

SSP 50146, Revision B

SSP 50146 Revision B

NASA/RSA BILATERAL S&MA PROCESS REQUIREMENTS FOR
INTERNATIONAL SPACE STATION

International Space Station Program



March, 2004

**National Aeronautics and Space
Administration
International Space Station
Program
Johnson Space Center
Houston, Texas**

**Rosaviakosmos
Moscow, Russia**

SSP 50146, Revision B

REVISION AND HISTORY PAGE

REV.	DESCRIPTION	PUB. DATE
-	Initial release per SSCD 000603, effective 06-12-97	02-20-98
A	Revision A per SSCD 000900 effective 05-28-99	08-16-99
B	Revision B per SSCD 008600 effective 03-14-05	04-07-05

SSP 50146, Revision B

PREFACE

ISS Program requirements for hardware and software safety and mission assurance requirements are defined and controlled in this document. This document establishes the applicable requirements for Safety, Reliability, Maintainability, and Quality Assurance between NASA and RSA.

In the implementation of safety and mission assurance requirements, consideration shall be given to criticality, complexity, state of hardware and software development, and unit and life cycle cost. The methods for implementing these requirements will be described in the respective Safety and Mission Assurance Plan (S&MA) from RSA.

This document is under the control of the Space Station Control Board (SSCB), and any changes or revisions will be approved by the Deputy Director.

SSP 50146, Revision B

NASA/Rosaviakosmos
INTERNATIONAL SPACE STATION PROGRAM

NASA Program Manager

Print Name

Date

_____/s/A. Krasouv_____
Rosaviakosmos

_____/A. Krasouv_____
Print Name

_____/03/12/05_____
Date

SSP 50146, Revision B

INTERNATIONAL SPACE STATION PROGRAM**NASA/RSA BILATERAL S&MA PROCESS REQUIREMENTS FOR INTERNATIONAL SPACE STATION****CONCURRENCE****OCTOBER 2004**

Prepared by:	<u>Nancy L. Steisslinger</u> JOINT AMERICAN-RUSSIAN SAFETY WORKING GROUP REPRESENTATIVE	<u>NE</u> ORG
	<u>/s/Nancy Steisslinger</u> SIGNATURE	<u>10/12/04</u> DATE
Controlled by:	<u>James W. Wade, PhD.</u> SAFETY & MISSION ASSURANCE PANEL	<u>OE</u> ORG
	<u>/s/Warren Pattison for</u> SIGNATURE	<u>10/12/04</u> DATE
Approved by:	<u>William H. Gerstenmaier</u> ISS, SPACE STATION CONTROL BOARD	<u>OA</u> ORG
	<u>/s/William H. Gerstenmaier</u> SIGNATURE	<u>10/13/04</u> DATE
DQA:	<u>Delegated Representative</u> CONFIGURATION MANAGEMENT REPRESENTATIVE	<u>ORG</u>
	<u>N/A</u> SIGNATURE	<u>DATE</u>

TABLE OF CONTENTS

1.0 INTRODUCTION	1
1.1 PURPOSE	1
1.2 SCOPE.....	1
1.3 GENERAL	1
1.3.1 NASA AND RSA ROLES AND RESPONSIBILITIES	1
1.3.2 NASA AND RSA MANAGEMENT APPROACH	2
1.3.3 SAFETY AND MISSION ASSURANCE PLAN.....	2
1.4 RELATION TO OTHER PROGRAM REQUIREMENTS	2
1.4.1 PROGRAM REQUIREMENTS	2
1.4.2 GSE	3
1.5 INDEPENDENT EVALUATIONS FOR NASA OR RSA	3
1.6 DATA ITEM DESCRIPTION (DID).....	3
1.7 MILESTONE REVIEWS	3
1.8 REFERENCE DOCUMENTS.....	3
2.0 SAFETY PROGRAM	5
2.1 SAFETY MANAGEMENT	5
2.1.1 ROLES AND RESPONSIBILITIES.....	5
2.1.1.1 NASA ROLES AND RESPONSIBILITIES:.....	5
2.1.1.2 RSA ROLES AND RESPONSIBILITIES.....	5
2.1.2 ORGANIZATION	6
2.1.3 SAFETY PLAN.....	6
2.1.4 SAFETY REVIEW REQUIREMENTS	6
2.1.4.1 SPACE STATION REVIEW.....	6
2.1.4.2 SPACE STATION CARGO	ERROR! BOOKMARK NOT DEFINED.
2.1.4.2.1 TECHNICAL SAFETY REQUIREMENTS FOR ISS CARGO.....	ERROR! BOOKMARK NOT DEFINED.
2.1.4.2.2 SAFETY REVIEW PROCESS FOR RSA ISS CARGO.....	ERROR! BOOKMARK NOT DEFINED.
2.1.5 MISHAP REPORTING AND INVESTIGATION	7
2.1.6 WAIVERS AND DEVIATIONS	7
2.2 SAFETY	7
2.2.1 OBJECTIVES.....	7
2.2.2 SAFETY TECHNICAL REQUIREMENTS.....	8
2.2.3 SAFETY ANALYSES	8
2.2.3.1 NASA GOVERNMENT EQUIPMENT FOR RS INSTALLATION.....	8
2.2.3.2 INTEGRATED SAFETY DATA	8
2.2.4 HAZARD ELIMINATION AND CONTROL	8

2.2.5 HAZARD REPORT/OFF-NOMINAL-SITUATION (ONS) CLOSURE CRITERIA	9
2.2.6 GROUND SUPPORT EQUIPMENT (GSE) SAFETY	9
2.2.7 REVIEW OF CHANGES	9
2.2.8 REVIEW OF FLIGHT AND GROUND HARDWARE FAILURES	10
2.2.9 EVALUATION OF TEST RESULTS	10
2.2.10 EVALUATION OF MISSION OPERATIONAL ACTIVITY	10
2.3 INDUSTRIAL SAFETY	10
2.3.1 GROUND OPERATIONS SAFETY.....	10
3.0 RELIABILITY AND MAINTAINABILITY (R&M).....	11
3.1 MANAGEMENT.....	11
3.1.1 NASA ROLES AND RESPONSIBILITIES	11
3.1.2 RSA ROLES AND RESPONSIBILITIES.....	11
3.1.3 RECIPROCITY	11
3.1.4 ORGANIZATION.....	12
3.1.5 PLANS.....	12
3.1.5.1 RELIABILITY AND MAINTAINABILITY PLAN.....	12
3.1.6 SUPPLIER CONTROL	12
3.1.6.1 SUPPLIER RELIABILITY AND MAINTAINABILITY CONTROL.....	12
3.2 RELIABILITY AND MAINTAINABILITY ENGINEERING.....	12
3.2.1 RELIABILITY AND MAINTAINABILITY DESIGN CRITERIA	12
3.2.2. FAILURE MODE EFFECTS ANALYSIS/CRITICAL ITEMS LIST (FMEA/CIL).....	12
3.2.2.2 RSA FAILURE ANALYSIS PROCEDURE.....	13
3.2.2.3 FAILURE MODE SUMMARY REPORT (FMSR)	13
3.2.2.4 CARGO FMEAs	13
3.2.3 CRITICALITY CATEGORIES.....	13
3.2.4 CRITICAL ITEMS LIST (CIL).....	13
3.2.5 R&M PREDICTIONS REPORT	13
3.2.5.1 RELIABILITY.....	14
3.2.5.1.A LIMITED-LIFE DATA.....	14
3.2.5.1.B RELIABILITY PREDICTION DATA	14
3.2.5.2 MAINTAINABILITY	14
3.2.6 DESIGN REVIEWS	14
3.2.7 REVIEW OF CHANGES	14
3.2.8 FAILURE REPORTING SYSTEM.....	14
3.2.9 VERIFICATION ASSURANCE	14
4.0 QUALITY ASSURANCE	15
4.1 MANAGEMENT.....	15

4.1.1 NASA ROLES AND RESPONSIBILITIES	15
4.1.2 RSA ROLES AND RESPONSIBILITIES	15
4.1.3 RECIPROCITY	15
4.2 QUALITY PROGRAM PLAN.....	15
4.3 ACCEPTANCE DATA PACKAGE (ADP).....	16
4.4 FAILURE REPORTING AND CORRECTIVE ACTION.....	16
4.5 CONTROL OF NASA AND INTERNATIONAL PARTNER (IP) PROPERTY.....	16
4.5.1 RSA RESPONSIBILITY	16
4.5.2 UNSUITABLE NASA OR IP PROPERTY.....	18
5.0 SOFTWARE QUALITY ASSURANCE.....	21
5.1 MANAGEMENT.....	21
5.1.1 ORGANIZATION	21
5.1.2 SOFTWARE PRODUCT ASSURANCE PLANNING	22
5.1.3 FORMAL AND INTERNAL REVIEWS	22
5.1.4 SUBTIER REQUIREMENTS.....	22
5.1.5 NONDEVELOPMENTAL SOFTWARE.....	22
5.1.6 NASA OR INTERNATIONAL PARTNER FURNISHED EQUIPMENT (GFE/IGFE).....	22
5.1.7 PROGRESS REPORTING.....	23
5.1.8 CONTROL BOARDS	23
5.1.9 OPERATIONS AND MAINTENANCE.....	23
5.1.10 TRAINING.....	23
5.1.11 SOFTWARE TOOLS.....	23
5.1.12 SOFTWARE PRODUCT ASSURANCE RECORDS	23
5.2 SOFTWARE QUALITY ASSURANCE.....	23
5.2.1 AUDITS.....	23
5.2.2 TOOLS, TECHNIQUES, AND METHODOLOGIES	24
5.2.3 SOFTWARE DOCUMENTATION.....	24
5.2.4 SOFTWARE CODE INSPECTION	24
5.2.5 SOFTWARE TESTING.....	25
5.3 CONFIGURATION MANAGEMENT	25
5.3.1 CONFIGURATION IDENTIFICATION, STATUS ACCOUNTING AND.....	25
VERIFICATION	
5.3.2 CONFIGURATION CHANGE CONTROL	25
5.3.3 SOFTWARE LIBRARIES	25
5.3.4 DEVIATIONS AND WAIVERS	26
5.4 NONCONFORMANCE REPORTING AND CORRECTIVE ACTION.....	26
5.4.1 NONCONFORMANCE REPORTING	26

SSP 50146, Revision B

5.4.2 PROBLEM REPORTING AND CORRECTIVE ACTION.....	26
5.5 RESERVED	26
5.6 SOFTWARE SAFETY.....	26
5.7 STANDARDS.....	26
5.8 TRADE STUDIES	27
5.9 INTEGRATION ASSURANCE.....	27
5.10 VERIFICATION AND VALIDATION.....	27
5.11 INDEPENDENT VERIFICATION AND VALIDATION (IV&V).....	27
5.12 CERTIFICATION.....	27
5.13 SECURITY AND PRIVACY ASSURANCE	27
GLOSSARY AND ACRONYMS.....	29
ATTACHMENT A - GROUND SAFETY REQUIREMENTS FOR RUSSIAN ELEMENTS LAUNCHED ON THE NASA SHUTTLE	A-1
ATTACHMENT B - DATA ITEM DESCRIPTION (DIDS).....	B-1
ATTACHMENT C - NASA/RSA SAFETY REVIEW PROCESS FOR ISS	C-1
ATTACHMENT D - NASA/RSA GENERAL PRINCIPLES AND REQUIREMENTS FOR ISS CARGO SAFETY	D-1
 ATTACHMENT E - NASA/ROSAVIKOSMOS/ESA TRI-LATERAL REQUIREMENTS FOR IMPLEMENTATION OF THE SAFETY AND MISSION ASSURANCE PROCESSES FOR THE ATV AND ISS RS.....	 E-1

1.0 INTRODUCTION

1.1 PURPOSE

This bilateral process agreement establishes specific roles and responsibilities that implement the interim agreement, establishes the ISS programmatic hardware and software safety and mission assurance requirements and defines the information and data exchanges which will allow NASA and RSA to conduct joint tasks successfully. This agreement is intended to be consistent with higher level agreements made in the Interim Agreement, the Joint Management Plan (JMP), and the Memorandum of Understanding (MOU).

1.2 SCOPE

Requirements defined in this agreement apply to all ISS elements developed by RSA and NASA, with respect to critical functions, as well as hardware and operations that may result in catastrophic hazards and/or crew injury in the event of an Off-Nominal Situation (ONS).

Where a reduced scope is applicable to Russian Transport Vehicles (Soyuz TM and Progress M, and Logistics Transfer Vehicle (LTV)) it is specifically delineated in the appropriate sections of this document. Automated Transfer Vehicle (ATV) safety is addressed in Attachment E to this document.

1.3 GENERAL

1.3.1 NASA AND RSA ROLES AND RESPONSIBILITIES

Overall roles and responsibilities in the S&MA area are established in Article 4 of the Interim Agreement between NASA and RSA which states the following:

- 4.1 In order to assure safety, NASA has the responsibility, working with the RSA and the Cooperating Agencies of the Space Station Partners, to establish overall Space Station safety and mission assurance requirements and plans.
- 4.2 RSA will develop detailed safety and mission assurance requirements and plans, using its own requirements for its Space Station hardware and software. Such requirements and plans must meet or exceed the overall Space Station safety requirements and plans. Requirements for which meet or exceed criteria are not appropriate will be determined by agreement of the Parties. RSA will have the responsibility to implement Space Station safety and mission assurance requirements and plans with respect to the elements and payloads it provides throughout the lifetime of the program, and to certify that such requirements and plans have been met. NASA will have the overall responsibility to certify that all Space Station elements and payloads are safe.

- 4.3 The Parties will support and exchange information necessary in order to conduct system safety reviews. The Parties will also conduct safety reviews of the elements and payloads they provide.

1.3.2 NASA AND RSA MANAGEMENT APPROACH

NASA and RSA management of S&MA shall include the following:

1.3.2.A Defining the major hardware and software safety and mission assurance tasks and assuring that they are performed as integral parts of all phases of the program

1.3.2.B Evaluating the safety, reliability, maintainability, and quality of hardware, software, and operations through analyses, tests, reviews, and assessments

1.3.2.C Providing timely status reporting through periodic project reviews and as a part of overall project status reports

1.3.2.D Ensuring compatible safety and mission assurance requirements among manufacturing, test, launch, and ground operations sites

1.3.2.E NASA shall assure that the results of the S&MA analysis on Russian Segment (RS) design conducted by RSA are integrated into ISS assessments activities.

1.3.3 SAFETY AND MISSION ASSURANCE PLAN

A Safety and Mission Assurance (S&MA) plan shall be prepared by RSA and NASA. This plan shall define the tasks and products of the Safety, Reliability, Maintainability, and Quality Assurance activities of the Russian and U. S. Segments and the organizational responsibilities for task implementation. The S&MA Plans shall be prepared in accordance with DID R-10-S01 and DID U-10-S08 for RSA and NASA, respectively.

1.4 RELATION TO OTHER PROGRAM REQUIREMENTS

1.4.1 PROGRAM REQUIREMENTS

The S&MA analytical and verification requirements set forth in this document shall take precedence in cases of conflict with requirements contained in sub tier documents. The RS S&MA design requirements are contained in SSP 41163, RS Specification International Space Station Program and the US S&MA design requirements are contained in SSP 41162, USOS Specification International Space Station Program. ISS components provided by RSA to NASA under the contract NAS 15-10110 may be covered by additional S&MA requirements stipulated by the contract.

1.4.2 GSE

1.4.2.A RS GSE hardware and software used at other than Russian ground sites shall be subject to the S&MA requirements of those facilities.

1.4.2.B USOS GSE hardware and software used at other than US ground sites shall be subject to the S&MA requirements of those facilities.

1.5 INDEPENDENT EVALUATIONS FOR NASA OR RSA

NASA and the RSA reserve the right to appoint independent representatives to assist in safety and mission assurance evaluation activities. These representatives will provide technical support to the applicable parent organization and determine effectiveness of and recommend improvements for S&MA activities.

1.6 DATA ITEM DESCRIPTION (DID)

DIDs which define the applicable S&MA documentation requirements for Russian and U. S. Segments elements shall be contained in SSP 50137, NASA/RSA Bilateral Data Exchange Agreement and in Attachment B of this document. The DIDs included in SSP 50137 shall take precedence in the event of a discrepancy.

1.7 MILESTONE REVIEWS

NASA and RSA S&MA activities shall include supporting internal and supplier design reviews, and ISS Program design and readiness reviews. Participation in milestone reviews shall assure that S&MA requirements are adequately considered.

1.8 REFERENCE DOCUMENTS

The following documents are reference documents that are invoked to the extent specified in the text of this document.

NSTS 13830B Implementation Procedure for NSTS Payloads System Safety Requirements

NSTS 1700.7B Safety Policy and Requirements for Payloads using the Space Transportation System

SSP 30223 Problem Reporting and Corrective Action System Requirements for the Space Station Program

SSP 30233 Space Station Requirements for Materials and Processes

SSP 30234 Instructions for Preparation of FMEA and CIL for Space Station

SSP 30309 Safety Analysis and Risk Assessment Requirements Document

SSP 50146, Revision B

SSP 30459 International Space Station Interface Control Plan

SSP 30599 Safety Review Process

SSP 41000 System Specification for the International Space Station

SSP 41162 United States On-orbit Segment Specification

SSP 41163 Russian Segment Specification

SSP 41170 Configuration Management Requirements

SSP 50021 Safety Requirements Document

SSP 50094 NASA/RSA Joint Specification/Standards Document for the ISS Russian Segment

SSP 50108 Certification of Flight Readiness Process

2.0 SAFETY PROGRAM

2.1 SAFETY MANAGEMENT

2.1.1 ROLES AND RESPONSIBILITIES

2.1.1.1 NASA ROLES AND RESPONSIBILITIES:

NASA Safety has the following roles and responsibilities for the ISS:

- a) To establish the overall safety requirements covering ISS detailed design, development activities, and mature operations and utilization.
- b) To certify that the overall integrated Space Station elements and cargo are safe.
- c) To conduct overall integrated system safety reviews for Space Station elements, launch packages and stages.
- d) To conduct safety reviews for the elements and cargo provided by NASA.
- e) To participate in and support as appropriate the reviews of other partners. To support these reviews, NASA will provide the necessary safety related information to enable the partners to conduct their reviews.
- f) To conduct interface hazards analysis between elements of the RS and elements of other International Partners (IP).

2.1.1.2 RSA ROLES AND RESPONSIBILITIES

RSA has the following roles and responsibilities:

- a) To develop detailed safety requirements which implement the overall safety requirements for the elements and cargo developed by RSA. These detailed requirements must meet or exceed the safety requirements in SSP 41163, including those specified in the SSP 50094, NASA/RSA Joint Specifications / Standards Document for the RS.
- b) To certify that the overall and detailed safety requirements have been met with respect to the elements and cargo RSA provides.
- c) To support the overall integrated system safety reviews conducted by NASA. This support includes participation as a developer and provider of safety data for elements being reviewed by the ISS Safety Review Panel (SRP). As a provider of data RSA participation in the meeting shall include the presentation of the safety data to the SRP and technical support to respond to questions related to the identification and control of hazards related to the detailed design and operation of the RS elements.

SSP 50146, Revision B

- d) To conduct safety reviews for the elements and cargo provided by RSA.
- e) To participate in and support as appropriate the reviews of other partners. To support these reviews RSA will provide the necessary safety related information to enable other IPs to conduct their reviews.
- f) To participate, as appropriate, in any Space Station safety review boards established by NASA. This includes membership in the ISS SRP which will conduct the overall integrated safety review of ISS elements. Elements being launched on the Space Shuttle shall be subject to the GSRP process documented in Attachment A. Cargo for the ISS shall be subject to the cargo safety process documented in Attachment D.
- g) To provide the support and information necessary for integrated analyses and assessments which lead to NASA's safety certification responsibilities.

2.1.2 ORGANIZATION

Organization of the NASA and RSA safety effort shall assure effective planning, management, implementation and performance of safety activities. While the accomplishment of all safety tasks may not be the responsibility of the same organizational element, management of the safety effort shall assure that all tasks are effectively accomplished.

2.1.3 SAFETY PLAN

The RSA and NASA safety organizations shall prepare, implement, and maintain a Safety Plan as a part of the S&MA Plan (Reference paragraph 1.3.3) which describes the compliance with requirements set forth herein.

2.1.4 SAFETY REVIEW REQUIREMENTS

2.1.4.1 SPACE STATION REVIEW

2.1.4.1.A SSP 30599, Safety Review Process, defines the safety review process that is used by NASA to implement its responsibilities for ISS elements.

2.1.4.1.B RSA shall utilize standard Russian S&MA processes to implement its internal responsibilities for the RS.

2.1.4.1.C To assure the joint review of RS Safety, RSA and NASA shall implement the safety review process defined in the "NASA/RSA Safety Review Process" provided in Attachment C.

2.1.4.1.D For RS Russian Transport Vehicles (e.g. Soyuz TM, Progress M, and LTV) NASA and RSA shall implement the Safety Review Process defined in the "NASA/RSA Safety Review Process" with the following reduced scope:

- Hazards to the ISS caused by any ISS vehicle that is temporarily in the proximity of or docked to the ISS must be identified and controlled. This excludes Hazards associated with autonomous flight of these vehicles (i.e. launch operations, orbit insertion, deorbit, and landing)
- Hazards resulting from the inability of the vehicles to perform critical ISS functions (Reference Attachment A)

2.1.4.2 SPACE STATION CARGO

The process for certification of the safety of Russian cargo on Shuttle and ISS, and NASA cargo on the Russian Segment and Russian transport vehicles, is defined in Attachment D “NASA/RSA General Principles and Requirements For ISS Cargo Safety”.

2.1.5 MISHAP REPORTING AND INVESTIGATION

Mishaps occurring during manufacturing, testing, and operations shall be investigated and reported as specified in the internal native specifications and reported in accordance to DID R-10-S03 and U-10-S09 for RS and USOS mishaps, respectively.

2.1.6 WAIVERS AND DEVIATIONS

The NASA and RSA will evaluate proposed hardware, software, and operational waivers and deviations for safety impact, and recommend disposition for management concurrence. Where the acceptance of a deviation or waiver impacts an existing hazard report, the hazard report will be updated to show the accepted risk status and resubmitted with the waiver or deviation.

