, will require the participation of the S&MA Integrated Product Team (IPT), the Program Integration and Risk Management (PIRM) Analysis Integration Team (AIT), and the responsible System Architecture IPT.

The requirements, procedures, and criteria contained in this paragraph are tailored for the ISSAP from those defined generically in the NASA Risk Management Program: NMI 8070.4, Risk Management Policy for Manned Flight Programs.

4.1 PURPOSE

The purpose of S&MA risk assessment is to provide a disciplined and documented management of risks throughout the program life cycles of the ISSA, ensuring that program management risk disposition decision-making is supported by risk identification. S&MA risk assessment also provides an independent path for risk concerns to be elevated through the ISSA management structure and communicated to all concerned levels of ISSA management the significance for assessed risk levels, and the decisions made regarding risk disposition. Safety risk items are the hazard causes identified by the performance of hazard analyses. Reliability risk arises from the presence of critical items. Maintainability risk arises from the presence of technical maintenance issues which threaten the survivability of the ISSA and/or its crew. Quality risk items are issues which arise from the presence of technical problems during qualification and production of ISSA components. Integrated safety, reliability, maintainability and quality risk considers the joint risk of design and operational hazards coupled with items in the design which fail to meet failure tolerance, redundancy, maintainability, quality or fail-safe requirements.

4.2 OBJECTIVES

The objectives of the Space Station Risk Management Program are in consonance with the NASA Risk Management Program, whose requirements for manned space flight programs are documented in NMI 8070.4. The objectives of the Integrated S&MA Risk Management process are to provide step-by-step procedures to:

a. Evaluate Hazards, Critical Items, PRACA items, Mishaps, and Maintainability technical issues to identify S&MA risks (as described in SSP 30234, respectively)

b. Assess the significance and acceptability of the identified risks by ranking the Hazards, Critical Items, PRACA items, Mishaps, and Maintainability technical issues

c. Communicate the risk assessment to ISSA management

d. Support development of risk reduction options, as necessary, for increasing safety, reliability, maintainability, and quality, or providing risk acceptance rationale (with the assistance of S&MA Team Leads)

e. Support system design trade-offs and decision making by incorporation of the S&MA technical risk perspective, at the S&MA IPT/SSAIT descretion

f. Track the implementation of technical risk reduction decisions and technical risks accepted by the ISSA Program.

4.3 TREATMENT OF INTEGRATED S&MA RISK IN THE SPACE STATION PROGRAM

This section summarizes the general approach to integrated S&MA risk assessment and management to be employed in the ISSAP. Paragraphs 4.4 and others detail the instructions for performance of quantitative risk assessment and risk management for the ISSAP.

4.3.1 FEATURES OF INTEGRATED S&MA RISK ASSESSMENT AND MANAGEMENT

The process of Integrated S&MA Risk Assessment and Risk Management answers five questions:

(1) What can go wrong?

(2) What are the consequences and how do they arise?

(3) What is the likelihood?

(4) Is the activity nevertheless safe enough?

(5) If not, what are cost-effective means of improving safety?

The first three questions are associated with risk assessment. The fourth and fifth are fundamental to risk management.

The first two questions are answered by the development of the Hazard Analysis and FMEA/CIL.

The answer to the third question, “What is the likelihood?” can be expressed as determined by the likelihood of occurrence in Table 3.1.1.2-II. The likelihood of occurrence and severity

category provide a universal language to be used by engineers when communicating safety issues during the entire ISSAP. Furthermore the hazard cause likelihood may be modified and updated as new evidence comes to light.

This provides the ability to rank hazard causes by severity and likelihood of occurrence and to update this ranking.

The fourth and fifth questions are answered by employing the products of risk assessment to evaluate the significance of the things that can go wrong and, if necessary, the best means of correcting them.

4.3.2 S&MA RISK ASSESSMENT

Hazard analysis generates primary inputs to S&MA risk assessment. Reliability analyses, especially Failure Modes and Effects Analysis (FMEA), independently develop inputs on hazardous hardware failures. Maintainability analysis generates inputs based upon the ability to maintain critical items on the ISSA. Quality analysis provides additional inputs on failures.

Hazard analysis provides a qualitative perspective list of hazards. It assigns likelihood and severity of hazards using qualitative categories (per paragraph 3.0). Integrated S&MA risk assessment has the ability to more precisely and unambiguously evaluate, rank, and explore significant hazards, failure modes, and maintain ability and quality assurance issues as defined in SSP 30234.

4.4 INTEGRATED SAFETY AND RELIABILITY RISK ASSESSMENT INSTRUCTIONS

The theory of risk assessment introduced in paragraph 4.3 is based on the development of Logic Trees that represent the stage design and operations and their identified hazards. Figure 4.4-1, summarizes the step-by-step procedure for achieving this approach in the Space Station Program. The “qualitative” aspects of the approach to risk analysis are described in paragraphs 4.4.1 through 4.4.6 below, and Steps 1 through 6 in Figure 4.4-1. As noted above, the results of standard hazard analyses, FMEA, PRACA, waivers, and deviations are inputs to the process. In Step 7, the importance rankings of risk contributors are obtained for S&MA Integrated Risk Assessment. Step 8 determines the need for quantification of those risk contributors where qualitative assessment was inadequate for high confidence risk decisions (acceptance, or means of mitigation as determined by the S&MA IPT/SSAIT). A separate task order will be provided to initiate any quantitative risk assessment. In Step 9, specific models and/or databases are developed to aid in the analysis of those risk items approved for Quantitative Risk Assessment, with the assistance of S&MA Team Leads. A separate task order will be provided to initiate any quantative risk assessments.