2.2 SAFETY

2.2.1 OBJECTIVES

The NASA and RSA safety objectives are to identify and evaluate their respective design and operational activities to assure that measures are taken to minimize risks. Safety objectives include the following:

2.2.1.A Performing safety analyses to identify the hazards associated with hardware, software, and operations during all program phases

2.2.1.B Assuring that proper design and performance requirements are developed, documented, and implemented which will eliminate whenever possible or control the identified hazards.

2.2.1.C Providing appropriate documentation to enable NASA and RSA to perform an overall risk assessment including: the identification of residual hazards/risks and providing recommendations with supporting data and rationale for management awareness and decision on acceptance of the residual hazards/risks.

2.2.2 SAFETY TECHNICAL REQUIREMENTS

Safety technical requirements have been established for the RS and the USOS and are defined in SSP 41163, "ISS RS Specification" and SSP 41162 "ISS USOS Specification", respectively. These requirements should be identified and implemented in system design, operations, and procurement documentation including flight hardware and safety critical software.

2.2.3 SAFETY ANALYSES

NASA and RSA shall perform hazards analyses, including hardware hazards analyses, operational hazards analyses, and software hazards analyses.

2.2.3.A NASA shall document the results of the USOS hazard analyses on hazard report forms as defined in SSP 30599. This documentation will be provided to RSA in accordance with the established distribution to the ISS Safety Review Panel.

2.2.3.B RSA shall document the results of RS hazard analyses, as defined in the "NASA/RSA Safety Review Process" provided in Attachment C, on hazard report forms in accordance with DID R-10-S02.

2.2.3.1 NASA GOVERNMENT EQUIPMENT FOR RS INSTALLATION

NASA equipment installed in the Russian Segment shall be subject to the process for safety reviews described in "NASA/RSA Safety Review Process." RSA representatives shall take part in the work of the Safety Review Panel for this hardware.

2.2.3.2 INTEGRATED SAFETY DATA

To provide information required for the RS and ISS integrated hazard analysis, NASA and RSA will exchange Safety Data in addition to hazard analysis. NASA shall provide this data to RSA in accordance with DID U-10-S05 and U-10-S07. RSA shall provide this data in accordance with DID R-10-S04 and R-10-S06.

2.2.4 HAZARD ELIMINATION AND CONTROL

The foremost consideration for resolving hazards shall be to eliminate them by design through removal of hazard sources and hazardous operations. Corrective action priorities shall be established to achieve maximum benefit in reducing potential personnel and material losses. Actions for satisfying safety engineering requirements shall be in the following order of precedence:

2.2.4.A Hazard Elimination. The hazard source or the hazardous operation shall be eliminated.

2.2.4.B 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 selection, and safety factors. Control and isolation of potential hazards and failure tolerance considerations are to be included in design considerations.

2.2.4.C 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.

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

2.2.4.E 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.

2.2.5 HAZARD REPORT/OFF-NOMINAL-SITUATION (ONS) CLOSURE CRITERIA

A hazard report/ONS shall be considered closed only after at least one of the following conditions have been satisfied:

- (1) The hazard/ONS has been eliminated by a design or operational change, and the change has been implemented and verified or;
- (2) The hazard/ONS has been controlled in accordance with at least one of the corrective actions identified in paragraph 2.2.4.B through 2.2.4.E, and the controls have been verified by successful completion of the required design change, test programs, analytical studies, or training programs or;
- (3) The hazard has been accepted by program management. Signature of the phase 3 safety hazard report at the conclusion of the NASA/RSA Safety Review Panel meetings shall indicate ISS program approval of the identified hazard.

2.2.6 GROUND SUPPORT EQUIPMENT (GSE) SAFETY

2.2.6.A RS GSE safety requirements have been established for the RS and are defined in SSP 41163.

2.2.6.B USOS GSE safety requirements have been established for the USOS and are defined in SSP 41162.

2.2.7 REVIEW OF CHANGES

When changes are proposed for equipment design (hardware and software) or procedures, NASA and RSA safety organization shall assure the identification and resolution of hazards that may be introduced into the system. These hazards shall be documented in hazard reports in accordance with the DID R-10-S02 for the RS, and in accordance with SSP 30309 and SSP 30599 for the USOS, respectively.

2.2.8 REVIEW OF FLIGHT AND GROUND HARDWARE FAILURES

NASA and RSA safety organization shall review, provide recommendations and concur in failure resolutions associated with catastrophic and critical hazards.

2.2.9 EVALUATION OF TEST RESULTS

NASA and RSA safety organizations shall evaluate results of tests that verify design safety compliance.

2.2.10 EVALUATION OF MISSION OPERATIONAL ACTIVITY

NASA and RSA safety organizations shall participate in mission operational activities and make safety evaluations of anomalous conditions. These safety evaluations will provide guidance to plan future activities and to establish necessary corrective actions.

2.3 INDUSTRIAL SAFETY

2.3.A Russian Industrial and personnel safety standards apply for all ISS hardware while in Russian facilities.

2.3.B US industrial and personnel safety standards apply for all ISS hardware while in US facilities.

2.3.1 GROUND OPERATIONS SAFETY

2.3.1.A Russian ground operations safety standards apply for all ISS hardware while in Russian facilities.

2.3.1.B US ground operations safety standards apply for all ISS hardware while in U.S. facilities.

3.0 RELIABILITY AND MAINTAINABILITY (R&M)

3.1 MANAGEMENT

3.1.1 NASA ROLES AND RESPONSIBILITIES

- a) NASA is responsible for establishing overall R&M technical and process requirements which will be necessary to assure vehicle life and system availability for scientific utilization. In doing this, NASA defines the system level R&M design requirements and is responsible for allocating and coordinating the appropriate requirements with RSA for the RS.
- b) NASA defines and documents the analytical processes which are to be used to perform integrated R&M assessments for the ISS. NASA is responsible to identify and agree with RSA on the processes applicable to the RS and the data required to fulfill NASA's integration needs.
- c) NASA will be responsible to assure that R&M requirements allocated to the RS have been verified by the RS providers or that the requirements are specifically verified by NASA. NASA is also responsible to assist RS providers in identifying verification methods for each R&M requirement.
- d) NASA is responsible to provide the program manager and program teams with status of R&M requirements implementation and an assessment of the risk involved for further evaluation at the program level.

3.1.2 RSA ROLES AND RESPONSIBILITIES

- a) RSA is responsible for developing the R&M requirements allocated to the RS in SSP 41163, "ISS RS Specification" for the elements and cargo provided by RSA. These detailed requirements must meet or exceed the requirements of SSP 41163.
- b) For each R&M requirement allocated to the RS, RSA is responsible for defining and conducting verification activities necessary to assure that the requirement is met.
- c) RSA is responsible to provide status of implementation and verification results for R&M requirements to NASA.
- d) RSA is responsible to provide NASA with R&M data , in order to support NASA's responsibilities to perform integrated analyses of the ISS.
- e) RSA will be responsible for the certification of the R&M characteristics of the RS with respect to the overall program R&M requirements.

3.1.3 RECIPROCITY

NASA and RSA shall establish and maintain a Reliability and Maintainability function which possesses attributes, performs the functions, or supplies the data described herein.

3.1.4 ORGANIZATION

Organization of the NASA and RSA reliability and maintainability efforts shall assure effective planning, management, implementation, and performance of reliability and maintainability activities. While the accomplishment of all reliability or maintainability tasks may not be the responsibility of the same organizational element, management of the reliability and maintainability efforts shall assure that all tasks are effectively accomplished.

3.1.5 PLANS

3.1.5.1 RELIABILITY AND MAINTAINABILITY PLANS

The NASA and RSA reliability organizations shall prepare, implement and maintain an integrated reliability and maintainability (R&M) plan, or separate plans, as a part of the S&MA Plan, which describes how the reliability and maintainability requirements will be implemented, controlled and verified and shall be prepared and maintained in accordance with DID R-10-S01 and U-10-S08 for RSA and NASA, respectively.

3.1.6 SUPPLIER CONTROL

3.1.6.1 SUPPLIER RELIABILITY AND MAINTAINABILITY CONTROL

The RSA and NASA reliability and maintainability efforts shall assure that ISS (USOS and RS) hardware obtained from any source meets the reliability and maintainability requirements of the overall system.

3.2 RELIABILITY AND MAINTAINABILITY ENGINEERING

3.2.1 RELIABILITY AND MAINTAINABILITY DESIGN CRITERIA

The reliability and maintainability efforts shall include a systematic approach for reviewing and concurring in design and procurement specifications and in design changes to assure that all design items reflect proper and complete reliability and maintainability design criteria and that the specifications contain applicable reliability and maintainability requirements.

Reliability and maintainability engineering tasks shall be accomplished, to the extent specified, for all flight equipment. Maintainability engineering efforts shall support maintenance planning efforts as appropriate.

3.2.2. FAILURE MODE EFFECTS ANALYSIS/CRITICAL ITEMS LIST (FMEA/CIL)

3.2.2.1 USOS FAILURE ANALYSIS PROCEDURE

The USOS segment shall perform Failure Mode Effects Analysis/Critical Items List (FMEA/CIL) in accordance with SSP 30234 Revision D.

3.2.2.2 RSA FAILURE ANALYSIS PROCEDURE

The RS segment shall perform failure analysis in accordance with its own standards and methodology in order to identify critical items and evaluate failure effects on critical capabilities and interfaces with other segments of ISS.

3.2.2.3 FAILURE MODE SUMMARY REPORT (FMSR)

Each respective segment shall exchange the results of failure analysis required by paragraphs 3.2.2.1 and 3.2.2.2 in the FMSR. At a minimum the FMSR shall be prepared for equipment whose single failure manifests critical effects at the physical and functional interfaces to the associated segment. The analysis shall be used to summarize the cases of non-compliance with segment specification reliability requirements and to identify critical items. These analyses shall be documented in accordance with DID R-10-R01 and U-10-R05 for RSA and NASA, respectively.

3.2.2.4 CARGO FMEAs

RESERVED

3.2.3 CRITICALITY CATEGORIES

Criticality Categories are defined in DID R-10-R03, and SSP 30234.

3.2.4 CRITICAL ITEMS LIST (CIL)

The CIL determines the equipment for which the established requirements for reliability and safety are not fully met. Preparation of the CIL will utilize a structured process which will assure that all failure modes of each component of critical functions of the ISS are considered in the critical items analysis. Based on results of system analysis, the CIL includes justification for use of the Critical Element as part of the ISS. CIL preparation, maintenance, and control are aimed at assuring an efficient monitoring of critical elements of the ISS, and initiation of corrective action to reduce the criticality of these elements. The CIL shall be prepared for the RS in accordance with DID R-10-R03. USOS CIL will be provided to RSA in accordance with DID U-10-R05.

3.2.5 R&M PREDICTIONS REPORT

3.2.5.A R&M Predictions data will be used to document the results of the ISS R&M analyses. NASA and RSA shall exchange R&M Prediction data. The reliability data shall be collected for functions critical to ISS as a whole. The R&M Predictions Report will be used to status analysis results concerning segment reliability, segment maintainability allocations, provide data which will be used to develop an integrated preventive maintenance plan, and to provide data which can be used to perform integrated system level predictions of R&M characteristics. For RS, this report shall be developed in accordance with DID R-10-R02. For the USOS, this data will be reported in accordance with DID U-10-R06.

SSP 50146, Revision B

3.2.5.B

RESERVED

3.2.5.1 RELIABILITY

3.2.5.1.A LIMITED-LIFE DATA

RESERVED

3.2.5.1.B RELIABILITY PREDICTION DATA

Reliability prediction data for hardware shall be compiled to assess the reliability of the ISS.

3.2.5.2 MAINTAINABILITY

Maintainability data for RS and USOS flight elements shall be compiled in order to estimate the time and equipment required to maintain RS and USOS systems, both during assembly and at assembly complete.

3.2.6 DESIGN REVIEWS

RSA and NASA Reliability and maintainability activities shall include supporting RS and USOS internal design reviews and Space Station Program design and readiness reviews. Participation in reviews shall assure that reliability and maintainability requirements are adequately considered in such reviews.

3.2.7 REVIEW OF CHANGES

When changes are proposed for equipment design (hardware and software) or procedures, the changes shall include a review of the reliability and maintainability impact of the proposed changes.

3.2.8 FAILURE REPORTING SYSTEM

Reliability and maintainability activities shall support the failure reporting system (defined in paragraph 4.4).

3.2.9 VERIFICATION ASSURANCE

RSA and NASA Reliability and maintainability shall assure that an effective verification program is established and implemented for RS and USOS hardware and software. Reliability and maintainability activities shall include participation in such verification processes as development, certification, acceptance, checkout and maintainability verification.

4.0 QUALITY ASSURANCE

4.1 MANAGEMENT

4.1.1 NASA ROLES AND RESPONSIBILITIES

- a) NASA is responsible for establishing overall QA program requirements for ISS and to allocate and coordinate them with RSA for the RS.
- b) NASA is responsible to establish and coordinate with RSA the QA data on RS equipment necessary to support integrated assessments of equipment certification status and problem resolution of critical ISS capabilities and segment interfaces.
- c) NASA is responsible to provide RSA with problem resolution status for USOS/RS interfaces, and critical functions for the ISS in accordance with DID U-10-QA03.
- d) NASA is responsible to conduct QA activities for RSA property while it is under the control of NASA in accordance with the requirements agreed upon with RSA.

4.1.2 RSA ROLES AND RESPONSIBILITIES

- a) RSA is responsible to conduct QA activities for the RS in accordance with the requirements agreed upon with NASA.
- b) RSA is responsible to notify NASA of unresolved problems identified while conducting QA activities which may impact RS quality, on-orbit performance, and safety.
- c) RSA is responsible to provide NASA with problem resolution status for equipment which supports critical functions and at RS/USOS interfaces in accordance with DID R-10-QA01.
- d) RSA is responsible to conduct QA activities for NASA property while it is under the control of RSA in accordance with the requirements agreed upon with NASA.

4.1.3 RECIPROCITY

NASA and RSA shall establish and maintain a Quality Assurance function which possesses attributes, performs the functions, or supplies the data described herein.

4.2 QUALITY PROGRAM PLAN

RSA and NASA shall prepare, implement and maintain a Quality Program Plan, as a part of the S&MA Plan, which describes the compliance with requirements established by RSA and NASA. The QA plan shall describe how the quality requirements will be implemented, controlled and verified and shall be prepared and maintained in accordance with DID R-10-S01 and DID U-10-S08.

4.3 ACCEPTANCE DATA PACKAGE (ADP).

NASA and RSA shall compile/maintain an Acceptance Data Package for their respective flight equipment in accordance with native requirements. This data shall be retained for the operational life of the equipment.

4.4 FAILURE REPORTING AND CORRECTIVE ACTION

A closed-loop system shall be provided for reporting and correcting failures. All problems involving flight articles shall be included in this system. NASA and RSA shall conduct activities aimed at failure detection, analysis of causes, and development of corrective actions, including supporting information in accordance with the respective existing requirements. NASA and RSA shall exchange information about failures per the detailed requirements for failure reporting, analysis, and resolution in accordance with DID R-10-QA01 and U-10-QA03, Failure Reporting and Corrective Action (FRACA) System Requirements.

4.5 CONTROL OF NASA AND INTERNATIONAL PARTNER (IP) PROPERTY

When NASA property is under the control of RSA, the following requirements apply. The designated NASA representative, acting as NASA Quality Assurance Representative (QAR), may travel with the hardware to support the planned activities and may perform quality assurance functions defined herein. (NOTE: these requirements will apply to NASA, when RSA property is under the control of NASA.)

4.5.1 RSA RESPONSIBILITY

RSA Quality Assurance shall ensure that a documented system for controlling NASA property and associated documentation has been established and is maintained as follows:

4.5.1.1 Upon receipt, RSA Quality Assurance shall inspect NASA property to detect damage in transit and to verify that the article and its hardware data package are complete and as specified in the shipping documents. Photo and/or imagery documentation of the hardware shall be taken whenever necessary by the NASA QAR. Articles found to be serviceable shall be re-preserved and repackaged unless the articles are to be used immediately. Should there be evidence of damage in transit, the article shall be inspected to determine the extent of damage in transit and a report of the damage provided to the NASA QAR for disposition/concurrence. Receiving inspection results shall be recorded in the historical log sheet for the article. The article is transferred following positive conclusion of the inspection, documented by joint signatures of both sides on the incoming inspection protocol.

RSA shall coordinate with the NASA QAR in the event of any unscheduled removal of an article or material from its container.

4.5.1.2 When testing or operating NASA property the NASA QAR shall be notified and shall participate in the activity unless otherwise agreed. RSA shall make necessary arrangements to allow the participation by the NASA QAR in the testing facility. RSA shall perform tests in accordance with jointly approved procedures and record and approve any deviations to the test

procedures. Any such deviation must be coordinated and approved jointly with the NASA QAR. Each test operation shall be traceable to the individual responsible for its accomplishment. Flight articles undergoing test shall not be adjusted, modified, repaired, reworked, or replaced except as authorized by the NASA QAR. Test conduct and verification shall include the following:

- a) Prior to testing, RSA shall ensure that approved test procedures are available, that test equipment is calibrated and properly configured, that the facility is properly configured, that lower level test operations are complete, and that the configuration of the flight article is correct and ready for test.
- b) During test, RSA shall ensure that testing is performed in accordance with approved test procedures, that approved procedure deviations are properly recorded, that test data are accurately recorded, and that all non-conformances are documented. When a nonconformance is detected, RSA shall halt the test, secure the hardware and the test setup, and immediately notify the NASA QAR. The test shall be resumed only after a joint decision is made to proceed following analysis.
- c) Subsequent to testing, RSA shall ensure that:
 - The history log is updated;
 - Test results, data, and test summary (AKT) are complete and traceable to the flight article and are inserted into the data package;
 - Non-conformances are document;
 - Proper dispositions of articles have been made; and
 - Integrity control of flight articles is properly established and implemented.

4.5.1.3 RSA shall provide for the proper storage and control of NASA property. Controls shall include the following:

- Limited personnel access
- Controlled receipt and withdrawal
- Identification of article status
- Inventory list of articles in the area
- Periodic inspection of the area and verification of the inventory list
- Control for items that must be environmentally protected such as temperature, humidity, electrostatic, etc. (as required)

4.5.1.4 RSA shall provide for the protection, maintenance, calibration, periodic inspection, and controls necessary to ensure that quality of NASA property is maintained and deterioration does not occur during handling, storage, installation, shipment, testing, or operations.

4.5.1.5 RSA shall assure that contamination sensitive items are controlled in accordance with documented procedures to the levels specified in the applicable technical documents and are maintained to these cleanliness levels. These procedures shall cover hardware, equipment, personnel, and control of such inspection, test, and storage. Specific cleanliness levels to be

maintained for systems, subsystems, and major components shall be indicated on drawings, specification, or documents controlling the test of those items. RSA shall assure that clean room disciplines and procedures are properly implemented and monitored to assure continuing compliance with requirements.

4.5.1.6 NASA property shall not be diverted or loaned from its assigned purpose without the prior approval of the NASA QAR.

4.5.1.7 RSA shall provide the NASA QAR test data and records of inspection and tests performed for NASA provided hardware.

4.5.1.8 RSA shall ensure the NASA QAR access to facilities in the various functions defined herein.

4.5.1.9 RSA shall maintain the hardware data package (defined in 4.5.2) and return the package to NASA at the completion of hardware use. Hardware life, time, and cycle data shall be maintained by RSA for articles identified by the hardware data package as having characteristics of quality degradation or drift with age and/or use.

4.5.1.10 RSA shall assure that requirements for flight article inspection and testing in a temperature, humidity, electrostatic discharge (ESD), or contamination controlled environment are properly implemented and recorded. The NASA QAR shall verify proper entrance in the history records.

4.5.2 NASA RESPONSIBILITY

NASA shall provide selected hardware documentation to RSA. The hardware data package shall be used to update the hardware acceptance data package (ADP). The hardware data package shall include requirements pertaining to handling, storage, operations, preservation, packaging, and shipping operations. Specifically, the list shall include the following items, as required:

- Checklist of data in package (with references)
- List of hardware including fidelity
- Applicable pre-shipment test results
- Post-delivery checkout procedures
- Storage and handling requirements
- Special storage and handling instructions including calibration instructions
- Hazardous material and special requirements
- Pyrotechnic lot certification
- Pressure vessel data
- Ground equipment calibration and operation instructions
- Hardware history log sheet (to allow for RSA input of activities)
- Hardware life, time, and cycle recording requirements
- Additional information as jointly agreed in a separate document by both sides, such as:
 - Technical description including interface information with host modules

- On-orbit configuration (including physical installation with dimensions, electrical schematics, and mechanical connections, if required. For reference only)
- Jointly approved test configuration
- Jointly approved test procedures (stand alone and integrated)

4.5.3 UNSUITABLE NASA PROPERTY

NASA property found to be damaged, fails to meet its specifications, or otherwise unsuitable for its intended use shall be identified as nonconforming, segregated to the extent practicable, held for review, and analyzed to ascertain the probable cause of damage. The report shall be generated by the organization that discovered the nonconformance. The report shall include the nonconforming article name, part number/serial number, date, location, activity when nonconformance occurred, nature of nonconformance with description and data, current status of nonconforming article, conclusions, and recommendation for resolution. NASA shall perform an analysis and shall provide a disposition report that includes the nonconforming article name, part number/serial number, date and event where nonconformance was reported, nonconformance description, the probable cause, resolution information including method and status, and instructions for further activity. When the cause is determined to be in the RSA's operations or activities, action shall be taken to prevent recurrence and to resolve compensation if required. Disposition shall not be assigned to discrepant NASA property nor shall this property be reworked, repaired, modified, or replaced without the specific written authorization of NASA.

4.5.4 TEST PROCEDURES

Test procedures shall be jointly developed and approved by the hardware provider and test conductor prior to the hardware shipment. Approved test procedures shall be readily available to inspection and test personnel at the time of inspection and test.

Steps identified as Mandatory Inspection Point (MIP) shall be verified/witnessed by the NASA QAR. The NASA QAR shall be notified of any tests requiring MIPs prior to hardware shipment.

4.5.5 INSPECTION AND TEST RECORDS AND DATA

4.5.5.1 Records and data of all inspections and test performed shall be prepared and maintained by RSA on the hardware history log in sufficient detail to verify and evaluate the status of the articles and materials.