4.4.1 STEP 1: DEFINE OBJECTIVES

As in any analysis, the purpose, scope, and specific objective of the study must be carefully defined. The most important aspect of this for an integrated S&MA risk analysis is the definition of the relevant consequence categories. It is anticipated that a fully developed integrated S&MA risk program for the ISSAP will address all of the following consequence categories:

a. Loss of or injury to Crew Member

b. Loss of Manned Station Element, the Launch or Servicing Vehicle or ISSA elements or components when part of NSTS Cargo Elements

c. Inadvertent Loss of Orbit

d. Loss of Attitude Control

e. Loss of Manned Element Habitability

f. Loss of Critical Mission Support Capability.

The Prime shall develop Logic Trees with the results from the contractor Hazard Analysis and FMEA/CIL and incorporate the results of the NASA/Prime Integrated Hazard Analyses and Integrated FMEA/CILs. The Logic Trees will include events related to hardware, software, crew operations and procedures, environments, and support operations.

The Logic Tree will evolve, grow, and be modified throughout the life of the ISSAP. During design, it will be performed at a level of detail commensurate with the design stage. Early in design, the Logic Tree will provide a safety and reliability perspective on the design concept and intent by identifying areas of concern to be corrected by the engineering, operations, and design groups. As the design concept stabilizes and detailed design progresses, the Logic Tree will provide safety and reliability insights into hazard cause interactions. Finally, the integrated S&MA risk assessment will provide an integrating tool to ensure that operational aspects are developed as intended; e.g., to maximize crew safety and mission success.

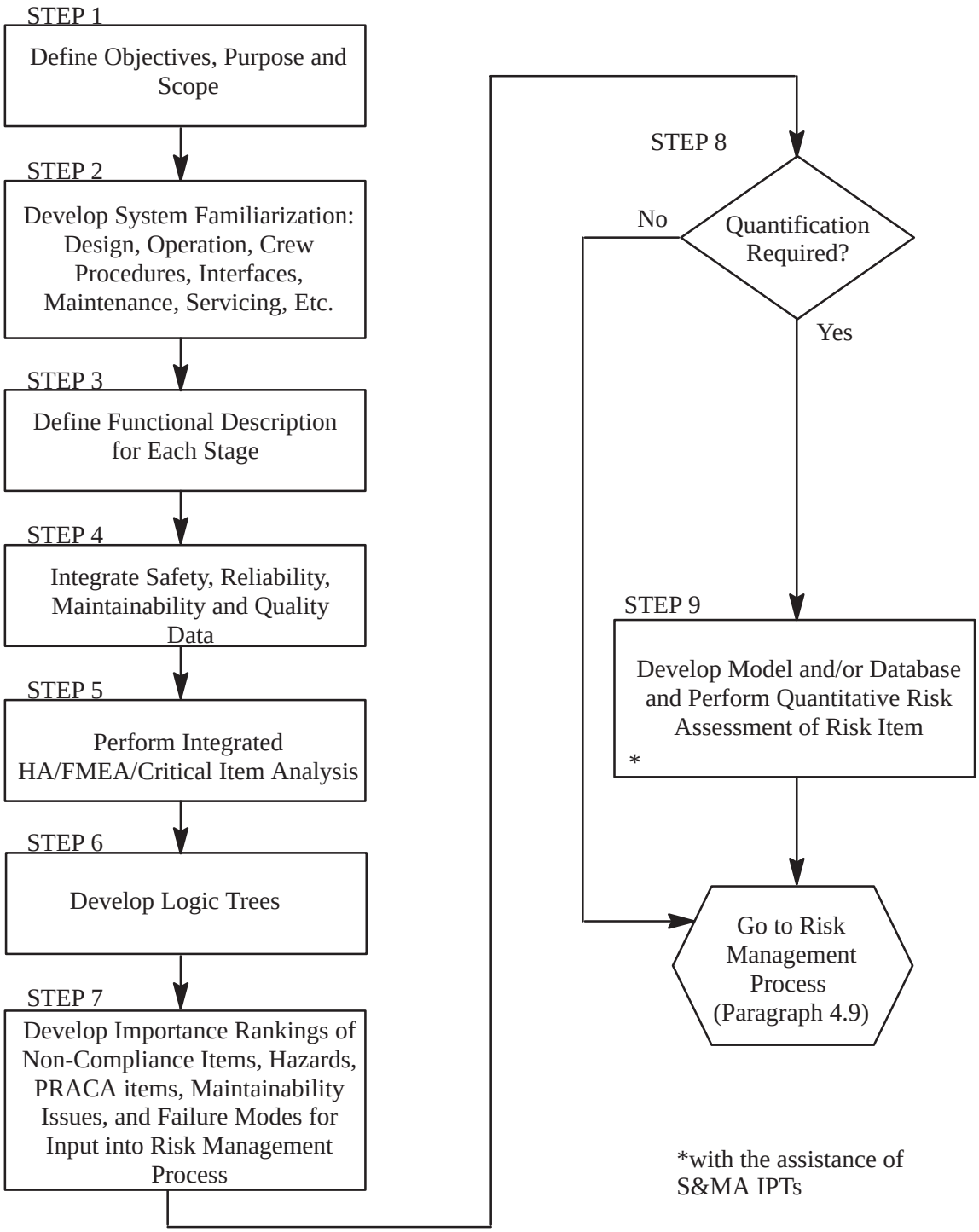


FIGURE 4.4-1 INTEGRATED RISK ASSESSMENT PROCEDURE

4.4.2 STEP 2: DEVELOP SYSTEM FAMILIARIZATION

An integrated S&MA risk analysis reflects the design, operation, support, and safety aspects of a system. A thorough knowledge of how the system works precedes Logic Tree development, Hazard Analysis, and Integrated S&MA Risk Assessment.

4.4.3 STEP 3: DEFINE SYSTEM FUNCTIONAL DESCRIPTION

A necessary precursor to the development of Logic Trees is a full understanding of a nominal, or successful, mission because departures from success are the basis for Logic Tree development. Therefore, it is necessary to define the set of system functions whose correct performance comprises success of the Space Station mission, and for each function to identify:

a. The minimum complement of subsystems required to perform that function;

b. The minimum complement of components of each subsystem required for successful performance of the function;

c. Given the degradation of a subsystem, the time interval over which the function degrades to a level of unacceptable performance. (For example: orbital decay period, system outages while awaiting maintenance, or loss of breathable atmosphere due to fire or meteoroid hit).

The above information will account for alternative, redundant, and backup means of performing the functions, and will be developed in conjunction with the ISSA Integrated Hazard Analysis.

4.4.4 STEP 4: INTEGRATE S&MA DATA

An integrated safety and reliability risk assessment of a very complex system such as the Space Station could involve a large number of Logic Trees. It is essential therefore to categorize, organize, and structure safety, reliability, maintainability and quality data in a way that makes the analysis traceable and the information useful. NASA and Prime will review the Contractor data to begin identifying areas where integration is required and to categorize significant risk items. NASA/Prime will utilize the data developed by the Contractor as an input to the development of Logic Trees (see paragraph 4.4.6).

4.4.5 STEP 5: PERFORM INTEGRATED HAZARD ANALYSIS/FMEA/CRITICAL ITEM ANALYSIS

As a result of the review of Contractor safety and reliability data, NASA/Prime will perform the Integrated Hazard, FMEA, and CIL analysis as defined in Section 3 and in SSP 30234.

Results of these analyses will be documented and archive for future reference. This completes the safety and reliability analyses needed to support the development of the Logic Trees, and the ISSA Integrated S&MA.

4.4.6 STEP 6: DEVELOP LOGIC TREE MODELS

Once the system functional models have been developed, the results of the Integrated FMEA activity and the Integrated Hazard Analysis activity will be utilized to develop the Logic Trees. Traceability to FMEA/CILs will be made through references in the Hazard Reports. Logic Tree events and causes will be used for additional risk analysis when directed by the S&MA IPT/SSAIT, on an as needed basis.

4.4.7 STEP 7: DEVELOP IMPORTANCE RANKINGS FOR RISK MANAGEMENT

The precursors to S&MA risk decision making are prioritized rankings of the contributors to risk. The importance ranking of each risk item will be obtained. As a minimum, the following shall be ranked.

a. Non-compliance item; i.e., an item which does not comply with program safety reliability, maintainability or quality assurance requirements.

b. Hazards: i.e., the relative importance of each significant hazard cause, as identified in paragraph 3.0.

c. Hardware/Software Failure Modes: i.e., the relative importance of failure modes, as identified by the FMEA process, such as single point failures.

d. Critical Items: i.e., the relative importance of each.

e. PRACA items affecting a critical or catastrophic hazard.

f. Maintainability issues affecting the ability to maintain ISSA critical items.

These lists of importance rankings will be documented in the Integrated Risk Items List (IRIL). Paragraph 4.7 discusses the IRIL in more depth.

The S&MA risks will be ranked by assigning a pre–determined risk factor number to each of the following five questions for each risk in question.

(1) Number of redundant paths.

(2) Time of exposure to hazard potential.

(3) Design confidence evaluation.

(4) Consideration of worst case effects.

(5) Human factors evaluation.

The product of these five risk factors will be used to establish a relative risk list for use by the S&MA AIT.