4.5.5.2 RSA shall ensure that hardware data packages are updated and maintained with the following:

- a) A summary of test and checkout operations and results with anomalies encountered.
- b) The completed test procedure and test data including strip charts, deviations, and other data applicable to evaluate test records.

- c) Documents have been properly identified as to inspection status by appropriate inspection stamps and the data package is complete.

4.5.6 PACKAGING, PACKING, MARKING, AND LABELING

RSA shall ensure that packaging and packing material, procedures, and instructions are used and that marking and labeling for packaging, storage, and shipping of articles and materials are performed in accordance with applicable specification. Special attention shall be given to critical, sensitive, dangerous, and high value articles. Reusable containers shall be inspected prior to each use. The NASA QAR shall be notified and shall participate in the activity, unless otherwise agreed.

RSA shall package the updated hardware data package with the flight article.

The article is authorized to be returned following joint signatures of both sides on the return inspection protocol.

5.0 SOFTWARE QUALITY ASSURANCE

SPA is a technical discipline which establishes requirements and criteria for the evaluation, assessment, assurance and enhancement of software safety, reliability, maintainability, and quality. It is to be accomplished to the extent specified for International Space Station software, including flight software, flight support software, software used for their design, development, verification, storage and maintenance, and software that controls or could affect flight hardware or software. SPA requirements apply to the software portions of a system. Assurance of a system shall include software affecting the system safety, reliability, maintainability or quality, and shall emphasize the use of preventative, as well as, corrective methods.

ISS Product Assurance requirements for hardware and operational procedures are addressed only as they relate to software. SSP 41000, System Specification for the International Space Station, and other paragraphs of this document "NASA/RSA Bilateral Safety and Mission Assurance Process Requirements," provide requirements for aspects of safety, reliability, maintainability and Quality Assurance that relate to the other system components, and are not repeated here.

This chapter establishes common SPA requirements for the ISS organizations including the International Partners, and contractors. The SPA requirements for the International Partners shall be equivalent to the requirements of this paragraph. Software, which is loaded in a class of memory that cannot be dynamically modified (i.e., firmware), is subject to these software assurance requirements to the extent practical.

5.1 MANAGEMENT

Software product assurance activities shall be planned, managed, and integrated in conjunction with other management, and technical functions to assure a complete, concise, and consistent approach to the development of program plans, and compliance with ISS program requirements.

5.1.1 ORGANIZATION

SPA shall be accomplished in accordance with the overall QA systems, accepted by NASA and RSA respectively. Personnel responsible for ensuring compliance with SPA requirements shall have the resources, responsibility, authority and organizational freedom to permit objective evaluations. SPA shall have the authority to initiate the corrective action process, and to verify corrective actions.

SPA management shall be structured to provide planning, management, and implementation of all SPA activities. While the accomplishment of all SPA tasks may not be the responsibility of a single organizational element, management of the SPA activities shall be coordinated with project management to ensure that all SPA requirements are assigned to the appropriate organization. Managers of all SPA functions shall have direct access to, and shall report status and issues to project management. Personnel evaluating a product or activity shall be personnel other than those who develop the product, perform the activity, or who are responsible for the product or activity. This does not preclude members of the development team from providing support to these evaluations.

5.1.2 SOFTWARE PRODUCT ASSURANCE PLANNING

SPA activities shall be planned and implemented throughout the software life-cycle. The procuring agency and the developer shall prepare and maintain SPA plans, which shall describe assurance activities during each life-cycle phase. SPA plans shall include an explanation of how tools, rules and procedures will be used to accomplish SPA activities. The preparation of SPA plans and other development plans shall be coordinated to assure an integrated approach. The ISS Quality Assurance IPT TEP, which includes Software Quality Assurance (SQA), and the RSA SPA Program Plan will be exchanged in accordance with SSP TBD, NASA/RSA Data Exchange Agreements, Lists and Schedules.

5.1.3 FORMAL AND INTERNAL REVIEWS

SPA shall participate in formal program, project, and software reviews to evaluate and report on compliance with ISS requirements. SPA shall have the option to participate in all reviews. Through participation in reviews, SPA shall assure that higher level requirements have been considered in decisions which affect detailed software requirements, software design, configuration controls, Computer Software Configuration Item (CSCI) testing, integration testing, acceptance, and readiness for flight. SPA shall evaluate software data presented to support management in assessing whether or not to proceed with the next program phase.

5.1.4 SUBTIER REQUIREMENTS

SPA shall assure that the requirements in this document are flowed down and adhered to by contractors, subcontractors, and other subtier providers of software. Direction and control shall be provided to assure that SPA requirements are properly implemented.

5.1.5 NONDEVELOPMENTAL SOFTWARE

SPA shall evaluate each item of nondevelopmental software to be incorporated into deliverable software to assure that:

5.1.5.1 Objective evidence exists, prior to its incorporation, that it performs its required functions

5.1.5.2 It is placed under contractor internal configuration management control prior to its incorporation into the developmental configuration

5.1.5.3 The data rights provisions are consistent with contractual and program requirements.

5.1.6 NASA OR INTERNATIONAL PARTNER FURNISHED EQUIPMENT (GFE/IGFE)

When software, related hardware, and documentation are furnished as GFE/IGFE, the accompanying ADP shall be reviewed. If it is determined that the GFE/IGFE does not provide functionality or performance consistent with its documented requirements or the GFE/IGFE is not consistent with the ADP, SPA shall ensure that the providing NASA Center or International Partner is promptly and formally notified.

5.1.7 PROGRESS REPORTING

SPA activities shall be reported through management meetings and status reports.

5.1.8 CONTROL BOARDS

SPA shall participate as members on configuration control boards, and other boards to assure changes are processed in accordance with approved plans and procedures, and to assure that safety, reliability, maintainability, and quality requirements are met.

5.1.9 OPERATIONS AND MAINTENANCE

SPA shall assure that a process is established for the planning and evaluation of software operation and sustaining engineering activities. The process shall ensure the retention of safety, reliability, maintainability, and quality attributes, and that changes will not adversely affect the required system failure tolerance.

5.1.10 TRAINING

SPA personnel shall have the training and qualifications commensurate with job responsibilities.

5.1.11 SOFTWARE TOOLS

SPA shall ensure software tools used in the development, verification and validation, integration, and test of deliverable software products (such as compilers and code checkers) are placed under configuration control prior to use, are maintained to an approved configuration, and operate consistent with approved configuration, and operate with approved changes following any modification or update.

5.1.12 SOFTWARE PRODUCT ASSURANCE RECORDS

SPA shall implement a system to identify, control and status SPA records generated as a result of the performance of SPA activities throughout the software life-cycle. SPA records shall be retained in a safe, accessible location for a period specified by the procuring agency.

5.2 SOFTWARE QUALITY ASSURANCE

Software development or acquisition shall be evaluated by SPA. SPA shall assure that: standards and procedural controls are established and implemented; audits, evaluations, and reviews are accomplished; procedures are followed; and all assurance activities are performed as scheduled.

5.2.1 AUDITS

SPA shall establish a plan and process to audit all activities conducted as part of the software life-cycle. Audits on activities such as development, documentation, testing, configuration management, nonconformance reporting, and corrective action activities shall be conducted on a

scheduled and unscheduled basis. SPA shall verify compliance with approved standards and procedures for these activities.

5.2.2 TOOLS, TECHNIQUES, AND METHODOLOGIES

SPA shall assure that software tools used in the development, verification and validation, integration and test of deliverable software products are evaluated, and that objective evidence exists that the tools perform their required functions. SPA shall participate in the identification and assessment of software development techniques and methodologies that facilitate the development of safe, reliable, maintainable, and quality software products.

5.2.3 SOFTWARE DOCUMENTATION

SPA shall ensure software documentation reviews are conducted throughout the software and acquisition life cycle. SPA shall review software documentation to ensure compliance with ISS documentation standards and applicable contractual requirements. SPA shall review software acquisition documentation to ensure software product assurance requirements are included. SPA shall ensure software development documentation is reviewed for conformance to applicable data requirements.

Software development documentation reviews shall be conducted to ensure the following:

5.2.3.1 Software requirements specifications contain software requirements that are complete, concise, consistent, accurate, realistic, unambiguous, verifiable, and traceable to higher level requirements.

5.2.3.2 Software design specifications have incorporated all applicable software requirements and that the software design conforms to applicable software standards and conventions.

5.2.3.3 Interface documents accurately specify hardware-to-software, software-to-software, and user-to-software interfaces.

5.2.3.4 Software test plans describe an acceptable test philosophy and approach, software test procedures verify applicable software requirements, and software test reports accurately reflect the conduct of each test.

SPA shall evaluate software documentation delivery processes and procedures to ensure delivery of complete, correct, and compliant software documentation and change information.

5.2.4 SOFTWARE CODE INSPECTION

SPA shall selectively participate in software code inspections and walkthroughs to ensure compliance with coding standards and design requirements. SPA shall verify the completion of all software code inspections and walkthroughs prior to integration and formal testing.

5.2.5 SOFTWARE TESTING

For all deliverable software preparatory to and during formal testing, SPA shall:

5.2.5.1 Review and approve test plans and procedures to verify conformance of test to requirements.

5.2.5.2 Verify documentation of the current configuration of the total test environment prior to any formal software test activities, to assure repeatability of test results, and to aid in the resolution and disposition of nonconformances.

5.2.5.3 Verify the software and test documentation configuration to assure approved and correct versions are used for testing, and to assure that only approved changes have been incorporated.

5.2.5.4 Selectively participate in tests and review test results to assure that test procedures have been performed, all test requirements have been met, and that actual test results are recorded.

5.2.5.5 Assure nonconformances are reported in accordance with paragraph 5.4.

5.2.5.6 Review test reports for completeness and accuracy.

5.3 CONFIGURATION MANAGEMENT

5.3.1 CONFIGURATION IDENTIFICATION, STATUS ACCOUNTING AND VERIFICATION

Software baselines established at the end of life-cycle phases, including configurations delivered for formal testing or for operational use, shall be evaluated or audited, as appropriate, to verify that the baselined configurations are correct, and at the proper revision level.

5.3.2 CONFIGURATION CHANGE CONTROL

The processing and implementation of change requests shall be evaluated to assure that the product conforms to baselined requirements and standards, only approved changes were implemented, and that the change has been incorporated in accordance with approved procedures. Change requests shall be reviewed for impact on software safety, reliability, maintainability, and quality.

5.3.3 SOFTWARE LIBRARIES

Software libraries shall be audited, and their processes evaluated to assure adherence to baselined configuration management processes, and to assure the proper storage and handling of software media and documentation. The audits and evaluations shall assure that different computer program versions are accurately identified and documented, only authorized modifications are

made, modifications are made in accordance with approved procedures, and software submitted for testing or operation is the required version.

5.3.4 DEVIATIONS AND WAIVERS

SPA shall evaluate all deviation and waiver requests to ISS baselined software requirements for potential impacts affecting safety, reliability, maintainability and quality, and recommend dispositions for management concurrence.

5.4 NONCONFORMANCE REPORTING AND CORRECTIVE ACTION

SPA shall ensure the establishment, implementation, and maintenance of a documented closed-loop system for nonconformance/problem reporting, and corrective action.

5.4.1 NONCONFORMANCE REPORTING

SPA shall assure a documented nonconformance reporting system exists throughout the software life-cycle. SPA shall ensure that the nonconformance reporting system includes provisions for recording, analysis, recurrence control, verification, and generation of summary and detailed reports on software which does not conform to specifications/requirements. Nonconformance reports shall be analyzed, including trend analyses, to categorize software errors, and to identify potential weaknesses in software life-cycle processes and products. Results of the analyses, and the actions taken shall be documented.

5.4.2 PROBLEM REPORTING AND CORRECTIVE ACTION

Detailed requirements for problem reporting, analysis, and resolution shall be in accordance with this agreement. SPA shall ensure that procedures are in place to evaluate the impact of a reported problem, the resources required for corrective action, and the impact of not taking corrective action. The procedures shall include requirements for retesting the software, and a process for incorporating the correction in new versions of the software. Software problem reporting and corrective action will be exchanged as part of the Failure Report in accordance with DID R10-QA01 and U10-QA03, NASA/RSA Data Exchange Agreements, Lists and Schedules.

5.5 RESERVED

5.6 SOFTWARE SAFETY

SPA shall assure analyses, of software, are performed as part of system safety analyses in accordance with the NASA/RSA Safety Review Process.

5.7 STANDARDS

SPA shall assure that software development standards are established and implemented. SPA shall assure that the software development standards meet ISS requirements, and support ISS objectives. SPA shall assure that the software development standards facilitate the development of safe, reliable, maintainable, and quality software products.

5.8 TRADE STUDIES

SPA shall assess the plan for trade studies, and their results to ensure that appropriate reliability and maintainability requirements are included.

5.9 INTEGRATION ASSURANCE

SPA shall ensure that a process exists to evaluate and integrate the software-to-hardware interfaces, software-to-software interfaces, and software-to-user interfaces of the system to meet the requirements defined in the interface documentation, and those contained in SSP 30459, Space Station Interface Development Process Requirements.

5.10 VERIFICATION AND VALIDATION

SPA shall ensure that verification and validation activities are performed for ISS software in accordance with SSP TBD, NASA/RSA Bilateral Integration and Verification Plan. SPA shall ensure that traceability analyses are performed from system level requirements to detailed requirements, to design, to code, to test, and back, to assure traceability of all requirements and the exclusion of unauthorized functions.

5.11 INDEPENDENT VERIFICATION AND VALIDATION (IV&V)

SPA shall ensure that IV&V is performed in accordance with applicable requirements (or for International Partners, equivalent activities which fulfill the intent of IV&V).

5.12 CERTIFICATION

SPA shall ensure that products requiring certification meet the following prerequisites:

5.12.1 Verification that the software products were developed and supported according to an approved process.

5.12.2 Verification that all software products are present, complete, current and controlled, and that no open nonconformances exist which are safety or mission critical.

5.12.3 Validation that the software products meet all of the applicable requirements including safety and reliability requirements.

5.12.4 Validation that the software products meet the requirements contained in SSP TBD BIVP.

5.12.5 Validation that the software products meet the requirements contained in SSP 50108 Certificate of Flight Readiness Process Document..

5.13 SECURITY AND PRIVACY ASSURANCE

SSP 50146, Revision B

SPA shall ensure that system security and privacy requirements for ISS have been implemented in accordance with approved procedures.

GLOSSARY

Cargo – All types of hardware stowed on a transport vehicle or module but not needed for its functionality, e.g. hardware transferred, stowed and operated on or removed from ISS. “Cargo” also relates to hardware items removed from service systems of the modules to be stowed, disposed of, or returned to the ground. Cargo items include scientific equipment, logistics, crew psychological support items, tools, spare instruments and assemblies, etc.

Catastrophic Hazard - Any condition which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the Orbiter, ISS, or major ground facility. Loss of ISS is to be limited to those conditions resulting from failures or damage to elements in the critical path of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.

Critical Function –Any capability required to achieve the Mission Objectives of the ISS, such as providing a micro-g working environment for the conduct of scientific inquiry.

Critical Hazard - Any condition which may cause a non-disabling personnel injury severe occupational illness; loss of a ISS 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 ISS 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.

Experiment – Any hardware and its contents, which is used on-board the ISS for carrying out research and technical experiments or production of materials; transported up to, located on-board (internal or external), or transported down from ISS but not part of the operational subsystems or structure of the ISS.

Mishap – Any unplanned occurrence, event, or anomaly. Mishaps that should be reported include those mishaps that may have significant program impact, may affect schedule, or cause death or permanent injury of crew or ground personnel.

Residual Risk – Risk that remains from a hazard after all mitigation and controls have been applied.

ADP Acceptance Data Package
 ATV Automated Transfer Vehicle
 CIL Critical Items List
 DID Data Item Description
 FMEA Failure Modes and Effects Analysis
 FRR Flight Readiness Review
 GFE Government-Furnished Equipment

SSP 50146, Revision B

GSE Ground Support Equipment
IP International Partner
NASA National Aeronautics and Space Administration
NDE Nondestructive Evaluation
NHB NASA Handbook
NSTS National Space Transportation System
ORU Orbital Replaceable Unit
PRACA Problem Reporting and Corrective Action
RS Russian Segment
RSA Russian Space Agency
SRP Safety Review Panel
SSCB Space Station Control Board
STD Standard
STS Space Transportation System
TBD To Be Determined
USOS United States On-orbit Segment

SSP 50146, Revision B

ATTACHMENT A

GROUND SAFETY REQUIREMENTS FOR THE SCIENCE POWER PLATFORM

ATTACHMENT A

Table of Contents

1.0	INTRODUCTION	4
1.1	PURPOSE	4
1.2	SCOPE	4
1.3	APPLICABILITY	4
1.4	RESPONSIBILITY	4
1.4.1	DELEGATION	5
1.5	CHANGES	Deleted
2.0	PHASE SAFETY REVIEWS	6
3.0	DOCUMENTATION	7
3.1	GENERAL	7
3.2	PHASE SAFETY REVIEW DOCUMENTATION	7
3.3	LAUNCH SITE DOCUMENTATION	8
3.3.1	PAYLOAD ORGANIZATION LAUNCH SITE SAFETY PLAN	8
3.3.2	TECHNICAL OPERATING PROCEDURES (TOPs)	8
3.3.3	PAYLOAD SAFETY NONCOMPLIANCE REPORTS	8
3.4	DOCUMENTATION CHANGES	9
4.0	SAFETY REQUIREMENTS	10
4.1	OPERATIONAL CONSIDERATIONS	10
4.1.1	FAILURE TOLERANCE	Deleted
4.1.2	PERSONNEL POLICIES	10
4.1.3	HAZARDOUS OPERATIONS	10
4.1.4	SAFETY INSPECTION	11
4.1.5	SAFETY EQUIPMENT	12
4.1.6	TOOLS	12
	4.1.7 PHOTOGRAPHY	12
4.2	PERSONNEL SAFETY	12
4.2.1	HUMAN FACTORS	12
4.3	PAYLOADS AND GROUND SUPPORT EQUIPMENT (GSE)	13
4.3.1	BIOMEDICAL SUBSYSTEMS	Deleted
4.3.2	ELECTRICAL	13
4.3.3	PRESSURE/VACUUM SYSTEMS	15
4.3.4	RADIATION	20
4.3.5	ORDNANCE	Deleted
4.3.6	MECHANICAL, ELECTROMECHANICAL DEVICES	23
4.3.7	AMMONIA	23
4.3.8	CRYOGENICS	24
4.3.9	GSE MATERIALS	24
4.3.10	INDUSTRIAL HYGIENE	25
4.3.11	OXYGEN	Deleted
4.4	ENVIRONMENTAL	26
4.4.1	METEOROLOGICAL REQUIREMENTS	Deleted
4.4.2	HAZARDOUS ATMOSPHERE	26
4.4.3	HUMIDITY	Deleted
4.4.4	TOXIC MATERIALS	27

SSP 50146, Revision B

4.5	HANDLING AND TRANSPORTS	27
4.5.1	HOISTING AND HANDLING	27
4.5.2	TRANSPORTERS	Deleted
5.0	MISHAP INVESTIGATION AND REPORTING	33
5.1	NASA MISHAP INVESTIGATION CONTROL	33
5.2	USAF MISHAP INVESTIGATION CONTROL	Deleted
5.3	MISHAP REPORTING	33
5.3.1	MISHAP CONTACTS	33
5.3.2	PAYLOAD ORGANIZATION INVOLVEMENT	33
5.3.3	PAYLOAD ORGANIZATION RESPONSIBILITIES	33
5.3.4	INVESTIGATION BOARDS	Deleted
5.3.5	MISHAP SCENE	34
APPENDIX A -	ACRONYMS, ABBREVIATIONS, AND GLOSSARY OF TERMS	35
APPENDIX B -	COMPLIANCE AND REFERENCE DOCUMENTS	Deleted
APPENDIX C -	GUIDELINES FOR THE PREPARATION OF TECHNICAL OPERATING PROCEDURES (TOP's)	42
APPENDIX D -	ORDNANCE STORAGE AND HANDLING DATA REQUIREMENTS.	Deleted
APPENDIX E -	PAYLOAD RELATED EMERGENCY PROCEDURES DOCUMENTS AND FACILITY SAFETY PLANS	48
<u>Tables</u>		
TABLE 4-1	SLING REQUIREMENTS	30

1.0 INTRODUCTION1.1 PURPOSE

The purpose of this document is to present the ground safety policy and the criteria applicable to Russian Flight hardware (referred to as “payload”) and ground support equipment (GSE) design. These criteria apply to ground processing at KSC from hardware arrival to Space Shuttle liftoff and during postlanding activities. By achieving compliance to this policy and criteria, RSC-E will be able to certify to the Launch Site Safety Office that their payload and GSE are safe.

1.2 SCOPE

This document establishes the minimum NASA ground processing safety policy, criteria, and requirements for payload and their associated GSE.

1.3 APPLICABILITY

This document applies to-

- A. Delete
- B. Contractors in direct support of RSC-E
- C. Other organizations or agencies providing direct personnel and equipment interface to payload or payload GSE support
- D. Any of the above organizations that are required to support payload postlanding operations at any landing site.

1.4 RESPONSIBILITIES

The KSC Director has been assigned overall authority for safety for all Space Shuttle payload activities conducted at KSC.

- A. The officials of the Launch Site Safety Office (LSSO) responsible for implementing the safety policy and criteria for the Space Shuttle Program payload activities are identified below:
 - 1) The KSC, Director of Safety and Mission Assurance is responsible for implementing the safety policy and criteria for Space Shuttle payload activities.
 - 2) Delete
- B. The Chiefs, Biomedical and Bioenvironmental Engineering Offices, are responsible for certain activities as identified in this document. Office contacts are identified below:
 - 1) For KSC, Biomedical Operations & Research Office (JJ).
 - 2) Delete

1.4.1 Delegation

SSP 50146, Revision B

The Launch Site Safety Representative (LSSR) is the designated representative of the LSSO and has been delegated the following authorities:

- A. Monitors LSSO selected operations and has safety approval authority for procedural deviations.
- B. Gives concurrence to start these selected operations.
- C. May halt any operation deemed unsafe.