4.4.8 STEP 8: DETERMINE WHICH RISK ITEMS REQUIRE QUANTIFICATION

In general, those risk items that are well understood or assessed to be of low risk relative to the other risk items and have not already become a constraint to flight by qualitative assessment need not be quantified (NMI 8070.4 Risk Management Policy for Manned Flight Programs). The risk items not fully addressed by the qualitative risk assessment will be briefed to the S&MA IPT for decisions on committing additional resources for Risk Item quantifications.

It is expected that the configuration and operation of the ISSA will change throughout its life cycle. It is important therefore that the Logic Trees will incorporate such changes periodically in order to maintain a current safety perspective. As part of this configuration management, the need for quantification of risk items must be reassessed. This will ensure that evaluations of the S&MA impacts of modifications to the ISSA will take into account all relevant risk items.

Paragraph 4.6 provides detailed criteria for when quantitative analysis may be needed and guidance for determining if the criteria are met.

Performance of Quantitative Risk Assessment (QRA) on the ISSAP is reserved for risk items which have high potential risk to the program and are not well understood. The decision to perform a QRA rests with the S&MA IPT and Program Manager, ISSAP. Approval of a QRA by the Program Manager requires a specific allocation of budget and a written plan identifying the scope of the assessment, the risk item to be studied, the technical approach to the study, the performing organization(s), the schedule, and the cost.

4.4.9 STEP 9: DEVELOP MODEL(S) AND/OR DATABASE AND PERFORM QUANTITATIVE RISK ASSESSMENT OF RISK ITEM

The general strategy for quantifying a S&MA risk item if approved by the S&MA IPT, is to predict the risk of its parts. Thus, Step 9 is performed to break down high levels of assembly, such as systems and integrated elements for which there are little or no usable data, to their component parts for which data can be obtained. The data of interest are the magnitudes or numbers of exposures, failures, malfunctions, degrations, repairs, replacements, and servicing of parts of the system.

Before the Space Station is orbiting and operating, it will not be possible to obtain data about it that will precisely reflect the conditions under which it will operate. This will also be true of its component parts. The S&MA Integrated Risk Assessment must, at first, be based on data of types other than from experience under exact Space Station operating conditions. Such types of data are from tests and simulations, from applicable generic sources, or form informed engineering judgements. Specific tools and techniques to be used in the QRA will be tailored to the risk item to be studied and must be specified in the QRA plan when requesting NASA/Prime approval. Once approved, data will be collected, models will be created, analyses will be performed, and conclusions will be reached. These conclusions will be the basis for the recommendations made as a result of the QRA to the Risk Management Process.

4.5 CRITERIA FOR PERFORMING QUANTITATIVE RISK ASSESSMENT STEPS

The qualitative modeling discussed in Steps 1 through 7 of paragraph 4.4 will be performed for all safety and reliability data. Step 8, the application of the criteria for quantitative risk assessment, will be applied to each risk item. Consistent with the requirements of NMI 8070.4 risk items will be considered candidates for quantitative risk analysis by NASA/Prime when one or more of the following situations occur:

a. A risk item is judged, by qualitative means, to have catastrophic or critical severity and a high likelihood of occurrence, and has not already become a constraint for flight by qualitative assessment.

b. There exist significant uncertainty about the severity and/or likelihood of occurrence of a risk item.

c. The controls to prevent the risk item are of the least effective Hazard Reduction Precedence Sequence (warning systems/procedures) methods.

d. There exists significant uncertainty about the effectiveness of the controls proposed to mitigate the risk.

4.6 RISK REPORTING AND DOCUMENTATION

The entire information base, consisting of system descriptions, stage and element descriptions, risk assessment methodology, summary of significant findings, and required integration Hazard and FMEA/CIL worksheets will be documented and kept current. The Integrated Risk Assessment Report (IRAR) and Integrated Logic Trees mentioned in paragraph 4.4.2 will constitute this information base. These will be compiled and updated at NASA/Prime. The IRAR and Integrated Logic Trees will be maintained and archived by NASA/Prime for future reference and use by the ISSAP. The IRAR will be used by the S&MA IPT/SSAIT to track and disposition risks.

4.7 INTEGRATED RISK ITEM LIST (IRIL) RESOLUTION FOR RISK MANAGEMENT

Under ISSA S&MA IPT and ISSA Program Management direction, IRIL resolution will be performed by NASA/Prime, the PGs, and the IPs.

4.7.1 PURPOSE OF INTEGRATED RISK ITEM LIST RESOLUTION PROCESS

The purpose of the IRIL resolution process is to document the risk management procedures and results for reach IRIL item and, in particular, to document the closures for IRIL items. This process is based on the hazard resolution process discussed in paragraph 4.8.2.

4.7.2 DESCRIPTION

A hazard database input (per Figure 3.3-1) shall be completed for each item of the IRIL. Technical resolution begins with development of elimination or control options for each risk item of the IRIL. The options are proposed by design staff and engineering staff working in concert with S&MA staff at NASA/Prime and the Contractor. Selection of a preferred option is made according to the cost, schedule, risk reduction, and feasibility trade-off studies of the risk management process. The selected option is then considered for acceptability by ISSAP management, using appropriate reviews and boards. The residual risk associated with the selected option will be prioritized and documented in the IRAR during the time period during which the risk is dispositioned by the S&MA IPT/SSAIT. The decision to accept (or tolerate via a waiver) a risk and, thereby, cease to pursue risk reduction options for a risk item (i.e., achieve closure) will be made in accordance with S&MA IPT and ISSA Program Management instructions.

4.7.3 CLOSURE STATUS AND RATIONAL

4.7.3.1 CLOSURE STATUS

A risk item which has not yet been accepted (or tolerated) nor which an elimination or control option has been implemented is called an open risk item. A risk item which has been accepted or for which an elimination or control option has been completed to ISSAP management's satisfaction is called a closed risk item. All closed risk items must have a documented closure rationale.

4.7.3.2 CLOSURE RATIONALE

If the risk item has been eliminate, the closure rationale must contain the evidence used to establish that the risk item cannot occur or has negligible risk. If the risk item has been

accepted or tolerated, or if it has been controlled and the residual risk accepted, then the closure rationale must include the assessment of the accepted risk and the reason that no further risk reduction actions will be required. This rationale shall be included on hazard report forms.

4.8 RISK MANAGEMENT PROCESS

4.8.1 OBJECTIVES

The objectives of ISSAP S&MA Risk Management are:

a. Identify the risk contributors in an IRIL (see paragraph 4.8),

b. Determine the level of risk of each item in the IRIL in relation to program-specific criteria,

c. Recommend options to eliminate or control the risk of each hazard and failure mode,

d. Provide the safety and reliability risk-reduction benefits of the recommended options,

e. Assess the residual risk resulting from implementation of the recommendation integrated with cost, schedule impacts and other factors in management decision.

4.8.2 DEFINITION OF THE RISK MANAGEMENT PROCESS

The Risk Management Process delineated in Figure 4.9.1-1 includes the steps described in the following paragraphs.

4.8.2.1 S&MA INPUTS TO THE IRA

FMEA, CIL, H A and system descriptions prepared by the PGs, International Partners and other pertinent sources are provided to NASA/Prime by electronic means.

4.8.2.2 NASA/PRIME RISK ASSESSMENT

The S&MA data are reviewed and analyzed by NASA/Prime for risk issues using Logic Trees and other analytical techniques for connectivity and propagation across interfaces. These identified issues are documented in the IRIL (see paragraph 4.8). Detailed analyses of each item in the IRIL are performed and recommendation for changes, modifications, or controls (design or procedural) are developed.

4.8.2.3 S&MA IPT MANAGEMENT REVIEW

The most significant risk issues (as defined by the product of the five risk–factors in paragraph 4.4.7) identified in the IRAR will be brought to the S&MA IPT forum, for review of technical risks focused on safety, reliability, and maintainability, and quality. The purposes of this forum are: 1) to conduct NASA/Prime investigations into risks with recommendations for changes to reduce or mitigate those risks; and 2) to review NASA Prime, PG and IP S&MA analyses and make recommendations to the Space Station PIRM AIT and SSAIT. The S&MA IPT will review and discuss risk items on a priority basis, identify actions required to resolve the acceptability of the risks, and assign the actions to the proper organizations for resolution. The S&MA IPT will review the recommended resolutions, and approve and dispose of risk items through either of two channels. Acceptable risk items will be sent to configuration management for processing through the formal approval process. Questionable risk including those with recommendations involving design, cost, or schedule impacts will be forwarded to the PIRM AIT for further review. The forum is supported by input data from the Safety Review Panel, MOD Operations Engineering, PG, IP and other engineering data as appropriate. Subsequent to dispositions, the IRAR will be updated and a final revision released to NASA.

The S&MA IPT will review the top risk items and generate recommendations to the PIRM AIT/SSAIT regarding ISSAP approval.

4.8.2.4 PIRM AIT REVIEW

The PIRM AIT provides the following: assist the S&MA IPT with the assessment, analyze, and abatement of the risks from the IRL; and facilitate the resolution of major, program–level issues that cannot be dealt with from within the S&MA IPT.

4.8.2.4.1 S&MA AIT SUMMARY

Upon completing the IRAR, the S&MA IPT will approve the IRAR for release to the PIRM AIT. The PIRM AIT critiques and recommends corrective actions to the S&MA IPT. The S&MA IPT decisions specifying requirements changes or design changes will be forwarded to Configuration Management via Change Request (CR) for processing. The S&MA IPT recommendations concerning risk acceptance will be forwarded as required to the SSAIT/SSCB for approval.

4.8.2.5 CONFIGURATION MANAGEMENT

Configuration Management, with instructions form the PIRM AIT, will forward the risk issues to top management for approval or acceptance of the risk via either of two channels: a) SSCB approval or b) out of board approval.