1.5 CHANGES -Delete

SSP 50146, Revision B

2.0 PHASE SAFETY REVIEWS

RSC-E is responsible for the safety of their own systems and personnel. To implement this safety effort, the NASA program of phase safety reviews are implemented by NSTS 13830, "Implementation Procedure for NSTS Payloads System Safety Requirements". NSTS 13830 permits the combining of the phased safety reviews based upon the complexity, technical maturity, and hazard potential of the payload. The KSC Ground Safety Review Panel Chairman, the International Space Station Program Office (code OE), and the Payload Organization (RSC-E) must agree to any combination of reviews.

SSP 50146, Revision B

3.0 DOCUMENTATION

3.1 GENERAL

Identification, submittal, and approval of the documentation required by NSTS 13830 for NASA and NASA-sponsored payloads is accomplished by the phase safety review process.

3.2 PHASE SAFETY REVIEW DOCUMENTATION

The KSC Ground Safety Review Panel Chairman, the ISS Program Office, and RSC-E have agreed to the following modification to the SSP 30599 implementation process.

RSC-E will evaluate its GSE and operations and determine compliance with the ground safety requirements of this document. Verification of compliance can, in part, be performed by using the matrices provided to RSC-E by KSC Safety. Initially, five hazardous areas will be addressed in the RSC-E ground safety data package for the Science Power Platform. These are 1) Lifting & Handling, 2) Pressurized Systems (greater than 30 psig), 3) Electrical (power supply for non-commercial equipment), 4) Hazardous Materials (toxic, corrosive chemicals), and 5) Radiation. Hazard Reports will be produced when compliance to requirements can not be verified. If a Hazard Report is required, the format for the Hazard Report will be in accordance with SSP 50146.

There is to be three formal submittals of the RSC-E developed ground safety data package. These three submittals will support the three formal Ground Safety Review Panel meetings.

The ground safety data package may reference other RSC-E documents as long as the referenced documents are provided to KSC Safety.

Based upon the above modifications, RSC-E shall provide the Safety Review panel the following data to support the two formal meetings:

- A. Block diagrams, schematics, and descriptions of safety-critical subsystems. This includes tables of design and operating parameters for such items as lifting equipment, pressure systems, and batteries.
- B. Launch site processing plan including timelines for handling, storage, assembly, servicing, and checkout operations.
- C. List of Technical Operating Procedures (TOP's), a synopsis of each procedure, and their preliminary classifications; i.e., hazardous or nonhazardous.
- D. Documentation certifying compliance with ionizing and nonionizing radiation control requirements.
- E. Hazard reports addressing both design and operations, if compliance can not be verified.
- F. Failure/accident summary reports.
- G. Copies of all noncompliance reports.
- H. Delete.
- I. A list of all hazardous materials and physical agents. Material Safety Data Sheets (MSDS's) (CFR 1910.1200) or equivalent shall be provided to the LSSO for all material and agents brought to the KSC by the payload organization.

- J. A list of all plastic films, quantity, and location of use.
- K. List of the payload T-O Umbilical functions.
- L. Critical software commands must be identified and managed. These critical software commands include commands which, if executed or executed out of sequence, would create a hazardous condition or would remove a safety inhibit.

3.3 LAUNCH SITE DOCUMENTATION

3.3.1 Payload Organization Launch Site Safety Plan

RSC-E shall provide a Launch Site Safety Plan which demonstrates the means by which RSC-E manages and interfaces safety within its organization and how it applies the launch site safety requirements. All plans shall be tailored to the complexity of the payload element and be provided to the LSSO for review and approval at least 30 days prior to first hardware delivery to the launch site.

3.3.2 Technical Operating Procedures (TOP's)

In order to be accomplished in a safe and orderly manner, payload ground operations must be conducted using detailed step-by-step instructions in TOP's. All TOP's designated hazardous by the LSSO or by RSC-E shall be written in English and are required to be approved by the LSSO and published and "on the shelf" 10 days prior to use (5 days prior to use for revisions). Draft or preliminary procedures should be submitted to the LSSO when available. Where procedures are used to control hazards identified in the hazard reports, a listing of those procedures and the applicable step numbers which control the hazard shall be identified in the Phase III data package as applicable. Appendix C contains guidelines for the preparation of TOPs.

3.3.3 Payload Safety Noncompliance Reports

RSC-E must obtain an approved variance (waiver) for each case of inability to comply with a specific safety requirement.

3.3.3.1 Waivers - Each waiver request shall be limited to a specific subsystem or component in a specific application. The following information is required for the waiver request:

- A. The payload name and the model of the payload or support equipment as applicable.
- B. The specific component and the subsystem in which the component functions shall be identified.
- C. The specific requirement (one per waiver) and document and paragraph number against which the waiver is being sought.
- D. The hazard created by noncompliance to this requirement and a cross-reference to the related hazard report. (If applicable).
- E. Reason for noncompliance to this requirement.
- F. Give rationale for acceptance of this waiver, including any required support data and drawings, and list possible methods and techniques used in mitigating the hazards.
- G. This waiver request must be signed by the program manager of the payload organization.

SSP 50146, Revision B

3.4 DOCUMENTATION CHANGES

Changes or modifications which affect any approved phase safety review or launch site documentation must be provided to the LSSO for review and reapproval.

SSP 50146, Revision B

4.0 SAFETY REQUIREMENTS

Payload organizations shall comply with the following policies, practices, and regulations.

4.1 OPERATIONAL CONSIDERATIONS

4.1.1 Failure Tolerance - Delete

4.1.2 Personnel Policies

RSC-E shall provide a description of their Training/Certification Program to the LSSO as part of the payload organization Launch Site Safety Plan. This program shall specify the personnel training required and the certification procedures employed to establish acceptable skill levels for all personnel involved in the ground processing of SSP payloads and GSE. Ground processing shall be performed only by persons certified in the discipline required for that process.

4.1.2.1 Training - Safety and health inputs to training programs shall be tailored to the task categories involved and included in lesson plans and examinations. Safety training of operating personnel is the responsibility of the RSC-E. RSC-E shall meet the applicable facility and operating site requirements.

4.1.2.2 Certification - RSC-E shall provide a list to the LSSO prior to commencement of hazardous operations of all personnel authorized to participate in hazardous operations certifying each individual's training and qualification by system to perform a specific hazardous operation.

4.1.2.3 Physical Examination - Personnel performing selected hazardous operations are required to have up-to-date physical examinations which meet the requirements of the cognizant medical office. The requirements for physicals for selected hazardous operations are as follows:

- A. Lifting Operations. Personnel operating overhead cranes require a crane operator (Category 1 or 2) physical examination.
- B. Noise. Personnel that work in or around flight or ground support equipment that produce a continual noise level above 85 dB(A) require a hearing conservation physical examination.
- C. Heavy Equipment. Personnel that operate mobile equipment that weighs more than 2000 pounds require a heavy equipment operator physical examination. Examples of this equipment includes forklifts and man lifts.
- D. Working at Heights. Personnel working at heights more than four feet above the ground will wear fall protection equipment and will require a high crew physical examination.
- E. Ammonia servicing. Personnel that work within 10 feet of ammonia servicing equipment while the equipment is in operation or during open ammonia system operation require a respirator physical examination. Examples of open ammonia system operation are component replacement, during connections/disconnections and tasks to repair leaks such as tightening connections.

4.1.2.4 Safety Enforcement - Delete

4.1.3 Hazardous Operations

- A. A ground processing activity is classified as hazardous based on the following considerations:
 - 1) Energy is involved and loss of control could result in injury to personnel or damage to equipment.

- 2) A significant change from ambient condition will occur; e.g., increase or decrease of oxygen content, pressure, or temperature.
- 3) Presence of hazardous materials or physical agents which presents potential exposure to personnel.
- B. TOPs are required for any activity, either by itself or in combination with another, which can result in injury to personnel or damage to property involving, but not limited to, the following:
 - 1) Delete.
 - 2) Delete.
 - 3) Delete.
 - 4) Cryogenics.
 - 5) Lifting/Handling.
 - 6) Radiation.
 - 7) Toxics/Combustibles/Corrosives.
 - 8) Pressure.
 - 9) Electrical.
- C. All hazardous or LSSO designated procedures require notification of the LSSR at least 24 hours prior to their performance.
- D. Concurrent hazardous operations within the same hazard control area are prohibited.
- E. Concurrent operations within a hazard control area require LSSR or LSSO approval.

4.1.4 Safety Inspection

LSSR and RSC-E shall perform joint systematic safety inspections of the facility, working environment, related GSE, and any work in progress which could cause accidental injury to personnel or damage to hardware. These safety inspections shall be performed on payload processing facilities at the following minimum times:

- A. Prior to payload/GSE installation in the facility.
- B. Immediately after installation of payload/GSE.
- C. Immediately before the start of LSSO selected hazardous operations.
- D. After any facility or equipment modification which may affect hazard potential.

4.1.5 Safety Equipment

RSC-E shall ensure that personnel protection is provided when engineering controls alone are not adequate to provide sufficient employee protection. All personal protective equipment shall be approved by the LSSO and Biomedical Office.

4.1.6 Tools

4.1.6.1 Temporary Restraints - Temporary restraints, such as tethers, shall be used for individual tools to prevent misplacement or loss in critical areas when working above personnel or sensitive equipment.

4.1.6.2 Control of Tools - All tools and related equipment used in the proximity of flight articles shall be controlled to minimize the potential for foreign object damage.

4.1.7 Photography

Camera permits are required for all photographic operations in controlled areas. The LSSO requires that the use of photographic lighting equipment (e.g., flashbulbs, strobe lights, and photofloods) be restricted within 100 feet of the Orbiter/payload whenever they are loaded with any propellant (not ammonia), within 100 feet of a propellant storage tank, and within 10 feet of exposed solid propellants. These control areas do not apply to the SPP while located in the Space Station Processing Facility. Photo equipment used above a payload must be tethered and the light sources shielded to prevent debris from falling onto the payload. The payload organization shall obtain LSSO approval to use photographic equipment in these and other hazardous atmosphere locations. Refer to paragraph 4.4.2.3 for the control area for ammonia servicing.

4.2 PERSONNEL SAFETY

4.2.1 Human Factors

RSC-E shall consider human factors in the design of GSE and the payload.

4.2.1.1 Human Error - All equipment controls shall be labeled.

4.2.1.2 Noise - Delete

4.2.1.3 Hazardous Materials - RSC-E shall assure through design/procedural controls that payload/ground processing GSE and operations will not expose KSC or RSC-E personnel to hazardous materials in excess of the limits specified by the cognizant Biomedical Office.

4.2.1.4 Physical -

- A. Accidental contact with sharp surfaces or protrusions shall be prevented by the use of ductile materials, energy absorbing devices, shields, rounded corners, and flush-mounted features. Sharp surfaces or protrusions include edges, crevices, points, burrs, wire ends, screw heads, corners, brackets, rivets, braided cable, cable swages, cable strands, clamps, pins, latches, lap joints, bolt ends, lock nuts, etc., which if contacted, could injure operating personnel.
- B. Hazards shall not be created by the inaccessibility of flight or ground hardware. Physical access for safety critical operations or maintenance functions shall be provided. Protrusions which create a hazard such as hoses, wave guides, cables, brackets, etc., which cannot be eliminated by design, shall be made to be removable during service or maintenance functions.
- C. Moving parts such as fans, belt drives, turbine wheels, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices.
- D. Delete

SSP 50146, Revision B

- E. Delete
- F. All GSE designs should include a center-of-gravity analysis to ensure that the GSE/flight hardware does not tip, fall, slide, or allow for any type of sudden load shift.

4.2.1.5 Temperature - RSC-E shall protect personnel from equipment which can generate high or low temperatures greater than 45°C (113°F) or less than 0°C (32°F). This equipment shall be shielded, insulated, isolated, and/or oriented away from personnel and labeled to warn them of the danger.

4.2.1.6 Radiation - The payload organization shall advise and protect personnel from equipment which radiates ionizing or non-ionizing radiation.

4.3 PAYLOADS AND GROUND SUPPORT EQUIPMENT (GSE)

4.3.1 Biomedical Subsystems - Delete

4.3.2 Electrical

All electrical equipment shall meet the requirements of this section to preclude hazardous conditions.

4.3.2.1 Electrical Requirements -

- A. Electrical connectors shall be designed to make it physically impossible to inadvertently reverse a connection or mate the wrong connectors if a hazardous condition can be created. These connectors for energized circuits must also be of "scoop-proof" design so that a partial inadvertent mismatch will not provide pin-to-pin contact.
- B. Electrical equipment shall not cause ignition of adjacent materials. The requirements for explosion/ hazardproofing at the launch site are identified in Paragraphs 4.4.2.3 and 4.4.2.4.
- C. Malfunction of the payload or GSE circuitry shall not induce overload into the Orbiter, GSE, or facility electrical systems.
- D. Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.
- E. Construction of the payload and electrical GSE shall assure that all conductive external parts and surfaces are at ground potential at all times.
- F. Cables extending across work areas shall be protected against damage from personnel activity or equipment use.
- G. Switches/controls which can create hazardous conditions if inadvertently operated shall be guarded, shielded, or otherwise protected against inadvertent switching.
- H. Electrical fuse and switch boxes shall be labeled on the outside or inside cover to show the voltage present, rated fuse capacity, and equipment that the circuit controls.
- I. Non-bypassable interlocks shall be used to prevent possible shock whenever a voltage in excess of 500 volts is exposed upon opening an access door, cover, or plate.
- J. All GSE shall meet the requirements of the Russian Industry Standards
- K. Dead-end wires shall be completely insulated.

- L. Three-phase power sequencing must be verified in each KSC processing facility prior to connection.
- M. Battery charging/conditioning shall be accomplished in the battery laboratories unless approval is granted from the LSSO to accomplish the charging elsewhere. Battery charging equipment shall be continuously monitored by personnel. Charging/conditioning performed in hazardous locations shall comply with paragraphs 4.4.2.4.1 and 4.4.2.4.2. The payload organization should consider incorporating voltage and current limiters, fuses, diodes, and temperature and pressure monitors in the charging/conditioning electrical GSE.
- N. The payload should be assessed to determine if the loss of power during any phase of ground processing is a hazard to personnel or equipment. If so, an alternate or backup power source may be required.

4.3.2.2 Grounding, Bonding, and Shielding -

- A. The design, construction, and installation of equipment shall be such that all external parts, surfaces, and shields are at ground potential at all times.
- B. Grounding and bonding schemes shall ensure proper interfacing between equipment and facility.
- C. Power cords on GSE shall provide a non-current carrying ground conductor unless the unit is double insulated.
- D. Grounding/bonding connections of GSE shall be designed to minimize the possibility of inadvertent disconnection.
 - 1) Solder shall not be used for external connections.
 - 2) Threaded fasteners shall use lock washers.
- E. GSE external bonding straps and jumpers shall be capable of carrying the maximum expected fault current.
- F. Delete.

4.3.2.3 Electrical Maintenance Operations - Maintenance operations on energized electrical circuits are normally prohibited. Maintenance operations shall be performed in accordance with accepted industrial practice. In addition, the following shall be included:

- A. Any accessible capacitor circuitry which presents a hazard to personnel shall be discharged prior to performing maintenance.
- B. Protective equipment such as nonconducting fuse pullers, rubber gloves, nonconductive matting, etc., shall be used when working on energized circuits which could cause personal injury.
- C. Procedures for tagging and lockout of control switches and circuit breakers shall be provided.
- D. All grounds shall be verified to be intact.
- E. Worn, abraded, or defective insulating material shall be repaired or replaced.

- F. Only fuses of proper voltage and current ratings shall be used in circuits. No other material will be used in place of a fuse.

4.3.2.4 Electrical Control of Hazardous Functions - Where electrical GSE is used to control a potentially hazardous function, it shall be designed to be failure tolerant. Acceptable failure tolerance will be determined by the LSSO during the safety review process. Where feasible, failure tolerance shall be implemented through design control rather than procedural control. Design control can be implemented by eliminating the potential hazard (e.g., the current-limiting features in EED bridgewire checkers), providing a fail safe design (e.g., current-limiting fuses) or requiring multiple component failures and/or operator actions prior to a hazardous event occurring.

4.3.2.5 Energized Electrical Equipment -

- A. Energized equipment will be manned or connected to the manned facility emergency power shut-off system. The electrical equipment will be powered down during non-working hours. All electrical equipment located outside of a hazardous processing area will be inhibited from supplying power to electrical equipment located within the hazardous processing area during non-working hours.
- B. Electrical equipment that must remain energized for hazardous operations (i.e., maintaining spacecraft thruster solenoid valves in an opened or closed state) shall be equipped with an uninterrupted power source such as a battery backup.

4.3.2.6 Battery Charging - Battery charging operations should occur in an approved charging facility. Battery charging requirements for batteries that cannot be removed from flight hardware will be assessed on a case-by-case basis.

4.3.3 Pressure/Vacuum Systems

Pressurized systems contain fluids above atmospheric pressure. Vacuum systems contain fluids below atmospheric pressure. Pressure system elements include tanks, accumulators, lines (e.g., piping, tubes, and hoses), fittings, gauges, filters, valves, regulators, and other components.

4.3.3.1 Pressure System Requirements -

4.3.3.1.1 Delete

4.3.3.1.2 The following requirements shall be met by both flight and ground pressure systems:

- A. To preclude personnel injury, provisions shall be made for accomplishing remotely controlled pressurization of the flight pressure system. Exception to this requirement is when the conditions of Paragraph 4.3.3.2.1 do not apply or when the payload operator provides a certification statement of system pressure testing to the LSSO in accordance with Paragraph 4.3.3.2.2. Normally, remote pressurization of GSE is not required.
- B. Regulator failure shall not create a hazard to personnel or equipment during ground processing.
- C. All items, including gauges, which come in contact with the service fluid shall be of compatible material.
- D. Delete

4.3.3.1.3 GSE containing pressure systems shall meet the following requirements:

- A. Delete

- B. GSE pressure systems hardware other than pressure vessels shall be marked as follows:
- 1) Pressure system lines (where the function of the line is not immediately apparent) shall be labeled with the maximum operating pressure (MOP), fluid content, and direction of flow.
 - 2) Delete
 - 3) Other system components shall be labeled with their manufacturer's name and part number, serial number (if applicable), pressure rating, and direction of flow.
- C. Pressure systems components shall have a design burst pressure (D.B.) of at least 4 times the MOP of the system. Components shall be pressure tested at 1.5 times MOP unless otherwise approved by the LSSO.
- D. Regulators shall be selected so that their working pressure falls within the center 50% of their total pressure range if susceptible to inaccuracies or creep.
- E. Flight and GSE components downstream of a GSE regulator shall be designed to safely operate under full upstream pressure. Open-ended purge systems may be protected by flow restriction orifice devices.
- F. If the requirements of Paragraph E (above) cannot be met, relief devices shall be provided as follows:
- 1) Downstream of last GSE regulator prior to flight hardware interface.
 - 2) GSE pressure vessels.
 - 3) Downstream of regulators where upstream pressure exceeds downstream design operating pressure.
 - 4) Container purge systems using metal tubing or flex hose.
 - 5) Container purge systems using plastic tubing when the failure of the tube provides sufficient margin of safety to the downstream equipment.
 - 6) All relief devices shall be relief valves when pressure exceeds 149 psig.
- G. Set pressure: Pressure relief valves shall be set to relieve at a pressure not to exceed the MAWP of the vessel or the design pressure of the system involved (including flight systems), and the set limits shall be specified in the Operation and Maintenance Requirements Document (OMRSD) or other operating and maintenance documents. The setting of relief valves shall be set to open at a pressure not to exceed 110% of the system MOP.
- H. For piping/tubing systems, the required relieving capacity shall be equal to or greater than the maximum flow capability of the upstream regulator or pressure source and shall prevent systems from exceeding their MAWP.
- I. Relief devices shall be located so that other components such as shut-off valves cannot render them inoperative. Relief devices and their associated discharge plumbing shall be adequately supported such that their discharge impulse will not cause structural failure.
- J. Pressure relief for toxic liquids and/or vapors shall be designed and located so that gases and liquids or vapors will not enter any inhabited areas. Pressure relief for inert gases shall not be

discharged into a confined, occupied area where oxygen content could be lowered below acceptable limits. Pressure reliefs for high pressure gases and liquids shall be located such that the discharge will not endanger personnel.

- K. Pressure systems shall be equipped with gauges as follows:
- 1) Downstream of each regulator.
 - 2) On any storage system.
 - 3) On any section of the system where pressure trapped by isolation valves creates a hazard.
- L. All pressure gauges shall comply with the following requirements:
- 1) Gauges shall be selected so that the operating pressure is not more than 75% of the highest graduation.
 - 2) Pressure gauges shall be of one piece, solid front construction and shall have an optically clear shatterproof window. Gauges should be designed for bolted flush front panel mounting.
 - 3) Gauges shall have blowout backs to allow unrestricted venting in the event the gauge sensing element ruptures.
 - 4) All items which come in contact with the service fluid shall be constructed of compatible material.
 - 5) A due date calibration sticker shall be affixed to gauges used for safety-critical monitoring.
 - 6) Gauges shall be equipped with a bourdon-tube bleeder or equivalent device to facilitate cleaning.
- M. All GSE using flex hoses with pressures above 150 psig shall be designed to provide attachments for flex hose restraining devices.
- N. Isolation valves shall be designed to permit flow or isolation in both directions at the valve's MAWP.
- O. Pressure systems shall be designed so that pressure cannot be trapped in any part of the system without bleed capability.
- P. Manually operated valves and regulators shall be selected so that over-torquing the valve stem or regulator adjustment cannot damage soft seats to the extent that seat failure occurs. Designs using uncontained seats are unacceptable.
- Q. Pressure system elements which are not intended to be reversible shall be designed or marked such that they will not be connected in a reverse mode.
- R. Lines, relief devices, and other pressure system elements shall be routed and/or located to provide for the protection of other systems and personnel.
- S. Control stations shall have adequate instrumentation to allow personnel to monitor pressure levels and confirm that initiated actions have occurred.

SSP 50146, Revision B

- T. Control stations shall be designed so that the operator does not have to leave the station to monitor hazard levels.
- U. Systems shall have shut-off valves located as close to the supply vessel as practicable.
- V. Check valves shall be provided where backflow of fluids would create a hazard.