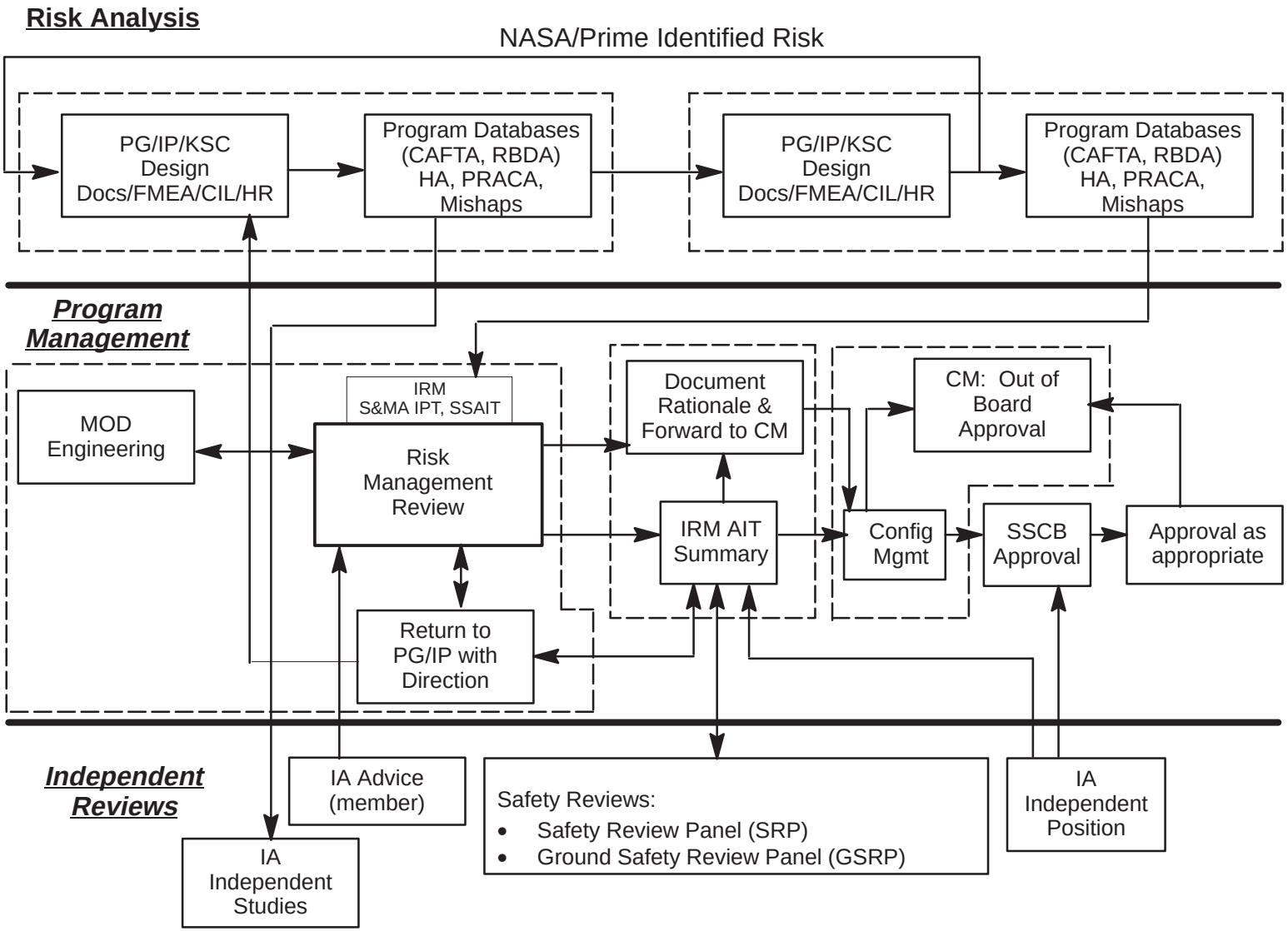


FIGURE 4.9.1-1 RISK MANAGEMENT REVIEW PROCESS

5.0 HAZARD CLOSURE AND APPROVAL

The ISSAP process for hazard resolution and approval of hazard closure is described in SSP 30599 entitled Safety Review Process.

5.1 PURPOSE

The purpose of the hazard resolution process is to evaluate the nature of each hazard, its level of risk, and its corresponding control. By evaluating the causes and effects of each potential mishap, the proposed hazard controls may then be classified and their corresponding impacts observed.

5.2 DESCRIPTION

The initial hazard classification process is outlined in Tables 3.1.1.2-1 through 3.1.1.2-2. Technical resolution begins with development of elimination and control options for each hazard consequence. The options are proposed by design staff working in concert with safety staff.

Implementation and approval of the hazard controls shall be recorded on a formal hazard report form to be supplied at an appropriate time in the development process. If there is some residual risk after a thorough hazard resolution process has been completed, the risk shall be categorized and the corresponding signature approval obtained in accordance with residual risk acceptance.

5.3 HAZARD CONTROLS

Design approaches are developed to control potential hazards in response to technical safety requirements which are derived from the safety analysis. Derived technical safety requirements should not dictate specific design solutions. Rather, they should state the requirement for safety in verifiable terms that will show that the reported hazard is either eliminated or controlled.

The associated selection of a particular hazard control method usually results from the performance of a trade study. Trade studies are typically conducted by systems engineering and design organizations, with participation by safety staff as necessary. The studies normally take into account costs, schedule impacts, and technical feasibility along with risk-benefit ratios in arriving at proposed solutions to resolve hazards.

5.3.1 HAZARD ELIMINATION

Hazard elimination is accomplished by removing the hazard source or by deleting the hazardous operations. Controlling the frequency is not considered a hazard elimination technique.

5.3.2 HAZARD REDUCTION PRECEDENCE SEQUENCE

Hazard control is accomplished by implementing measures to lower the frequency of occurrence and/or by mitigating the severity of the effects of the hazard. Four basic levels of mitigation used in this approach are listed below in order of their effectiveness and desirability.

5.3.2.1 DESIGN FOR MINIMUM HAZARD

The major goal throughout the design phase shall be to ensure inherent safety through provisions of appropriate design features, materials and parts selections, and safety factors. Damage control, containment, and isolation of potential hazards and failure tolerance considerations are to be included in design considerations.

5.3.2.2 SAFETY DEVICES

Known hazards which cannot be eliminated by design shall be reduced to an acceptable level by incorporating safety devices as part of the system, subsystem, or equipment.

5.3.2.3 WARNING SYSTEMS

Where it is not possible to preclude the existence or occurrence of a known hazard, warning and caution devices shall be employed for the timely detection of hazardous conditions and the generation of adequate warning and caution signals.

5.3.2.4 SPECIAL PROCEDURES

Where it is not possible to reduce the magnitude of an existing or potential hazard by design or by use of safety and warning devices, special procedures (including the requirement for personal protective clothing/equipment) shall be developed to counter hazardous conditions for enhancement of ground and flight crew safety.

5.3.3 RAISING DAMAGE THRESHOLD

Increasing damage thresholds with stronger materials, design resistance, or armor, such as personnel protective clothing and/or equipment can be used to minimize the effects of hazards. This method is used when susceptibility to the problem remains of concern in spite of the control implementation.

5.4 CLOSURE STATUS AND RATIONALE

5.4.1 STATUS

5.4.1.1 OPEN HAZARD

A hazard report 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.

5.4.1.2 CLOSED HAZARD

A hazard for which elimination or corrective action has been defined and planned for by NASA Program management for which controlled or accepted risk status has been granted by management.

5.4.2 CLOSURE RATIONALE

If the scenario has been eliminated, the closure rational must contain the evidence used to establish that the scenario cannot occur or has negligible risk. If the scenario has been accepted or tolerated, or if it has been controlled and the residual risk accepted, then the closure rational must include supported explanation for closure approval.

5.4.3 CLOSURE APPROVAL SIGNATURES

In order to formally document the closure of a hazard, management must affix their signature to the reported hazard. Approval and closure of all hazard reports will be made through the Safety Review Panel (SRP). This process will be documented in SSP 30599, Safety Review Process.

(This Page Intentionally Blank)

APPENDIX A ABBREVIATIONS AND ACRONYMS

A.1 ABBREVIATIONS AND ACRONYMS

AIT	Analyses and Integration Team
CAFTA	Computerated Fault Tree Analysis
CDR	Critical Design Review
CEI	Contract End-Item
CIL	Critical Item List
CM	Configuration Management
CSC	Computer Software Components
CSCI	Computer Software Configuration Item
DCR	Design Certification Review
DDHA	Detailed Design Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GSE	Ground Support Analysis
GSRP	Ground Safety Review Panel
HAs	Hazard Analyses
HR	Hazard Report
IA	Independent Assessment
IELD	Initiating Event Logic Diagram
IMR	Interim Management Review
IP	International Partner
IPT	Integrated Product Team
IRAR	Integrated Risk Assessment Report
IRIL	Integrated Risk Items List
IRS	Interface Requirements Specifications
ISSA	International Space Station Alpha
ISSAP	International Space Station Alpha Program
ISSAPP	International Space Station Alpha Program Participants
IVA	Intravehicular Activity
JSC	Lyndon B. Johnson Space Center
KSC	Kennedy Space Center
LeRC	Lewis Research Center

MISA	Mission Integrated Safety Assessment
MOD	Mission Operations Directorate
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NSTS	National Space Transportation System
ORU	Orbital Replacement Unit
O&SHA	Operating and Support Hazard Analysis
PDL	Program Design Language
PDR	Preliminary Design Review
PG	Product Group
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PIRM	Program Integration and Risk Management
PRACA	Problem Reporting and Corrective Action
QRA	Quantitative Risk Assessment
RBDA	Reliability Block Diagram Analysis
RCL	Risk Contributors List
RIC	Risk Index Classification
RMSR	Risk Management Status Report
SAR	Safety Assessment Report
SCCSC	Safety Critical Computer Software Components
SHA	System Hazard Analysis
SOW	Statement of Work
SRB	Safety Review Board
SRHA	Software Requirements Hazard Analysis
SRP	Safety Review Panel
SRS	Software Requirements Specification
SSCB	Space Station Control Board
SSHA	Subsystem Hazard Analysis
SSPE	Space Station Program Element
SSRP	System Safety Review Panel
SSS	System/Segment Software
STS	Space Transportation System
TBD	To Be Determined
THDA	Top-Level Design Hazard Analysis
TSE	Test Support Equipment

APPENDIX B GLOSSARY

B.1 GLOSSARY

Accepted Risk - A hazard that has not been eliminated and the residual risk has been accepted by project/program management on the basis of documented risk acceptance rationale.