4.3.3.1.4 Delete

4.3.3.1.5 Flexible Hoses - Flexible hoses consist of an inner liner tube of teflon or other material (compatible with the service fluid) reinforced by layers of wire and/or fabric braid or wrap. Use of flex hoses should be minimized. Requirements for flexible hoses are as follows:

- A. Delete
- B. Flexible hoses shall be installed so that they do not carry any external mechanical load and are not subjected to tension, torsion, or overheating.
- C. All flexible hoses shall have a design burst pressure equal to or greater than 4 times the MAWP.
- D. All flexible hoses pressurized to 150.0 psig (10.34 bars) or greater shall be contained or restrained. Hose restraint shall be accomplished using a chain or cable securely anchored to a substantial object and to the hose assembly at the following points: 1) Hose end connector; 2) each union or hose splice; and 3) intervals not to exceed 6 feet (1.83 meters). Hose restraint devices and attachment methods shall be approved by the LSSO.
- E. The payload organization shall establish criteria and obtain LSSO approval for periods of inspection and retest. Time in service, type of service, and pressure are factors for determining need of pressure test. LSSO approval shall be obtained prior to performing pressure testing at the launch site.
- F. All flexible hoses shall be inspected prior to use. Flexible hoses which show signs of physical damage shall be replaced.
- G. Flexible hose assemblies shall be pressure tested to 1.5 times their MAWP.
- H. GSE flexible hoses shall be identified and marked. Each flexible hose assembly shall have a metal tag(s) attached which bears the following information:
 - 1) Date of proof test (month and year).
 - 2) Dedicated fluid service; e.g., fuels, oxidizers, hydraulics.
 - 3) MAWP.
 - 4) Identifier (manufacturer/part number).
- I. After each pressure test recertification, the old tag(s) will be removed and new ones attached.

4.3.3.1.6 GSE Hydraulic Systems - Delete

4.3.3.2 Pressure System Operations - Pressure system operations shall comply with the following:

SSP 50146, Revision B

4.3.3.2.1 The following flight and ground support system pressurization operations shall be accomplished remotely (e.g., locate control station behind a blast shield) unless otherwise approved by the LSSO:

- A. The first time a flight system is pressurized above 25% of the design burst at the launch site. This pressure is designated the "initial pressurization level."
- B. Any flight system pressurization above the initial pressurization level; this latter pressurization becomes the new initial pressurization level.
- C. Any pressurization above MOP/MAWP.
- D. Any pressurization of a system that has suspect integrity.

4.3.3.2.2 Remote pressurization may not be required if RSC-E provides documentation which certifies the following:

- A. The assembled system has been pressure tested at a pressure which is at least 1.5 times the system MOP unless otherwise approved by the LSSO.
- B. The assembled system has been functionally leak tested at a pressure equal to or greater than MOP. The system log book shall track system handling/movement in addition to pressurizations, maintenance, etc.
- C. System configuration has not been modified or repaired subsequent to the above testing. Unwelded relief or sensing devices may be replaced after system pressure testing but not after system leak testing, in accordance with Paragraph 4.4.3.2.9.
- D. A procedure has been written which requires inspection of the system upon arrival at the launch site for damage sustained during transportation and handling. The procedure shall also require a check of the pressure system log book to verify that activity after the pressure test and leak test did not affect the integrity of the system. Provide procedure name and number, step numbers and test which require the inspection, and any additional inspection criteria.

4.3.3.2.3 Personnel will be allowed in the immediate proximity of pressure systems only when pressure does not exceed the system MOP.

4.3.3.2.4 System integrity shall not be broken on pressurized systems without first depressurizing to 10 psig or less. Depressurization shall be accomplished only using components designed for the purpose. Backing off of line fittings, when pressures exceed 10 psig, to depressurize is permitted if the trapped volume does not exceed 1.5 cubic inches. Tightening of line fittings under pressure is also prohibited.

4.3.3.2.5 Systems shall not be pressurized or depressurized at rates which present unsafe situations, such as heat rise to autoignition. These rates shall be identified in the applicable operating procedure.

4.3.3.2.6 Pressure system bolts and fittings shall not be torqued while the component is under pressure.

4.3.3.2.7 Relief valves shall be inspected, reset, tested, and labeled annually.

4.3.3.2.8 Pressure gauges shall be inspected and calibrated annually and a due date label applied where used in safety critical systems.

SSP 50146, Revision B

4.3.3.2.9 All nonhydraulic pressure systems are to be leak tested with an inert medium at MOP at the launch site prior to using propellants or hazardous gases. Any time a component is modified, repaired, or replaced, it shall be pressure tested to 1.5 times MOP at the component level. The reassembled system shall again be leak tested at MOP using an inert medium.

4.3.3.3 Vacuum Systems and Requirements - Negative pressure protection shall be provided for systems not designed to withstand pressure below 1 atmosphere. This can be accomplished by the use of check valves or ambient automatic pressure valves.

4.3.4 Radiation

Sources of ionizing and nonionizing radiation must be adequately controlled during all phases of ground, launch, and postlaunch operations to assure the protection of personnel, facilities, and equipment, and the compliance with applicable federal, state, and NASA regulations and requirements. Such sources include radioactive materials, radiation-producing equipment (e.g., x-ray devices, particle accelerators, radio frequency/microwave emitters, etc.), lasers, and optical emitters (e.g., ultraviolet, infrared, and high intensity visible light sources). Specific requirements are provided in detail in the referenced applicable control documents and must be coordinated through the LSSO.

4.3.4.1 Radiological Health -

- A. Applicable radiological health program documents governing uses of ionizing and nonionizing radiation sources at KSC include:

KHB 1860.1A, "KSC Ionizing Radiation Protection Program"

KHB 1860.2, "KSC Non-Ionizing Radiation Protection Program"

The above-mentioned documents contain procedural/administrative requirements for radiation source approvals and usage.

- B. All uses of radiation sources require review and evaluation for approval by the appropriate launch site Radiation Protection Officer (RPO). Radioactive materials procurement, use, storage, and transportation at launch/landing sites are subject to specific requirements. Such activities must be coordinated with the launch/landing site RPO at least 60 days in advance of arrival to the launch site to assure compliance with applicable regulations. Identification of the launch/landing site RPO will be provided through the LSSO.

4.3.4.2 Radiation Safety - Additional radiation hazard controls required by the LSSO are provided below:

- A. Radiation sources associated with payloads must be compatible with and have no adverse safety effects on ordnance items, propellants, high pressure systems, critical structure components, or systems of any other payload, the Space Shuttle, or its crew.
- B. Delete
- C. Radiation source shields, interlocks, fail-safe systems, and limit switches shall be checked for proper operation.
- D. All radiating systems shall be designed, constructed, and operated to prevent exposure of personnel, facilities, and equipment to extreme temperatures, high voltages, toxic fumes and gases, and unnecessary radiant energy.

4.3.4.3 Optical Systems - The potential hazards which must be considered in the design, handling, and operation of optical equipment and associated energy sources may be grouped into five categories as follows:

SSP 50146, Revision B

- A. Hazardous optical radiation to include ultraviolet, infrared, and visible radiation.
- B. Temperature extremes.
- C. Shatterable materials.
- D. Contamination from gases and cryogenics.
- E. High voltage and x-rays.

4.3.4.3.1 General Optical Requirements - The following requirements shall apply to both flight and ground optical systems:

- A. Optical instruments shall be designed such that harmful light intensities and wavelengths cannot be viewed by operating personnel.
- B. Quartz windows, apertures, or beam stops and enclosures shall be used for hazardous wavelengths and intensities unless other suitable protective measures are taken to protect personnel from ultraviolet and/or infrared burns or x-ray radiation.
- C. Light intensities and spectral wavelengths at the eye piece of direct-viewing optical systems shall be limited to levels below the maximum permissible exposure (MPE).

4.3.4.3.2 Laser System Requirements - In addition to the referenced documents, the following requirements shall apply to both flight and ground hazardous laser systems:

- A. Limit stops, interlocks, and shields shall be provided to ensure that a laser beam cannot be misdirected.
- B. Laser power shall be locked out during all operations except laser testing.
- C. Positive locking features shall be provided to preclude focus and/or directional changes due to vibrations or inadvertent contact by operating personnel.
- D. Laser systems shall be designed so that all external components are at ground potential at all times.
- E. Materials used must be able to withstand the stresses caused by repetitive laser pulsing for the duration of checkout and mission performance.
- F. Laser systems shall incorporate a shutter system, beam stop, or attenuator capable of preventing output emissions in excess of the appropriate MPE level when the laser or laser system is on standby.
- G. Provisions shall be made to measure power output and perform boresighting with the beam totally enclosed and without unnecessary exposure to operating personnel.
- H. Laser target materials shall be nonreflective and fire resistant and shall not emit toxic contaminants.
- I. Laser installations shall incorporate adequate means to prevent the accumulation of hazardous cooling fluids and their by-products.
- J. Whenever toxic chemicals and/or cryogenic materials are utilized with laser systems, shut-off valves shall be provided to control leakage in the event of a line rupture.

4.3.4.3.3 Laser Operations - Laser operations shall include but not be limited to the following requirements:

- A. Alignment of target, optics, filters, etc., shall be accomplished utilizing low-powered visible lasers.
- B. Active beam or target viewing shall be done only by closed circuit television or an optical comparator with an appropriate filter.
- C. Laser beams shall not be directed toward flammable or explosive materials.
- D. Activated lasers shall not be left unattended.
- E. Personnel whose occupation or assignment may involve exposure to laser radiation shall use laser safety goggles approved by the Biomedical Office. These goggles shall protect for the specific wavelength of the laser and be of optical density adequate for the energy levels involved.

4.3.5 Ordinance - Delete

4.3.6 Mechanical, Electromechanical Devices

Mechanical or electromechanical devices that are used for such purposes as structure deployment or actuating release mechanisms must be evaluated to establish whether in the event of inadvertent activation damage to equipment or injury to personnel could occur. These devices shall be identified in the operational hazards analysis with the requirement for caution and warning notations incorporated in the TOP's (See 3.3.2).

4.3.7 Ammonia

The following requirements apply to the servicing of the SPP in the Space Station Processing Facility (SPPF) with ammonia. This operation is assumed to be performed using the KSC provided ammonia servicing cart. If RSC-E decides to use their own cart for the ammonia servicing operations, the design of the cart shall comply with the requirements of paragraph 4.3.3 above. Materials selected for use in ammonia systems shall be compatible with ammonia.

4.3.7.1 Ammonia Servicing Requirements -

- A. Ammonia servicing operations shall be performed only in areas and at times approved by the NASA Safety office. Personnel shall be limited to those directly involved in the ammonia servicing operation. Ammonia servicing shall only occur during 2nd and 3rd shifts on weekdays. 1st shift operations may be conducted on weekends.
- B. RSC-E shall describe their plans for controlling an ammonia leak throughout the ground processing at KSC. Procedures shall contain emergency instructions to handle leaks and spills.
- C. The SPP and the ammonia servicing equipment shall be grounded during ammonia servicing operations.
- D. Prior to opening the SPP ammonia system, the system shall be drained and flushed or purged to safe concentration levels.
- E. A leak test at maximum operating pressure with an inert gas shall be performed initially prior to servicing and after any modification or repair to the SPP ammonia system.

SSP 50146, Revision B

Refer to paragraph 4.3.3.2.9 above for more details. The proper operation of quick disconnects shall be demonstrated during the leak tests.

- F. The disposal of ammonia (liquid) shall be coordinated with the NASA Safety office.
- G. Venting of ammonia shall only be performed with approval from the NASA Safety Office. Ammonia shall be captured or vented to the atmosphere outside the SSPF.
- H. During ammonia servicing, a 10 foot control area shall be established around the ammonia fill lines, equipment, and flight hardware. Personnel protective equipment is required to be worn by all personnel within the control area. Protective equipment includes a rubber apron, rubber elbow length gauntlet style gloves, face shield, and a supplied air respirator for line connects and disconnects.

4.3.8 Cryogenics

4.3.8.1 Cryogenic Systems Requirements -

- A. Source flow shall have throttling capability
- B. Delete.
- C. GSE cryogenic valves with extended stems shall be installed with the actuator approximately vertical above the valve.
- D. Joints in piping systems shall be of either butt-welded, flanged, bayonet, or hub type.
- E. Cryogenic systems shall provide for thermal expansion and contraction without imposing excessive loads on the system. Bellows, reactive thrust bellows, or other suitable load relieving flexible joints may be used.
- F. GSE vacuum-jacketed systems shall be capable of having the vacuum verified.
- G. Cryogenic systems shall be designed so that anywhere a cryogen can be trapped between any valves in the system, automatic relief is incorporated to preclude excess pressure caused by conversion from liquid to gaseous state causing a rupture.
- H. Cryogenic systems shall be insulated with an oxygen compatible material or be vacuum-jacketed to preclude liquefaction of air.

4.3.8.2 Cryogenic Systems Operations -

- A. Cryogenic systems must be pressure tested with an inert medium at cryogenic temperature followed by a proof test at ambient temperature (no less than 60 °F). Pressure testing shall be 1.5 times MOP except where lesser factors (no less than 1.1 times MOP) are warranted to avoid adverse effects (e.g., plastic deformation or strain hardening) on the system.
- B. Cryogenic systems, including vacuum-jacketed pipe, shall be cold-shock tested with an appropriate cryogenic inert medium (at MOP or greater) prior to introducing any hazardous commodity into the system. Cold-shock leak testing can be accomplished at proof pressure to satisfy the cryogenic proof pressure requirements in paragraph A above.
- C. Delete.
- D. All personnel involved in cryogenic propellant transfer operations, repairs, or adjustments to the system must wear LSSO and Biomedical Office approved personal protective equipment.
- E. Delete.

4.3.9 GSE Materials

- A. A list of materials shall be maintained for each piece of GSE which interfaces with hazardous fluids. Hazardous fluids include, but are not limited to, gaseous oxygen, liquid oxygen, gaseous hydrogen, liquid hydrogen, Freon-21, ammonia and potassium hydroxide. This list will be of sufficient detail to permit an evaluation of the compatibility of the GSE design with the environment in which it is to be used.
- B. Mercury in liquid or vapor form shall not be used in GSE if a substitute of equivalent performance exists or an appropriate alternate design or method can be

used. Mercury shall not be used in any applications where contamination of flight hardware or exposure to personnel could result.

- C. Cleaning solvents and adhesive materials shall be contained in NFPA-approved safety containers. The use of and quantity allowed in the payload processing work area shall be approved by the LSSO. All users of these materials must comply with local fire, safety, and health regulations. Except where approved by the LSSO, the use of glass containers is prohibited in all payload processing work areas.
- D. Use of flammable materials and static-producing materials shall be kept to a minimum in all payload processing areas. If any plastic film is to be used, the material shall be selected from the LSSO approved plastics list. The material, quantity, and location of use shall be included in the RSC-E safety data package and approved by the LSSO. If a plastic film is not on the approved list, a sample (minimum 1 square yard) shall be submitted to the LSSO for test/evaluation and approval.
- E. GSE that contains components made of shatterable materials which is to be used inside the Orbiter or in areas where it could fall into the Orbiter shall be designed to provide positive containment to prevent fragments from entering the Orbiter.
- F. GSE designed for use directly in the Orbiter crew cabin or payload bay must meet the same materials flammability requirements as the payload/experiment itself.
- G. GSE used in flight vehicle habitable areas or in the payload bay shall not be painted or coated with materials subject to chipping, flaking, or scaling.
- H. Delete

4.3.10 Industrial Hygiene

Hazardous materials and physical agents must be controlled during all phases of launch/landing site operations to protect personnel by preventing exposures in excess of applicable limits and to comply with applicable federal and state regulations and requirements.

- A. Descriptive information concerning proposed uses of hazardous materials and physical agents will be provided by the payload organization to the LSSO for review and evaluation by the Biomedical Office.
- B. General Industrial Hygiene requirements include, but are not limited to, the following:
 - 1) Equipment which contains, possesses, or emits hazardous materials and/or physical agents will be designed, constructed, installed, and operated in a manner to ensure that the potential for exposure is kept as low as feasible.
 - 2) The payload organization shall provide a list of all hazardous materials and physical agents containing names, quantities, locations, and proposed uses (reference Paragraph 3.2.I). The payload organization shall also submit to the Launch Site Support Manager (LSSM) their input for the MSDS for each of these materials 60 days before arrival at the KSC.
 - 3) Hazardous materials and physical agents shall be used only by properly trained personnel and in accordance with procedures reviewed by the Biomedical Office and approved by the LSSO.

- 4) Engineering or administrative controls shall be the primary means for preventing personnel exposures. When such controls are not feasible or adequate to control exposure, personal protective equipment will be required.
- 5) Planned releases of hazardous materials shall not be permitted without review and approval by the LSSO and the Biomedical Office. Supportive data shall be provided by the payload organization to identify maximum expected quantities and concentrations of planned releases.
- 6) All activities involving hazardous materials or physical agents are subject to monitoring by the Biomedical Office.

C. Delete

4.3.11 Oxygen - Delete

4.4 ENVIRONMENTAL

4.4.1 Meteorological Requirements - Delete

4.4.2 Hazardous Atmosphere

4.4.2.1 General - Hazardous atmospheres are defined as follows:

- A. Flammable/Explosive Atmospheres - Hazardous atmospheres are defined as follows: A percentage of the lower explosive limit (LEL) shall be established to define a hazardous atmosphere for flammable/explosive gases or vapors by the LSSO on a case-by-case basis. Factors such as commodity involved, quantity, confinement area, the presence of oxygen-enriched atmospheres (greater than 25%), credible time for a hazardous condition to develop, and response time to complete emergency actions must be considered in establishing the percentage of the LEL. This percentage is usually 25% of the commodity LEL.
- B. Oxygen Deficient Atmospheres - A hazardous oxygen-deficient atmosphere may develop in enclosed spaces where operations or processes consume oxygen or release asphyxiating gases or vapors into the atmosphere. Entry into any atmosphere containing less than 19.5% oxygen is considered hazardous.
- C. Toxic/Corrosive Atmospheres - Hazardous toxic/corrosive atmospheres may be present where processes or operations generate airborne materials. Hazardous airborne materials include dusts, fibers, mists, fogs, smokes, fumes, gases, and vapors.

4.4.2.2 Confined Space Entry - Specific technical operating procedure approved by the LSSO, is required for work in confined spaces.

4.4.2.3 Hazardous Atmosphere Areas for Electrical Equipment - The hazardous atmosphere area for ammonia servicing shall be defined as 10 feet radially from the ammonia servicing equipment or the flight hardware (SPP).

4.4.2.4 Requirements for Electrical Equipment in Hazardous Atmospheres -

4.4.2.4.1 When operated within the area prescribed in paragraph 4.4.2.3 above, electrical equipment that is operated during ammonia servicing shall be either explosion proofed for ammonia or hazard proofed. Hazard proofing may be obtained by potting, hermetically sealing, or by positive pressurization with an inert gas or clean air. This

equipment must be monitored by personnel at all times during operation. This requirement does not apply to cables and their connectors on the flight hardware.

4.4.2.4.2 Electrical equipment to be operated outside the 10 foot control area shall be controlled by a single switch capable of deactivating all the nonexplosion proof equipment within the area. The switch shall be manned at all times when the equipment is in use. The switch shall be explosion proof/hazard proof if it is located within the 10 foot control area. Equipment which cannot meet this requirement shall be identified in the safety data package.

4.4.3 Humidity - Delete

4.4.4 Toxic Materials

The LSSO and Biomedical Office will establish criteria for operational controls involving all toxic materials.

4.5 HANDLING AND TRANSPORTS

The following definitions are to be used in this section:

- A. Lifting devices - slings, linkage, mechanisms, etc., that extend between a lifting hook on a hoist and the object being lifted. Only those items below the lifting hook are intended to be designed to the criteria contained in this Handbook. The requirements for the design of hoists, winches, and cranes are not included.
- B. Ground handling/transportation devices - trucks, dollies, transporters on which an object is placed for subsequent transportation or rotation.
- C. Work stand - work platforms, ladders, etc., that are fixed structures, are designed specifically to support personnel, and do not experience the dynamic loading associated with lifting and transportation.
- D. Support stand - GSE structure designed to support flight or ground equipment.
- E. Rated load - the maximum static weight that the basic equipment can safely support or lift.
- F. Working (actual) load - the expected or measured weight of a piece of equipment that is to be supported, lifted, or transported.

4.5.1 Hoisting and Handling

4.5.1.1 General - Delete

- A. All lifting and hoisting equipment must show evidence of the equipment having been tested in compliance with the requirements of the paragraphs in this section. This must be accomplished within 1 year prior to use.
- B. Records of all testing and inspections shall be maintained and shall be made available to the LSSO upon request.
- C. Rated loads will be posted on all lifting and hoisting equipment and fixtures.
- D. Magnetic particle, dye penetrant, radiography, or other suitable crack-detecting tests shall be performed on all load-bearing hooks, shackles, and eyebolts after the initial proof test of the assembled sling but prior to use and annually thereafter. The nondestructive inspection (NDI) method selected will require approval by the LSSO during the phase safety review process. A defect-detecting method such as radiography or ultrasonics which evaluates the material through

100% of its depth shall be performed on all welds constituting a single point of failure (i.e., critical weld) after the initial proof test of the assembled sling. Critical welds shall be eliminate where feasible. If RSC-E certifies that their lifting hardware is for a specific function, is properly controlled in terms of usage/misusage and the environment, and has undergone a thorough NDI prior to application of a protective coating, the LSSO may not require an annual NDI.

- E. Thimbles, shackles, links, eyebolts, swaged fittings, wire ropes, and similar devices must be subjected to and comply with the testing, preoperational and periodic inspection, and maintenance requirements set forth in Section 4.5.1. Eyebolts which are permanently fixed to the load are to be considered exempt from proof loading and NDI requirements. However, the eyebolts must comply with the design requirements of Table 4-1.
- F. Eyebolts that can be removed and replaced must have a positive means of determination of full thread engagement (i.e., shoulder, color marking, etc.).
- G. Attach points to payloads for the purpose of ground handling shall be classified as either utilizing the flight structural interfaces to the Orbiter or having special attach fittings for the purpose of ground handling. When utilizing the flight attach fittings for ground handling, structural analysis shall not be required if this determination has been made for flight dynamics. When special fittings for ground handling are used, an analysis shall be conducted to ensure the load paths have adequate safety factors for ground handling. The attach points (S/C) and fittings (GSE) shall be adequately described in the safety data package, including single failure points, verification methods (e.g., proof testing, NDI), and the methods used to assure proper connection during ground handling.
- H. Proof loading and associated NDI will be reaccomplished for modified or repaired lifting equipment.
- I. A load will not be lifted, suspended, or transported over personnel. This requirement should be considered during design of GSE for hardware integration and assembly.