Catastrophic Hazard - Any condition which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the orbiter, ISSA or major ground facility.

Loss of ISSA: Loss of the ISSA is to be limited to those conditions resulting from failures or damages to elements in the critical path of the ISSA that render the ISSA unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISSA in a condition which prevents further rendezvous and docking operations with ISSA launch elements.

Closed Hazard - A hazard for which elimination or corrective action has been defined and planned for by NASA Program Management which controlled or accepted risk status has been granted by management.

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, encode, cryogenic pump, star-tracker)."

Controlled Hazard - A hazard that has been reduced to an acceptable level by implementing the appropriate hazard reduction precedence sequence to comply with program requirements.

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 Hazard - Any condition which may cause a non-disabling personnel injury, severe occupational illness; loss of a ISSA element, on-orbit life sustaining function or emergency system; or involves damage to the orbiter or a major ground facility. For safety failure tolerance considerations, critical hazards include loss of ISSA elements that are not in the critical path for station survival or damage to an element in the critical path which can be restored through contingency repair.

Critical Items List - The CIL is a listing comprised of all critical items identified as a result of performing the FMEA. The CIL contains Criticality 1 and 2 single failure points and redundant items in life-essential applications which do not meet the program failure tolerance requirements. (See definition for critical item.)

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

a. Item(s) which cannot be checked out prelaunch or in orbit before being required to operate.

b. Item(s) whose loss cannot be detected by the flight or ground crew during any mission phase.

c. Item(s) which cannot be restored on orbit.

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, assures the loss of all redundant hardware element.

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 is 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 is 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 of 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 and generally include hazard causes from the environment, collision, fire/explosion (explosion/ implosion), vibration/shock/acoustic effect, thermal effects, contamination, radiation, electrical discharge, biological/physiological/ psychological impact, toxicity and other general items.

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

Hazard Analysis - 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 Closure Categories - Eliminated Hazard. A hazard that has been eliminated by removing the hazard source or by deleting the hazardous operations.

Controlled Hazard - Appropriate hazard reduction procedures have been incorporated, and a minimal residual risk remains. The likelihood of occurrence has been reduced to an acceptable level by implementing the appropriate hazard reduction procedure sequence to comply with program requirements.

Hazard Level

Catastrophic - Any condition which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the orbiter, ISSA or major ground facility.

Loss of ISSA: Loss of the ISSA is to be limited to those conditions resulting from failures or damages to elements in the critical path of the ISSA that render the ISSA unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISSA in a condition which prevents further rendezvous and docking operations with ISSA launch elements.

Critical - Any condition which may cause a non-disabling personnel injury, severe occupational illness; loss of a ISSA element, on-orbit life sustaining function or emergency system; or involves damage to the orbiter or a major ground facility. For safety failure tolerance considerations, critical hazards include loss of ISSA elements that are not in the critical path for station survival or damage to an element in the critical path which can be restored through contingency repair.

Marginal - Any condition which may cause major damage to an emergency system, damage to an element in a non–critical path, minor personnel injury, or minor occupational illness.

Mission Capabilities - Any condition which may cause loss of major mission capabilities.

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

Marginal Hazard - Any condition which may cause major damage to an emergency system, damage to an element in a non–critical path, minor personnel injury, or minor occupational illness.

Open Hazard - A hazard report 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.

Operating And Support Hazard Analysis - As described in NHB 1700.1 (V1.B) 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 - As described in NHB 1700.1 (V1.B) 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. Procedurally controlled hazards contain residual risk.

Risk - Exposure to the chance of loss of injury or loss. It is a function of the possible frequency of occurrence of an undesirable event and the potential severity of the resulting consequences.

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

Risk Index Classification - Represents the combination of the Severity Level and the Frequency codes to derive a subjective understanding for the magnitude of a hazard. This index is used in evaluation of the program significance of the hazard.

Risk Management - The process of balancing risk with cost, schedule, and other programmatic considerations. It consists of risk identification, risk assessment, decision making on the disposition of risk (acceptance, tolerance through waiver/deviations, or mitigation), and tracking the effectiveness of the results of the action resulting from the decision.

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

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

Safety Critical - Any component, configuration, or operation that may cause personnel injury or loss, loss of system, or damage to or loss of equipment or property.

Single Failure Point - As defined in NHB 5300.4, "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."

Subsystem Hazard Analysis - As described in NHB 1700.1 (V1.B) 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 - As described in NHB 1700.1 (V1.B) and this document. The SHA is identical to the SSHA but at the system level. Once the subsystems 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."

APPENDIX C RESERVED

(This Page Intentionally Blank)