4.5.1.2 Requirements for Slings -

- A. Slings shall be designed and tested as an assembled unit (unless otherwise approved by the LSSO) which includes spreader beams and drop legs (ropes, chains, shackles, eyebolts, pins, turnbuckles, etc.) in accordance with Table 4-1. Proof or periodic load test shall be accomplished within 1 year prior to use.
- B. All sling assemblies shall be visually inspected each day prior to use. A periodic inspection shall be performed by the using organization on a regular basis with frequency of inspection based on frequency of sling use, severity of service conditions, nature of lifts being performed, and experience gained on the service life of slings used in similar circumstances. Periodic inspections shall be performed by an authorized person. Any deterioration which could result in appreciable loss of original strength shall be carefully noted, and determination made whether further use of the sling would constitute a safety hazard. Periodic inspections shall be conducted annually, as a minimum.
- C. Wire rope slings shall be immediately removed from service if any of the following conditions are present:
 - 1) Ten randomly distributed broken wires in one rope lay or five broken wires in one strand in one rope lay.
 - 2) Wear or scraping of one third the original diameter of outside individual wires.

SSP 50146, Revision B

- 3) Kinking, crushing, bird caging, or any other damage resulting in distortion of the wire rope structure.
- 4) Evidence of significant heat damage.
- 5) End attachments that are cracked, deformed, or worn.
- 6) Hooks that have been opened more than 15% of the normal throat opening measured at the narrowest point or twisted more than 10 degrees from the plane of the unbent hook.
- 7) Significant corrosion of the rope or end attachment.

SSP 50146, Revision B

Table 4-1 Sling Requirements

SLING COMPONENT	SAFETY* FACTOR (ULTIMATE:RATED)	PROOF TEST (PROOF:RATED)	PERIODIC LOAD TEST (TEST:RATED)
Wire Rope	5	2	1.25
Alloy Steel Chain	5	2	1.25
Metal Mesh	5	1.5	1.25
Natural or Synthetic Web	5	1	1
Natural or Synthetic Rope			
Manila	5***	1	1
Polypropylene	6***	1	1
Polyester	9***	1	1
Nylon	9***	1	1
Structural Members (e.g., spreader beams)	5****	2	1.25
Shackles, Turnbuckles, Eyebolts, etc.	5	2	1.25

* As relates to this table, safety factor is defined as the ratio of a load that predicts a failure to a rated load.

** Delete

*** Use of rope slings will be limited to 50% of the rated capacity (manufacturer's rating).

**** A 3:1 safety factor against the worst case failure mode that will result in local yielding is acceptable.

- D. Structural sling inspection shall be performed at least annually. Discrepancies found during the following inspections shall be cause for replacement or repair:
- 1) Verify, overall, that there is no evidence of visual damage, gouges in metal, flaking paint, loose bolts, rivets, or connections, or deformation such as galling or gouges in pins, eyes, and end connections.
 - 2) Ensure that there are no bent, deformed, cracked, or excessively corroded support or main members.
 - 3) Inspect load-bearing bolts and verify that there is no visual evidence of bending, cracking, gross wear, or improper configuration.
 - 4) Inspect attached and lifting lugs for visual deformation and evidence of local yielding.
 - 5) Ensure that there are no elongated attach or lifting holes.
 - 6) Inspect around fasteners for local yielding and deformation.
 - 7) Remove and inspect load-bearing slip pins for visual deformation, evidence of bending, abnormal defects such as galling, scoring, brinelling, and diameters not within drawing tolerances. NDI shall be used when required by design requirements or when cracks are suspected.
 - 8) Inspect pin bores visually for cracks, deformation, local yielding, scoring, galling, and brinelling. NDI shall be performed as required.
 - 9) Inspect welds for cracks and evidence of deformation, deterioration, damage, or other defects by—
 - a. Visual inspection of all welds.
 - b. Magnetic particle, x-ray, or other suitable crack-detecting methods as appropriate for critical welds as identified on the drawings.
 - 10) Inspect all parts, particularly bare metal, for corrosion. Corrosion-protect all surfaces that are to be painted, lubricated, or coated with strippable vinyl, as necessary. Do not paint over uninspected areas; do not paint over cracks, deformations, deterioration, or other damage until engineering assessment has been made.
- E. For identification and on-site assurance purposes, equipment shall have a periodic recertification tag containing equipment identification, next required test date, and quality control stamp.

SSP 50146, Revision B

Hoists/winches and slings shall have proof load tags containing rated load, proof load, and proof load date.

- F. Slings which have components that are normally disassembled shall be either marked, coded, or tethered to assure proper assembly of verified hardware. Components not marked, coded, or tethered will invalidate the proof load/certification of the whole assembly. Removable lifting lugs used on flight hardware or GSE must be identified to ensure the lugs can be reinstalled in the proper location if necessary.
- G. Synthetic or natural rope slings shall be derated by 50% after the proof load; this then becomes the rated load; i.e., manufacturer's rating x 1.0 (proof test factor) x 0.50 (derating factor) = posted rated load.

4.5.1.3 Hydrasets - Delete

4.5.1.4 Chainfall - Delete

4.5.1.5 Load cells - Delete

4.5.1.6 Stands -

- A. Ground handling devices and support stands shall have a safety factor of 3:1 against yield.
- B. Personnel work stands shall have a safety factor of 4:1 against ultimate.
- C. Delete

4.5.2 Transporters- Delete

SSP 50146, Revision B

5.0 MISHAP INVESTIGATION AND REPORTING

5.1 NASA MISHAP INVESTIGATION CONTROL

Reporting and investigation for mishaps involving NASA payloads and associated GSE will be conducted.

5.2 Delete

5.3 MISHAP REPORTING

5.3.1 Mishap Contacts

The payload organization shall immediately report to the LSSO mishaps which result in death or injury/exposure of personnel or damage to resources, equipment, or facilities. Close calls shall be similarly reported. The LSSO mishap point of contact is as follows:

A. KSC Payload, Space Station and Industrial Safety Division (EI-F).

B. Delete

C. At contingency landing sites: The designated on-site LSSR.

Note: In the event that the mishap involves the release of and/or exposure to hazardous chemical agents, the Biomedical Office representative will be notified in addition to the LSSO.

D. Facility operators involved with or observing a mishap shall notify their safety point of contact.

Note: The LSSO mishap point of contact, above, is responsible for further notification to other LSSO mishap points of contact as necessary.

5.3.2 Payload Organization Involvement

RSC-E is responsible for investigating all mishaps and anomalies with which they may be involved, to the extent of their involvement.

5.3.3 Payload Organization Responsibilities

For mishaps involving RSC-E, the following defines investigation and written reporting responsibilities:

A. If government personnel/property, including contractors, are injured/damaged from or contribute to the mishap, then RSC-E shall report as follows:

- 1) A preliminary written report of the mishap to the LSSO mishap point of contact within one working day after the mishap occurs.
- 2) RSC-E may be requested to conduct its own investigation concurrently with the government investigation.
- 3) RSC-E will provide a copy of the final report to the LSSO mishap point of contact.

B. If only RSC-E personnel/property, including RSC-E contractors, are injured/damaged from or contribute to the mishap, and the mishap is not considered a near miss to government property/personnel, then the RSC-E shall report as follows:

- 1) When the LSSO mishap point of contact is notified, the need for a preliminary written report will be determined.

SSP 50146, Revision B

- 2) Investigation shall be done by the payload organization using its own internal procedures.
- 3) A copy of the final report of the mishap investigation shall be sent to the LSSO mishap point of contact for Lessons Learned purposes.

5.3.4 Investigation Boards- Delete

5.3.5 Mishap Scene.

The scene of the mishap shall not be disturbed until the investigating authority has given concurrence to do so.

APPENDIX A

ACRONYMS, ABBREVIATIONS, AND GLOSSARY OF TERMS

AC - Alternating Current.ACGIH - American Conference of Governmental Industrial Hygienists.AFM - Delete.AFOSH - Delete.AFR - DeleteAFSC - DeleteAFSCF - DeleteANSI - Delete.ASME - DeleteAWG - American Wire Gauge.BUDDY SYSTEM - The buddy system requires that two people be designated to be concerned with each other's safety in a hazardous situation. The system does not demand shoulder-to-shoulder contact, but rather visual contact and a proximity that allows each buddy to help the other in an emergency.C - Centigrade.CCAFS - DeleteCFR - Code of Federal Regulations.CLOSE CALL - An unplanned occurrence in which there is no injury/damage but under similar circumstances could have resulted in a reportable mishap.cm² - Centimeter Squared.CPIA - DeleteCREDIBLE - A condition that can occur and is reasonably likely to occur. For the purpose of this document, failures of structure, pressure vessels, and pressurized lines and fittings are not considered credible failure modes if those elements comply with the applicable requirements.CRITICAL WELD - A weld where a single failure of any portion could result in injury to personnel or damage to property or flight hardware.DAMAGE - Breakage, mangling, mutilation, ruin of items, transmitted across system or component interfaces inadvertently by internal or external action, including component failure and human error which could cause obstruction of critical functions and requiring repair or replacements.D.B. (DESIGN BURST PRESSURE) - A specified test pressure that pressurized components must withstand without rupture to demonstrate design adequacy in a qualification test.dB - Decibel.

SSP 50146, Revision B

dBA - Decibel, A-scale.

DC - Direct Current.

DEVIATION - Granted use or acceptance of an article for more than one mission which does not meet the specified requirements.

DH - Delete

DOD - Delete.

DOP - Delete

EED - Electroexplosive Device.

ELS - Eastern Launch Site, including Kennedy Space Center and/or Cape Canaveral Air Force Station.

EMI - Electromagnetic Interference.

EPD - Emergency Procedures Document.

ETA - Explosive Transfer Assembly.

EXPLOSIONPROOF APPARATUS - Apparatus enclosed in a case that is capable of withstanding an explosion of a specified gas or vapor which may occur within it and of preventing the ignition of a specified gas or vapor surrounding the enclosure by sparks, flashes, or explosion of the gas or vapor within, and which operates at such an external temperature that a surrounding flammable atmosphere will not be ignited thereby.

F - Fahrenheit.

FAILURE - The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

FLUID - Liquids or gases.

GSE (GROUND SUPPORT EQUIPMENT) - The ground equipment and systems needed to support the payload such as propellant loading units, data recording, instrumentation, etc.

HAZARD - A risk of personnel exposure, injury, or death; or of hardware damage or loss.

HAZARDPROOF - Prevention of an explosive atmosphere penetrating electrical fixtures where sparking or arcing could occur.

HAZARDOUS FLUID - Any fluid that is toxic, cryogenic, flammable, or corrosive.

HAZARDOUS MATERIAL - This includes solid, liquid, or gaseous materials which, under foreseeable conditions, are toxic, carcinogenic, cryogenic, explosive, flammable, pyrophoric, water-reactive, corrosive, an oxidizer, a compressed gas, a combustible liquid, or are chemically unstable.

HB - Handbook.

I.D. - Identification.

IMC - Interim Message Change.

SSP 50146, Revision B

IUS - Delete

JP - Delete.

JSC - Johnson Space Center, NASA, Houston, Texas 77058.

KHB - Kennedy Handbook.

KMI - Kennedy Management Instruction.

KSC - Kennedy Space Center, NASA, Florida 32899.

KSC-STD - KSC Standard.

LEL - Lower Explosive Level.

LSSO - Launch Site Safety Office.

LSSR - Launch Site Safety Representative.

mA - Milliampere.

MAWP (MAXIMUM ALLOWABLE WORKING PRESSURE) - The maximum pressure at which a component can continuously operate based on allowable stress values and functional capabilities. MAWP is synonymous with MDOP (Maximum Design Operating Pressure) or "Rated Pressure."

MDOP - Maximum Design Operating Pressure.

MIL - Delete

MIL-STD - Delete.

MISHAP - An unplanned event which results in personnel fatality, injury, or exposure; damage to or loss of the Space Shuttle, environment, public property, or private property; or could result in an unsafe situation or operational mode.

MOP (MAXIMUM OPERATING PRESSURE) - The maximum pressure at which the system or component actually operates in a particular application. MOP is synonymous with MEOP (Maximum Expected Operating Pressure) or maximum working pressure.

MPE - Maximum Permissible Exposure.

MRS - Major Radiological Sources.

MSDS - Material Safety Data Sheets.

mV - Millivolt.

mW - Milliwatt.

N/A - Not Applicable.

NASA - National Aeronautics and Space Administration.

NDI - Nondestructive Inspection.

NEC - Delete

SSP 50146, Revision B

NFPA - Delete

NHB - NASA Handbook.

NMI - NASA Management Instruction.

NONCOMPLIANCE REPORT - The request form submitted by the payload organization to obtain a waiver or deviation for those technical safety requirements of this document that have not been met.

OMD - Operations and Maintenance Documentation.

OMI - Operations and Maintenance Instructions.

OSHA - Occupational Safety and Health Administration.

PAYLOAD - Any equipment or material carried by the Space Shuttle that is not considered part of the basic Space Shuttle itself. It, therefore, includes items such as free-flying automated spacecraft, individual experiments or instruments, payload support equipment, etc. As used in this document, the term payload also includes payload-provided GSE and systems and flight and ground systems software.

PAYLOAD BAY - The 15-foot diameter by 60-foot long enclosed volume within the Orbiter, designed to carry carriers, payloads, payload-support equipment, and associated mounting hardware.

PAYLOAD ELEMENTS - Experiments, instruments, or other individual payload items which are subsets of an integrated, multipayload cargo complement on missions such as Spacelab, etc.

PO (PAYLOAD ORGANIZATION) - The funding or sponsoring organization for the experiment, payload, or mission. This does not mean the principal investigator, payload contractor, designer, or developer except to the extent delegated by the sponsoring organization. For NASA-sponsored payloads, a NASA Headquarters payload program office is the sponsoring organization and usually delegates to a NASA Field Center the authority for formal interface with the SSP operator in the implementation of this document. Other payload organizations include, but are not limited to, the following: DOD, other U.S. Government agencies, non-U.S. Government public organizations, private persons or private organizations, international organizations, European Space Agency, foreign governments, etc.

PHE - Delete.

PHYSICAL AGENT - Any environmental factor, such as noise, temperature extremes, vibrations, etc., which may cause harm or injury to personnel.

PRESSURE TEST - A test pressure which demonstrates that no part of a pressure system component shall fail, take any permanent set, or be damaged in any manner, when subjected to the applicable proof pressure.

psi - Pounds Per Square Inch.

psig - Pounds Per Square Inch Gauge.

RATED LOAD - The static weight that the basic equipment can safely support or lift.

REFEREE FLUID - A compatible fluid, other than that used during normal operation of a system, which is substituted for test purposes because it is safer due to characteristics such as being less toxic, less explosive, easier to detect, etc.

REM - Roentgen Equivalent, Man.

SSP 50146, Revision B

REQUIREMENT - A specified mandatory condition which must be complied with unless a noncompliance report is approved by the Center Commander/Director.

RF - Radio Frequency.

RH - Relative Humidity.

RHU - Radioisotope Heater Unit.

rms - Root Mean Square.

RP - Delete

RPO - Radiation Protection Officer.

RTG - Radioisotope Thermoelectric Generator.

S&A - Safe and Arm.

SAE - Delete

SAFETY CRITICAL - Any condition, event, operation, process, equipment, or system with a potential for exposing personnel to a hazardous material, injury or death, or for causing damage to, or loss of, equipment or property.

SAFETY FACTOR - The ratio of a load that predicts a failure to a rated load.

S/C - Spacecraft.

SD - Delete

SDR - Delete

SHALL - Mandatory action.

SHOULD - Recommended action.

SPIF - Delete

SPW - Delete

SPWR - Delete

SSP - Space Shuttle Program.

STD - Standard.

STS (SPACE TRANSPORTATION SYSTEM) - The Space Shuttle, Spacelab, Inertial Upper Stage (IUS), and the ground sites needed to support these elements.

SYSTEM CERTIFICATION PRESSURE - The maximum pressure that has been applied to a system; however, no system element can have its MAWP exceeded when the certification pressure has been applied.

TBD - To Be Determined.

T.O. - Delete

SSP 50146, Revision B

TOP's - Technical Operating Procedures (See Appendix C).

TP - Delete

UDS - Delete

USAF - Delete

WAIVER - Granted use or acceptance of an article for a single mission which does not meet the specified requirements.

WILL - Advising of future action.

SSP 50146, Revision B

APPENDIX B

COMPLIANCE AND REFERENCE DOCUMENTS

(DELETED)

APPENDIX C

GUIDELINES FOR THE PREPARATION OF TECHNICAL OPERATING PROCEDURES (TOP's)

1. The Safety Community applies the generic term, Technical Operating Procedures (TOP's), to all test or operations procedures. The term "TOP's" only implies that the procedure must meet minimum content and processing standards. In practice, procedures will carry the nomenclature of the system under which they are developed such as Operations and Maintenance Instructions (OMI's) of the Operations and Maintenance Documentation (OMD) system. The host organization prescribes the system to be used.

2. TOP's are categorized as follows:

TOP's are classified as hazardous or nonhazardous in accordance with the criteria provided in Paragraph 4.1.3A of the basic document.

- a. Category I TOP: Provides detailed procedures authorizing work for the operation, maintenance, verification of ground support systems/equipment, and instructions for checkout, servicing, handling, and transportation of the payload systems/subsystems and experiments during prelaunch, launch, and postlaunch operations. Repetitive hazardous and nonhazardous operations use Category I TOP's.

- b. Category II TOP: Provides engineering instruction, authorizes work, establishes work control methods, and is normally prepared for a one-time-only nonhazardous operation in order to accommodate special tests or authorize temporary installations, removals, or replacements.

A Category II TOP may also be used for one-time-only hazardous operations and for repetitive nonhazardous operations when work is of limited scope and does not economically justify preparation of a Category I TOP.

3. The review and approval process for TOP's is in accordance with the TOP category.

- a. Category I hazardous TOP's are submitted to the LSSO for safety approval.
- b. Delete
- c. Category II hazardous TOP's are submitted to the LSSR for approval.

NOTE: Nonhazardous TOP's are submitted to the LSSO for review only.

4. All TOP's shall be prepared in clear, precise language that can be readily understood by personnel involved in the operations. All hazardous TOP's will be reviewed for content as follows:

- a. A brief description of the task operation or checkout.
- b. Identification of the operating location for hazardous operations (e.g., facility, building, test area, etc.) and/or departing/arriving areas [e.g., Shuttle Payload Integration Facility (SPIF), Pad 39A, etc.].
- c. Specific hazards to which personnel will be exposed during the operation (e.g., explosives, propellants, radiation, etc.). Configuration of the payload prior to, during, and at completion of operation shall be provided.
- d. Identification of inhibits and a means for verifying that the inhibits are in place.

e. Identification of any condition(s) which cause the TOP to be classified hazardous. Safety precautions (CAUTION/WARNING notes) will be specified for any activities, hazardous or nonhazardous, where specific guidelines must be observed or actions taken to prevent or limit hazards. The notes will immediately precede the step/sequence which directed the action. Public address announcements, where available, will be made to alert personnel of the dangers and information associated with the hazardous operation. All procedures involving manually controlled pressurization of systems where MAWP can be reached shall contain a CAUTION/WARNING stating the MAWP immediately before the step which calls for pressurization. Definitions are—

Warning: Operational step(s), etc., which if not adhered to or observed could result in personal injury or exposure.

Caution: Operational step(s), etc., which if not adhered to or observed could result in damage to equipment.

- f. Identification of organizational elements and facilities required to support the operation (e.g., Safety, Security, Medical, etc.).
- g. Identification of tools, equipment, and clothing required for the safe performance of a hazardous operation or as required by emergency procedures associated with the operation. Protective equipment shall be specified by manufacturer and model number. This information will be contained/specified within the "warning note" immediately preceding the first step/sequence or group of steps within a sequence which is hazardous.
- h. Safety related quality assurance verifications have been identified. These include verifying calibration of monitoring equipment and gauges, load testing of lifting devices, specification of torque values, calibration of torque wrenches, etc.
- i. A list of referenced documents containing all the instructions that are specifically called out within the TOP or required to support the operation. The list will contain the document identifying number, revisions, and title with the originator listed in parenthesis after the title. Where the latest issue of the document or drawing is to be used rather than a specific revision, latest issue (LI) will be entered in the revision column.
- j. Unique safety rules and regulations that cannot be addressed to a specific step in the operational sequence of the TOP, but which are required for the safe conduct of a hazardous operation. Note: The final authority for the Safety Requirements Section will be the responsibility of the appropriate safety office.
- k. A list identifying those essential personnel required in the specified control area during hazardous steps/sequences. The list will be included immediately preceding the first step/sequence or group of steps within a sequence which are hazardous. The list will identify the individuals by call sign/functional title, number of personnel, approximate location, function, and the organization or contractor employing the individual. Changes to this list shall be considered on a case-by-case basis with approval by the LSSR. If the list is identical throughout the TOP, it may be detailed once and referenced thereafter.
- l. A procedural step (placed immediately preceding the first step/sequence of the hazardous steps) to identify/specify each control area for hazardous operations and directing all nonessential personnel to clear the specified control area, allowing sufficient time for them to do so before the start of a hazardous step/sequence. Control areas are normally specified in the appropriate LSSO documentation or must be approved by the LSSO. Special consideration will be given to a potential release of explosive/toxic vapors. The controlled area will be determined on quantity (worst case calculation).
- m. When LSSR participation is required, the following steps are included:

- 1) 24-hour notification prior to start of procedure.
- 2) LSSR concurrence prior to start of step/sequences or subtask TOP's containing hazardous operations.
- 3) Prior to opening the control area for controlled work at the conclusion of hazardous activities.

n. A procedural step to verify the payload organization completion of the facility safety inspection. A procedural step requiring the performance of a pretest and pretask briefings. The pretest briefing will immediately precede the beginning of the operational steps of the Technical Operating Procedure (TOP). The pretask briefings will precede each step/sequence or group of steps within a sequence which are hazardous. If a shift change occurs prior to the completion of the hazardous task, then the briefing must be repeated for the relieving employees. Items to be addressed are specific hazards personnel and equipment will be exposed to, safety protective equipment, emergency alarms, evacuation routes, emergency instructions and Emergency Procedures Documents (EPD's), the specific revisions of TOP's to be used, and identification of critical items.

- o. Prior to and following each hazardous step/sequence, section, paragraph, or step within the TOP text introducing a hazardous operation(s), notes will be inserted similar to the following:

- 1) Prior to:

WARNING

THE FOLLOWING STEPS/SEQUENCES ARE HAZARDOUS -
INSTALLATION OF CATEGORY A ORDNANCE (SPECIFY ALL HAZARDS)

- 2) Following:

NOTE

END OF HAZARDOUS STEPS/SEQUENCES

- p. All hazardous operations require the use of the "Buddy System."
- q. Identification of those job categories requiring certification/license for the performance of the TOP task, and procedural step prior to the performance of hazardous operations ensuring that personnel are properly certified, equipped, and briefed.
- r. A procedural step verifying that a preroute survey has been accomplished before transporting GSE and flight hardware where length, height, or width may cause interference problems/hazards.
- s. A procedural step verifying that a safety walkdown of the area involving flight hardware and/or related GSE has been performed prior to the commencement of any hazardous steps.
- t. A procedural step with the task leader verifying that personnel participating in a hazardous operation are equipped, briefed, and ready to proceed.
- u. Each integrated/controlling TOP must specify specific safety controls which are contained in sub-task TOP's/documents.
- v. Emergency Instructions. Any TOP, hazardous or non-hazardous, must have emergency instructions when operations directed in the TOP activate systems/equipment capable of causing personnel injury or equipment damage if not expeditiously shutdown, safed, or secured should a malfunction occur (i.e., electrical, pneumatic, hydraulic, propellants or chemicals, lifting/hoisting). During those periods when individual TOP's are in progress, the emergency instruction in the TOP will take precedence for those operations under its control; however, the EPD will contain emergency instructions for other emergency situations not under direct control of an active TOP. Instructions shall:

- 1) Contain specific actions necessary to cope with emergency/contingency conditions and identify the individual directing the actions.
 - 2) Address hazards unique to the operation and shall provide steps for rendering safe (e.g., propellant flow shutdown, pressure relief, safe ordnance, mission/operation abort, etc.) to protect personnel and equipment.
 - 3) Be located in an appendix and available to the test team at all times.
5. Covers used on TOP's must be approved by the LSSO and shall meet the following requirements:
- a. Covers shall contain a statement that the TOP contains hazardous operations or does not contain hazardous operations. The formatting of the cover is at the discretion of the payload organization; however, the following format is suggested:
 - 1) In red block letters at least 3/16 inches high:

THIS DOCUMENT CONTAINS HAZARDOUS OPERATIONS
 - 2) In black block letters at least 3/16 inches high:

THIS DOCUMENT DOES NOT CONTAIN
HAZARDOUS OPERATIONS
 - b. Emergency TOP's shall be so identified and should use a distinctive cover, preferably a different color.
 - c. The cover or title page shall contain the approval signatures as defined by the LSSO, date, and revision number.
6. TOP's changes/revisions shall be processed as follows:
- a. Formal changes/revisions to existing Category I TOP's shall be reviewed, filed, and approved by the LSSO in the same manner as the original TOP.
 - b. Interim changes to existing Category I and II TOP's may be made providing they are made in accordance with the following:
 - 1) Whenever there is insufficient time to make a formal change to a previously released TOP.
 - 2) By an approved deviation or other documentation authorizing interim change(s).
 - 3) Change shall be identified (select applicable term) as follows:

THIS CHANGE (DOES/DOES NOT) INCREASE
THE HAZARD LEVEL OF THIS DOCUMENT
 - c. Interim changes made to TOP's performed at KSC that add or increase a hazard, are written within a hazardous sequence, or involve the flight termination system require LSSO approval for release and use. Deviations (modifications) prepared when the LSSR is not present can be approved prior to performance by the LSSR by telephone, recorded OIS, or safety radio nets. LSSR signature on the deviation sheet is to follow as soon as possible.

- d. A written approved deviation is required for changes/deviations to any section of a hazardous technical operating procedure, including out-of-sequence testing. For emergency or time critical operations, the test may continue with the deviation written after the fact provided concurrences are recorded on the net.
- e. Out-of-sequence performance of nonhazardous tests, operations, sequences, or operational steps may be accomplished if the out-of-sequencing is annotated (along with time, date, and new location in order) in the TOP designating concurrence of key test/task personnel. Changes to technical work steps of Category I non-hazardous TOP will require a written, approved deviation.
- f. For both hazardous and nonhazardous procedures, the writer may choose to preplan sequences that can be performed out of order. By writing the proper notes identifying these preplanned sequences, they may be performed without the requirement to write a deviation.
- g. In addition to Paragraph e. above, redline changes will only be used to correct clerical errors or make pen-and-ink changes.

SSP 50146, Revision B

APPENDIX D

ORDNANCE STORAGE AND HANDLING
DATA REQUIREMENTS

(DELETED)

SSP 50146, Revision B

APPENDIX E

PAYLOAD RELATED EMERGENCY PROCEDURES DOCUMENTS AND FACILITY SAFETY PLANS

1. Delete
2. Delete
3. Delete
4. Delete
5. Delete
6. Delete
7. Delete
8. Delete
9. Delete
10. Delete
11. Delete
12. Payload Ground Operations Contract (PGOC) Emergency Procedures Plan, MDCY 1009, Revision I, Annex A (consolidates all the previously existing Emergency Procedure Plans). (SSPF ONLY)

Document references:

1. NSTS 13830, Implementation Procedure for NSTS Payloads System Safety Requirements.
2. SSP 30599, Safety Review Process, International Space Station Program.
3. United States Code of Federal Regulations, Department of Labor, Occupational Safety and Health Administration (OSHA), Part 1910.1200, Hazard Communication Standard.
4. KHB 1860.1, KSC Ionizing Radiation Program.
5. KHB 1860.2, KSC Non-Ionizing Radiation Program.

NOTE: The requirements of the above documents will be enforced per latest issue.

ATTACHMENT B - DATA ITEM DESCRIPTION (DIDs)

R-10-S01	Safety and Mission Assurance (S&MA) Plan	B2
U-10-S08	Safety and Mission Assurance (S&MA) Plan	B5
R-10-S02	Hazard Reports and System Description	B8
R-10-S03	Mishaps and Investigation Reports	B11
U-10-S09	Mishaps and Investigation Reports	B12
R-10-S04	Integrated Safety Data	B13
U-10-S05	Integrated Safety Data	B15
R-10-S06	Logic Tree Development	B16
U-10-S07	Logic Tree Development	B17
R-10-R01	Failure Mode Summary Report (FMSR)	B18
U-10-R05	Failure Mode and Effects Analysis (FMEA) and Critical Items List (CIL)	B20
R-10-R02	Reliability and Maintainability Predictions Report	B21
U-10-R06	R&M Predictions Report	B24
R-10-R03	Critical Item List (CIL)	B27
R-10-QA01	Failure Reporting and Corrective Action	B30
U-10-QA03	Failure Reporting and Corrective Action	B32

SSP 50146, Revision B

DATA ITEM DESCRIPTION (DID)

1. DID Number: R-10-S01

2. DID Title: Safety and Mission Assurance (S&MA) Plan

3. Approval Required Yes X No

4. Initial Submittal Date: May 15, 1996

5. Update Frequency: N/A

6. Number of Copies:

6.1 English version: N/A

6.2 Russian version: 1

7. Preparation information:

7.1 Use: To define RSA planned method of accomplishing S&MA task required to show compliance with requirements in SSP 41163 and NASA/RSA Bilateral S&MA Process Requirements for ISS for all RSA provided international partner contributions to the ISS.

7.2 Content: The S&MA Plan shall address the philosophy, organization , approach and processes for all aspects of Safety, Reliability, Maintainability, Quality Assurance, and Software Quality Assurance programs. The plan should include all stages to the program including design, manufacture and test, certification and verification, flight test, operations, and document control.

7.2a. Safety Plan: The Safety Plan shall define the methodology and techniques for achieving safety requirements. This will be a description of how the safety program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the safety program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.2b. Reliability Plan: The Reliability Plan shall define the methodology and techniques for achieving Reliability requirements. This will be a description of how the Reliability program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the Reliability program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.2c. Maintainability Plan: The Maintainability Plan shall define the methodology and techniques for achieving Maintainability requirements. This will be a description of how the Maintainability program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the Maintainability program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.2d. Quality Assurance Plan: The Quality Assurance Plan shall define the methodology and techniques for achieving Quality Assurance requirements. This will be a description of how the Quality Assurance program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. ORGANIZATION
2. PLANNING FOR ON-ORBIT ACTIVITIES
3. TRAINING
4. INTERNAL QUALITY PROGRAM AUDITS AND SURVEYS
5. MILESTONE REVIEWS
6. DESIGN AND DEVELOPMENT CONTROLS
7. CHANGE CONTROL VERIFICATION
8. PRODUCT/PROCESS DEVELOPMENT AND VALIDATION
9. IDENTIFICATION AND DATA RETRIEVAL
10. RETENTION OF RECORDS
11. SUPPLIER/PROCUREMENT CONTROLS
12. RECEIVING INSPECTION
13. AUDITS AND SURVEYS OF PROCUREMENT SOURCE OPERATIONS
14. FABRICATION CONTROLS
15. ARTICLE AND MATERIAL CONTROLS

16. CLEANLINESS/CONTAMINATION CONTROL
17. PROCESS CONTROLS
18. NONDESTRUCTIVE EVALUATION (NDE)
19. WORKMANSHIP STANDARDS
20. CONTROL OF TEMPORARY INSTALLATIONS AND REMOVALS
21. TEST CONTROLS
22. INSPECTION AND TEST RECORDS AND DATA
23. NONCONFORMANCE CONTROL SYSTEM
24. PROBLEM REPORTING
25. METROLOGY
26. HANDLING, STORAGE, PRESERVATION, MARKING, LABELING,
PACKAGING, PACKING, AND SHIPPING
27. SAMPLING PLANS, STATISTICAL PLANNING, AND ANALYSES

7.2e. Software Quality Assurance The Software Quality Assurance Plan shall define the methodology and techniques for achieving Software Quality Assurance requirements. This will be a description of how the Software Quality Assurance program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the Software Quality Assurance program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.3 Format: The S&MA Plan will be organized by the major functions of S&MA. Organization with a separate volume for each discipline area will permit each volume to be revised and approved (i.e., Safety, Reliability, Maintainability, Quality Assurance, and Software Quality Assurance).

DATA ITEM DESCRIPTION (DID)

1. DID Number: U-10-S08

2. DID Title: Safety and Mission Assurance (S&MA) Plan

3. Approval Required Yes X No

4. Initial Submittal Date: May 15, 1996

5. Update Frequency: N/A

6. Number of Copies:

6.1 English version: 1

6.2 Russian version: N/A

7. Preparation information:

7.1 Use: To define NASA planned method of accomplishing S&MA task required to show compliance with requirements in SSP 41000 and NASA/RSA Bilateral S&MA Process Requirements for ISS for all NASA provided contributions to the ISS.

7.2 Content: The S&MA Plan shall address the philosophy, organization, approach and processes for all aspects of Safety, Reliability, Maintainability, Quality Assurance, and Software Quality Assurance programs. The plan should include all stages to the program including design, manufacture and test, certification and verification, flight test, operations, and document control.

7.2a. Safety Plan: The Safety Plan shall define the methodology and techniques for achieving safety requirements. This will be a description of how the safety program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the safety program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.2b. Reliability Plan: The Reliability Plan shall define the methodology and techniques for achieving Reliability requirements. This will be a description of how the Reliability program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the Reliability program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.2c. Maintainability Plan: The Maintainability Plan shall define the methodology and techniques for achieving Maintainability requirements. This will be a description of how the Maintainability program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the Maintainability program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.2d. Quality Assurance Plan: The Quality Assurance Plan shall define the methodology and techniques for achieving Quality Assurance requirements. This will be a description of how the Quality Assurance program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. ORGANIZATION
2. PLANNING FOR ON-ORBIT ACTIVITIES
3. TRAINING
4. INTERNAL QUALITY PROGRAM AUDITS AND SURVEYS
5. MILESTONE REVIEWS
6. DESIGN AND DEVELOPMENT CONTROLS
7. CHANGE CONTROL VERIFICATION
8. PRODUCT/PROCESS DEVELOPMENT AND VALIDATION
9. IDENTIFICATION AND DATA RETRIEVAL
10. RETENTION OF RECORDS
11. SUPPLIER/PROCUREMENT CONTROLS
12. RECEIVING INSPECTION
13. AUDITS AND SURVEYS OF PROCUREMENT SOURCE OPERATIONS
14. FABRICATION CONTROLS
15. ARTICLE AND MATERIAL CONTROLS

16. CLEANLINESS/CONTAMINATION CONTROL
17. PROCESS CONTROLS
18. NONDESTRUCTIVE EVALUATION (NDE)
19. WORKMANSHIP STANDARDS
20. CONTROL OF TEMPORARY INSTALLATIONS AND REMOVALS
21. TEST CONTROLS
22. INSPECTION AND TEST RECORDS AND DATA
23. NONCONFORMANCE CONTROL SYSTEM
24. PROBLEM REPORTING
25. METROLOGY
26. HANDLING, STORAGE, PRESERVATION, MARKING, LABELING,
PACKAGING, PACKING, AND SHIPPING
27. SAMPLING PLANS, STATISTICAL PLANNING, AND ANALYSES

7.2e. Software Quality Assurance The Software Quality Assurance Plan shall define the methodology and techniques for achieving Software Quality Assurance requirements. This will be a description of how the Software Quality Assurance program will be conducted to meet the design requirements and process requirements. The plan shall include, as a minimum, the following:

1. An identification of each task, as defined in other DIDs to be accomplished under the Software Quality Assurance program.
2. A description of how each task will be performed
3. The procedures (where existing procedures are applicable) to evaluate the status and control of each task
4. The identification of the organization unit with the authority and responsibility for executing each task

7.3 Format: The S&MA Plan will be organized by the major functions of S&MA. Organization with a separate volume for each discipline area will permit each volume to be revised and approved (i.e., Safety, Reliability, Maintainability, Quality Assurance, and Software Quality Assurance).

DATA ITEM DESCRIPTION (DID)

1. DID Number: R-10-S02
2. DID Title: Hazard Reports and System Description
3. Approval Required: Yes X No
4. Initial Submittal Date: 45 days prior to Phase 1 safety review (see schedule included in NASA/RSA Safety Review Process for ISS) for element specific data
(See table attached)
5. Update Frequency: 45 days prior to each phase safety review for elements
(See table attached)
6. Number of Copies:
 - 6.1 English version: N/A
 - 6.2 Russian version: 1
7. Use: The ISS SRP will use the Hazard Reports and System Description to assess the design and operation of ISS element hardware configuration.
8. Preparation Information:
 - 8.1 Scope: R-10-S02 shall consist of hazard reports and system descriptions for all Russian flight hardware. Additionally, R-10-S02 shall document integrated hazard analyses for the overall Russian Segment.
 - 8.2 Format: These deliverables shall be in the format agreed-upon in the NASA/RSA Safety Review Process.
 - 8.3 Content: Hazard Reports and System Descriptions shall be provided that are commensurate with the level of maturity of the design.
 - 8.3.1 System Description: RSA shall provide a description of the on-orbit configuration of the hardware and software in accordance with NASA/RSA Safety Review Process for ISS. Functional diagrams shall be submitted and supplemented with descriptions of interfaces and operations. When this data has been previously provided to NASA by RSA, it is acceptable to use the documents containing design and system descriptions. If necessary, additional data shall be provided.

8.3.2 Hazard Reports: Hazard Reports/Off-nominal Situations shall be done in accordance with NASA/RSA Safety Review Process for ISS. For Phase I maturity, Hazard Reports shall reflect the preliminary design review level of detail that define hazards causes, and provide the preliminary hazard controls. Additionally, preliminary verification methods when available should be included. For Phase II maturity, the Hazard Reports shall be updated to reflect the critical design level of detail and define the finalized hazard controls and verification methods. For Phase III, the Hazard Reports shall be updated to reflect the as-built design and document completion of verification.

Service Module	Initial Report (due 45 days prior to Phase 0 SRP)
Service Module	Interim Report (due 45 days prior to Phase 1 SRP)
Service Module	Interim Report (due 45 days prior to Phase 2 SRP)
Service Module	Final Report (due 45 days prior to Phase 3 SRP)
FGB	Initial Report (due 45 days prior to Phase 1 SRP)
FGB	Interim Report (due 45 days prior to Phase 2 SRP)
FGB	Final Report (due 45 days prior to Phase 3 SRP)
UDM	Initial Report (due 45 days prior to Phase 1 SRP)
UDM	Interim Report (due 45 days prior to Phase 2 SRP)
UDM	Final Report (due 45 days prior to Phase 3 SRP)
DC	Initial Report (due 45 days prior to Phase 1 SRP)
DC	Interim Report (due 45 days prior to Phase 2 SRP)
DC	Final Report (due 45 days prior to Phase 3 SRP)
Soyuz	Initial Report (due 45 days prior to Phase 0 SRP)
Soyuz	Interim Report (due 45 days prior to Phase 1 SRP)
Soyuz	Interim Report (due 45 days prior to Phase 2 SRP)
Soyuz	Final Report (due 45 days prior to Phase 3 SRP)
Progress	Initial Report (due 45 days prior to Phase 0 SRP)
Progress	Interim Report (due 45 days prior to Phase 1 SRP)
Progress	Interim Report (due 45 days prior to Phase 2 SRP)
Progress	Final Report (due 45 days prior to Phase 3 SRP)
SPP	Initial Report (due 45 days prior to Phase 1 SRP)
SPP	Interim Report (due 45 days prior to Phase 2 SRP)
SPP	Final Report (due 45 days prior to Phase 3 SRP)
LTV	Initial Report (due 45 days prior to Phase 1 SRP)
LTV	Interim Report (due 45 days prior to Phase 2 SRP)
LTV	Final Report (due 45 days prior to Phase 3 SRP)
DSM	Initial Report (due 45 days prior to Phase 1 SRP)
DSM	Interim Report (due 45 days prior to Phase 2 SRP)
DSM	Final Report (due 45 days prior to Phase 3 SRP)
Research M-1	Initial Report (due 45 days prior to Phase 1 SRP)
Research M-1	Interim Report (due 45 days prior to Phase 2 SRP)
Research M-1	Final Report (due 45 days prior to Phase 3 SRP)
Research M-2	Initial Report (due 45 days prior to Phase 1 SRP)
Research M-2	Interim Report (due 45 days prior to Phase 2 SRP)
Research M-2	Final Report (due 45 days prior to Phase 3 SRP)
Research M-3	Initial Report (due 45 days prior to Phase 1 SRP)

SSP 50146, Revision B

Research M-3	Interim Report (due 45 days prior to Phase 2 SRP)
Research M-3	Final Report (due 45 days prior to Phase 3 SRP)
LSM	Initial Report (due 45 days prior to Phase 1 SRP)
LSM	Interim Report (due 45 days prior to Phase 2 SRP)
LSM	Final Report (due 45 days prior to Phase 3 SRP)

DATA ITEM DESCRIPTION (DID)

1. DID Number: R-10-S03
2. DID Title: Mishap and Investigation Reports
3. Approval Required: Yes ____ No X
4. Initial Submission: Within one week of occurrence (by telephone or written notification).
5. Frequency of Submission: As required.
6. Number of Copies:
 - 6.1 English version: N/A
 - 6.2 Russian version: 1
7. Use: Provide notification and status of investigation of accidents or incidents related to the RS of the ISS Program. To provide technical assistance to NASA and RSA boards investigating mishaps that are within their jurisdiction.
8. Preparation Information:
 - 8.1 Scope: RSA Mishap reports shall encompass ISS Program mishaps occurring during manufacturing, testing, and operational period. The RSA organizations shall provide records and other administrative or technical support to review boards investigating mishaps.

A mishap is defined as any unplanned occurrence, event, or anomaly. Mishaps that should be reported to NASA by RSA include those mishaps that may have significant program impact, may affect schedule, or cause death or permanent injury of crew or non-Russian ground personnel.
 - 8.2 Format: The mishap report is to be done in the RSA format.

DATA ITEM DESCRIPTION (DID)

1. DID Number: U-10-S09
2. DID Title: Mishap and Investigation Reports
3. Approval Required: Yes ☐ No ☒
4. Initial Submission: Within one week of occurrence (by telephone or written notification).
5. Frequency of Submission: As required.
6. Number of Copies:
 - 6.1 English version: 1
 - 6.2 Russian version: N/A
7. Use: Provide notification and status of investigation of accidents or incidents related to the USOS of the ISS Program. To provide technical assistance to NASA and RSA boards investigating mishaps that are within their jurisdiction.
8. Preparation Information:
 - 8.1 Scope: NASA Mishap reports shall encompass ISS Program mishaps occurring during manufacturing, testing, and operational period. The NASA organizations shall provide records and other administrative or technical support to review boards investigating mishaps.

A mishap is defined as any unplanned occurrence, event, or anomaly. Mishaps that should be reported to RSA by NASA include those mishaps that may have significant program impact, may affect schedule, or cause death or permanent injury of crew or ground personnel.
 - 8.2 Format: The mishap report is to be done in the NASA format.

DATA ITEM DESCRIPTION (DID)

1. DID Number: R-10-S04
2. DID Title: Integrated Safety Data
3. Approval Required: Yes ____ No X
4. Initial Submittal: RSA: June 01, 1996 (for Stage 2R) TBD
5. Update Frequency: RSA: 90 days prior to each phase of each IDR Element Integrated Stage Safety Review
6. Number of Copies: 1 each (in native format)
7. Preparation information:
 - 7.1 PURPOSE/USE: Identification and tracking of integrated hazards, their resolution, control actions, and status.
 - 7.2 SCOPE: All hazards that have an effect on the interfaces or USOS/IP elements. All hazards that cannot be fully controlled within RS. Data will be provided at a level equivalent to the hazard analysis provided to the SRP prior to the submittal.

7.3 DESCRIPTION:

RSA will provide:

1. Hazards and off-nominal situations descriptions for RS hazards which affect the interface or USOS/IP elements.
 2. List of causes identified (at the time of submittal) during the RS hazard analysis that will require one or more controls from the USOS to assure ISS safety.
 3. Description of how the agreed-upon controls requested by the USOS/IP will be implemented on the RS.
- For Phase 1 IDR review:
 - Data outlined above with sufficient detail for a Phase 1 Safety Review as defined in “NASA/RSA Safety Review Process”

Hazard data:

- Failures which affect the interface or other elements
- Identification of additional controls required from other elements to meet total safety failure tolerance requirements
- Implementation of controls required by USOS/IP elements or ISS partners
- For Phase 2 IDR review:
 - Update of Phase 1 data consistent with requirements defined in “NASA/RSA Safety Review Process”
- For Phase 3 IDR review:
 - Update of Phase 2 data with status of verification and open work as defined in “NASA/RSA Safety Review Process”

SSP 50146, Revision B

8. **FORMAT:** Native format is acceptable.

DATA ITEM DESCRIPTION (DID)

1. DID Number: U-10-S05
2. DID Title: Integrated Safety Data
3. Approval Required: Yes ____ No X
4. Initial Submittal: NASA/Boeing: March 30, 1996
5. Update Frequency: NASA/Boeing: 135 days prior to each phase of each IDR Safety Review
6. Number of Copies: 1 each (in native format)
7. Preparation information:
 - 7.1 PURPOSE/USE: Identification and tracking of integrated hazards, their resolution, control actions, and status.
 - 7.2 SCOPE: All hazards that have an effect on the interfaces or RS elements. All hazards that cannot be fully controlled within US/IP segment.
 - 7.3 DESCRIPTION:

NASA/Boeing will provide to RSA:

 1. Boeing-Prime integrated hazard reports
 2. Boeing-Prime integrated logic tree
 3. Detailed recommending list of ISS hazards and causes requiring controls partially on USOS and partially on RS.
 - For Phase 1 IDR review:
 - Data outlined above with sufficient detail for a Phase 1 Safety Review as defined in “NASA/RSA Safety Review Process”
 - Hazard data:
 - Failures which affect the interface or other elements
 - Identification of additional controls required from other elements to meet total safety failure tolerance requirements
 - Implementation of controls required by RS elements
 - For Phase 2 IDR review:
 - Update of Phase 1 data consistent with requirements defined in “NASA/RSA Safety Review Process”
 - For Phase 3 IDR review:
 - Update of Phase 2 data with status of verification and open work as defined in “NASA/RSA Safety Review Process”
8. FORMAT: Native format is acceptable.

SSP 50146, Revision B

DATA ITEM DESCRIPTION (DID)

1. DID Number: R-10-S06
2. DID Title: Logic Tree Development
3. Approval Required: Yes____ No __X__
4. Initial Submittal: TBD
5. Update Frequency: 90 days prior to each phase of each IDR Element Integrated Stage Safety Review
6. Number of Copies: 1 in English
7. Preparation information:
 - 7.1 PURPOSE/USE: Identification and tracking of hazards, their causes.
 - 7.2 SCOPE: All hazards that have an effect on the interfaces or other elements. All hazards that cannot be fully controlled within that segment.
 - 7.3 DESCRIPTION: RSA will provide to NASA:
 - Additions/corrections to the integrated logic tree
8. FORMAT: Consistent with the format of the Boeing developed Logic tree as developed using CAFTA software.

DATA ITEM DESCRIPTION (DID)

1. DID Number: U-10-S07
2. DID Title: Logic Tree Development
3. Approval Required: Yes ____ No X
4. Initial Submittal: September 1995
5. Update Frequency: 135 days prior to each phase of each IDR Safety Review
6. Number of Copies: 1 in English
7. Preparation information:
 - 7.1 PURPOSE/USE: Identification and tracking of hazards, their causes.
 - 7.2 SCOPE: All hazards that have an effect on the interfaces or other elements. All hazards that cannot be fully controlled within that segment.
 - 7.3 DESCRIPTION: NASA/Boeing will provide to RSA:
 - Boeing-Prime integrated logic tree for each stage of ISS
8. FORMAT: Consistent with the format of the Boeing developed Logic tree as developed using CAFTA software.

SSP 50146, Revision B

DATA ITEM DESCRIPTION (DID)

1. Data Requirement Number: R-10-R01
2. Data Requirement Title: Failure Mode Summary Report (FMSR)
3. Approval Required: Yes ____ No X
4. Initial Submittal: September 30, 1996
5. Update Frequency: As required, per Bilateral Protocols
6. Number of Copies:

- 6.1 ENGLISH VERSION: N/A
- 6.2 RUSSIAN VERSION: 1

7. SOW Reference: N/A

8. Electronic Delivery Required: Yes

9. Purpose: To document the cases of non-compliance with the specification requirements concerning reliability, to identify critical items.

10. Preparation Information:

FMSR for each module shall contain the list of all items with single failures of which the specification requirements of failure tolerance and failure propagation are not fulfilled. Failure propagation is assumed to be violated if failure effects, as manifested at the RS/USOS interfaces, are outside specified interface conditions. The list shall include items whose single failure causes an effect on the ability of the RS/USOS to perform the specified capabilities within the RS/USOS specification. (For capabilities allowed to exhibit degraded performance, this is defined as inability to deliver specified life and station critical functionality and specified interface conditions to the USOS/RS.) The following information is given for every item of such type:

1. Item's title and designation
2. Item's capability (function)
3. System in which the item is utilized
4. Impact of item's failure on:
 - 4.1 Capability, mentioned in paragraph 3.2.3.1, Failure tolerance requirements of the USOS/RS specification.
 - 4.2 Interfaces with ISS other modules (systems)
 - 4.3 Crew/ISS safety

5. Approximate time to effect (instantly, seconds, minutes, etc.)
6. Approximate time to detect (instantly, seconds, minutes, etc.)
7. Approximate time to restore (instantly, seconds, minutes, etc.)

The RS shall consider the effects on hardware in the event of failure effect on the other side of the interface. The interface conditions shall be evaluated/analyzed by the receiving segment/system for possible damage to equipment. The results shall be documented in the respective FMSR.

Service Module	Initial Report
Service Module	Update Report
FGB	Initial Report
FGB	Update Report
UDM	Initial Report
UDM	Update Report
DC	Initial Report
DC	Update Report
SPP	Initial Report
SPP	Update Report
LTV	Initial Report
LTV	Update Report
DSM	Initial Report
DSM	Update Report
Research M-1	Initial Report
Research M-1	Update Report
Research M-2	Initial Report
Research M-2	Update Report
Research M-3	Initial Report
Research M-3	Update Report
LSM	Initial Report
LSM	Update Report

DATA ITEM DESCRIPTION

1. DID Number: U-10-R05
2. DID Title: Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)
3. Frequency of Submission: Formal electronic update 30 days prior to Program Design Reviews
4. First Submission Date: 30 days prior to the first IDR, electronically available
5. Copies and Distribution: 1 copy in English
8. Remarks: N/A
9. Use: The FMEA serves as a source that documents the systematic evaluation by item failure mode analyses, the potential impact of each functional or hardware failure on mission success, personnel, and systems safety, system performance, maintenance, and maintainability requirements. Each potential failure is assessed in order that appropriate corrective action(s) may be taken to eliminate or control the high risk items. The CIL documents the item's inability to meet program requirements.
10. References:
 - (a) Statement of Work (SOW); paragraph 1.7.1.a.(3)
 - (b) SSP 30234, Failure Modes, Effects, and Criticality Analysis
11. Interrelationships: DRs SM05 and VE32
12. Preparation Information:
 - 12.1 Scope: The FMEA/CIL shall be performed on program hardware to the equipment level consistent with the identified on-orbit maintenance level and ground support equipment as specified in SSP 30234.
 - 12.2 Format: The data element format shall be as specified in SSP 30234.
 - 12.3 Content: The FMEA/CIL contents are specified by SSP 30234.
 - 12.4 Maintenance: The worksheets shall be maintained electronically.

DATA ITEM DESCRIPTION

1. DATA REQUIREMENT NUMBER: R-10-R02
2. DATA REQUIREMENT TITLE: Reliability & Maintainability Predictions Report
3. APPROVAL REQUIRED: Yes _____ NO X
4. INITIAL SUBMITTAL DATE: June 1996, Preliminary data January 1996
5. UPDATE FREQUENCY: For each stage of the ISS, as required.
6. NUMBER OF COPIES:
 - 6.1 ENGLISH VERSION: N/A
 - 6.2 RUSSIAN VERSION: 1
7. SOW REFERENCE N/A
8. ELECTRONIC DELIVERY REQUIRED: YES X NO _____
9. PURPOSE: Reliability and Maintenance predictions data shall be used to status quantitative R&M characteristics of Space Station functions, capabilities, and equipment. The quantitative predictions data are used to estimate the probability that an item will perform its required functions during the mission and to estimate the end of service life. The predictions also estimate the demand for maintenance and identify areas where special emphasis or attention is needed.
10. PREPARATION INFORMATION:
 - 10.1 REFERENCE DOCUMENTS:
 - 10.2 DATA DESCRIPTION (CONTENTS): The R&M predictions report shall document information related to critical Space Station functions (As defined in the NASA/RSA Bilateral Process Requirements Document, Attachment A, and below) and the interfaces between segments. The reports shall consist of :

Reliability:

 - 1) An estimate of overall functional reliability for each critical Station function.
 - 2) A report which describes the system or systems included in the estimates.

Maintainability

 - 1) An estimate of crew maintenance time per year for IVA, EVA and EVR maintenance for each stage of the ISS, and for all ISS equipment utilized at assembly complete.

10.3 DATA REQUIREMENT SPECIFIC FORMAT : The analysis shall be submitted in the native RSA format.

11.0 DEFINITIONS : Critical functions for estimating the reliability of the Space Station are as follows:

1. Determine navigational parameters
2. Maintain attitude - non propulsive
3. Control attitude - propulsive
4. Execute translation maneuvers
5. Maintain habitable atmosphere
6. Provide Electrical Power
7. Maintain thermal conditioning
8. Provide command and data handling
9. Support on orbit - ground communications
10. Support Space Station to external vehicle communication
11. Support assured crew return

Service Module	Initial Report
Service Module	Update Report
FGB	Initial Report
FGB	Update Report
UDM	Initial Report
UDM	Update Report
DC	Initial Report
DC	Update Report
Soyuz	Initial Report
Soyuz	Update Report
Progress	Initial Report
Progress	Update Report
SPP	Initial Report
SPP	Update Report
LTV	Initial Report

SSP 50146, Revision B

LTV	Update Report
DSM	Initial Report
DSM	Update Report
Research M-1	Initial Report
Research M-1	Update Report
Research M-2	Initial Report
Research M-2	Update Report
Research M-3	Initial Report
Research M-3	Update Report
LSM	Initial Report
LSM	Update Report

DATA ITEM DESCRIPTION

1. DID Number: U-10-R06
2. DID Title: R&M Predictions Report
3. Frequency of Submission: Formal updates 30 days prior to Program Design Reviews
4. First Submission Date: 30 days prior to the first IDR
5. Copies and Distribution: 1 copy in English
6. Use: The S&MA allocations, assessments, and analysis reports shall be used to identify, validate and status quantitative and qualitative S&MA allocation and performance characteristics of space station function and equipment and to document preventive maintenance requirements and limited life items.
7. Preparation Information:
 - 7.1 Scope: This report shall provide requirement allocations, predictions, trade studies, and analysis for the space station system according to designated capabilities, functions, and on-orbit repairable items. Predicted S&MA performance shall be documented according to capability, function, and on-orbit repairable item for each stage of the assembly sequence.
 - 7.2 Format: These reports shall be delivered in the Contractor's format.
 - 7.3 Content: The S&MA allocations, assessments, and analysis report shall document the program status and progress in executing the S&MA requirements and objectives. The report shall contain the following:
 - (a) S&MA Requirements Compliance Summary
 - (1) Compare predictions to allocations
 - (2) Assess compliance at system, segment, function, and CI level
 - (3) Identify percent compliant, percent non-compliant and percent TBD
 - (4) Define areas of non-compliance, level, rationale, and corrective action
 - (b) S&MA Qualitative Assessments
 - (1) Provide ground rules and assumptions used in assessments
 - (2) Identify methods/tools used in performing assessments
 - (3) Provide results summary, conclusions and recommendations
 - (c) S&MA Trade Studies
 - (1) Identify associated ground rules and assumptions used in study
 - (2) Define trade candidates and characteristics/features that were evaluated

- (3) Provide S&MA position (e.g., preferred design option)
 - (4) Summarize decision rationale used in the option selection
- (d) S&MA Quantitative Predictions and Analyses
 - (1) Define the approach/process used and levels of reserve (where applicable).
 - (2) Identify associated ground rules and assumptions used in making predictions and performing analyses .
 - (3) Define prediction techniques, methodologies and tools.
 - (4) Provide EVA, EVR, and IVA crew maintenance time predictions for corrective and preventive maintenance to demonstrate compliance with allocations.
 - (5) Provide EVA, EVR, and IVA overhead maintenance time predictions for corrective and preventive maintenance
 - (6) Provide maintenance action rate predictions
 - (7) Provide summaries of major contributors to probability of failure, crew maintenance time, safety hazards
 - (8) Provide percentages of detecting failures modes at the capability, function and on-orbit maintainable equipment item level
 - (9) Provide percentages of failure modes capable of being isolated to a single maintainable equipment item and to the ambiguity group
 - (10) Provide source data used in analysis
 - (11) Identify prediction data fidelity levels
 - (12) Provide reliability block diagrams and associated data
 - (13) Provide a summary table of current reliability (probability of success) predictions to demonstrate compliance with requirements.
- (e) S&MA Assembly Analysis
 - (1) Define the approach/process used and levels of reserve (where applicable).
 - (2) Identify associated ground rules and assumptions used in making predictions and performing analyses.
 - (3) Define prediction techniques, methodologies and tools.
 - (4) Provide EVA, EVR, and IVA crew maintenance time predictions for corrective and preventive maintenance by flight.
 - (5) Provide EVA, EVR, and IVA overhead maintenance time predictions for corrective and preventive maintenance.
 - (6) Provide maintenance action rate predictions by flight.
 - (7) Provide percentage of detecting failures modes by stage at the capability, function and on-orbit maintainable equipment item level.
 - (8) Provide percentage of failure modes capable of being isolated to a single maintainable equipment item and to the ambiguity group.
 - (9) Provide manifest and activation flights of all on orbit maintainable items.
 - (10) Provide reliability block diagrams and associated data by stage.
 - (11) Provide a summary table of current reliability predictions by stage.
- (f) Preventive Maintenance

SSP 50146, Revision B

- (1) Define the approach and process used to define preventive maintenance requirements.
- (2) Identify ground rules and assumptions.
- (3) Provide preventive maintenance requirements and rationale.

7.4 Maintenance: These reports shall be maintained electronically.

DATA ITEM DESCRIPTION

1. **DATA REQUIREMENT NUMBER:** R-10-R03
2. **DATA REQUIREMENT TITLE:** Critical Item List (CIL)
3. **APPROVAL REQUIRED:** Yes note 1 NO _____
Note 1: Document requires ISS program approval.
4. **INITIAL SUBMITTAL DATE:** SEPTEMBER 30, 1996
5. **UPDATE FREQUENCY:** As Required, per Bilateral Protocols
6. **NUMBER OF COPIES:**
6.1 NATIVE VERSION: 1
7. **SOW REFERENCE:** N/A
8. **ELECTRONIC DELIVERY REQUIRED:** YES X _____
NO _____
9. **PURPOSE:** The CIL shall document failure modes of equipment and single failure points. The purpose is to support risk assessment, additional design action, safety analysis, preparation of mandatory inspection points, hardware/software interface analyses, test planning, maintainability analysis and planning, and logistics planning.
10. **PREPARATION INFORMATION:**
 - 10.1 **REFERENCE DOCUMENTS:** SSP 30234 REV A
 - 10.2 **DATA DESCRIPTION (CONTENTS):**

A critical item list shall be developed for all criticality 1, 1S, and 1P items. The CIL will also include criticality 1R items which fail the redundancy screens. Critical Item criticality categories are defined as:

Criticality 1

Those single failure points that could result in loss of Space Station or loss of flight personnel.

Criticality 1S

A single failure point of the system component designed to provide safety of protection capability against a potentially hazardous condition or event or a single failure point in a safety or hazard monitoring system that causes the system to fail to detect, or operate when needed during the existence of a hazardous condition that could lead to loss of flight personnel or Space Station.

Criticality 1P

A single failure point which is protected by a safety device, whereby the proper functioning of the safety device, would prevent the hazardous consequences of the failed (protected) component.

Criticality 1R items that fail one of the redundancy screens below

Criticality 1R items are those redundant items, all of which if failed, could result in loss of Space Station or loss of flight personnel. Note: For purpose of CIL Identification, both the flight and ground detection screens must be failed for the item to be identified as a CIL (reference SSP 30234)

At a minimum the CIL shall be prepared to the assembly level at which the item is repaired or replaced. The CIL shall be prepared for each individual module in the Russian segment and shall contain the following data elements as a minimum (note: FGB CILs will be prepared according to separate contract requirements):

Item name (14)* - Nomenclature and part number of the item being analyzed.

SSP 50146, Revision B

Item function	- The function of the item under analysis.
Type of Redundancy	- Indication whether the redundancy is active or standby. Indicate the level of redundancy(example 2 of 3 required).
System Name	- Name of the system the item is associated with.\
System function	- The function(s) of the system the item failure mode affects. Reference functions described in Table IX of the Russian Segment Specification, SSP 41163.
Failure mode text (29)*	- Additional description of the failure mode under analysis, i.e., 1. Premature operation; 2. Failure to operate within specification or failure to operate at a prescribed time; 3. Failure during operation, including failure to contain or store energy or fluids; 4. Failure to cease operations at a prescribed time.
Criticality category (31)*	- Criticality for the worst case effect
Failure detection (35)*	- How the failure mode for the item would be detected and verified.
Time to detect (36A&B)*	- Time expressed as seconds, minutes, hours, days, weeks or months that describe the estimated time from failure occurrence to detection of the failure by the crew.
Failure effect on - Crew/ISS (44)*	- Worst case failure mode effect on the crew/ISS /Orbiter
Time to effect (45A&B)*	- Estimated time from failure occurrence to manifestation of worst case failure mode effects. Expressed as seconds, minutes, hours, days, weeks or months
Redundancy screen	
- Checkout Prelaunch(49)*	- Indication for redundant items if they have passed or failed the redundancy screen. Indicates if redundant item can be checked out without maintenance.
- Checkout on-orbit(50)*	- Indication for redundant items if they have passed or failed the redundancy screen. Indicates if inactive redundant item can be checked out without maintenance.
- Detection Flight Crew (51)*	- Indication for redundant items if they have passed or failed the redundancy screen. Indicates if the failure mode can be detected by the flight crew during any mission phase.
- Detection Ground Control (52)*	- Indication for redundant items if they have passed or failed the redundancy screen. Indicates if the failure mode can be detected by the ground crew during any mission phase.
- Loss of Redundancy from a Single Cause (53)*	- Indication for redundant items if they have passed or failed the redundancy screen. Indicates that all redundant items could not be lost by a single credible event or cause (excludes fire or M/OD).
Hazard number (56A)* exists)	- Reference to the applicable hazard report (where a hazard analysis exists)
Retention rationale:	
- design (73)*	- Specific design features which minimize the probability of occurrence of the failure mode and its causes.
- test (74)*	- Specific testing which will be accomplished which supports the premise that the critical failure mode/cause has been addressed properly.
- inspection (77)*	- Specific inspection points and critical process controls implemented to minimize the probability that the points and critical process controls implemented to minimize the probability that the failure mode causes will occur in the system.
- failure history (78)*	- Summary of information relative to the performance history of the hardware for the failure mode. Include only failures from acceptance testing of modules and in-flight operation of the item

- operational use (79)* - Description of the crew and/or ground personnel operations used to mitigate the failure's effect. (May reference hazard reports)
- maintainability (80)* - Describe the possibility of performing maintenance or repair of the item prior to the occurrence of the failure effects. Discuss the availability of spare items on the ground or in orbit. Identification of specific maintainability verifications performed (analysis or flight test). Identify level of repair/replacement.

* Note: The number in parenthesis refers to SSP 30234 Appendix C data element.

10.3 FORMAT: Each submittal shall have a discrete title page stating :
TBD

10.4 DATA REQUIREMENT SPECIFIC FORMAT AND PREPARATION INSTRUCTIONS:

10.4.1 RSA shall perform appropriate failure analysis and document the following:

- Assumptions and ground rules used in the analysis
- Summary report of analysis
- CILs

Data Submittals:

Service Module	Initial Report
Service Module	Update Report
FGB	Initial Report
FGB	Update Report
UDM	Initial Report
UDM	Update Report
DC	Initial Report
DC	Update Report
SPP	Initial Report
SPP	Update Report
LTV	Initial Report
LTV	Update Report
DSM	Initial Report
DSM	Update Report
Research M-1	Initial Report
Research M-1	Update Report
Research M-2	Initial Report
Research M-2	Update Report
Research M-3	Initial Report
Research M-3	Update Report
LSM	Initial Report
LSM	Update Report

DATA ITEM DESCRIPTION

1. DID NUMBER: R-10-QA01
2. DID TITLE Failure Reporting and Corrective Action
3. APPROVAL REQUIRED YES _____ NO X
4. INITIAL SUBMITTAL DATE: For on orbit failures and failures which may affect program schedule, failure reports shall be issued within 15 days of occurrence. For others, failure reports shall be delivered 5 days prior to FRR or equivalent review.
5. UPDATE FREQUENCY: Initial report; final report following satisfactory resolution of problem
6. NUMBER OF COPIES:
 - 6.1 ENGLISH VERSION: N/A
 - 6.2 RUSSIAN VERSION: 1
7. SOW REFERENCE N/A
8. ELECTRONIC DELIVERY REQUIRED: YES _____ NO X
- 8.1 ELECTRONIC FORMAT REQUIRED: N/A
9. PURPOSE: To provide a system for failures reporting and recurrence control for flight and test hardware.
10. PREPARATION INFORMATION:
 - 10.1 REFERENCE DOCUMENTS: N/A
 - 10.2 DATA DESCRIPTION (CONTENTS): The following types of failures shall be reported:

On Orbit: All failures with effect on US/RS interface, or effect on a critical function. (defined in NASA/RSA Bilateral Process Requirements Document, Attachment A).

Prior to launch: 1) All problems which could affect Program schedule. 2) All unresolved problems, which affect critical functions or USOS/RS ICD limits, and which remain unresolved at FRR or equivalent.

A report shall be prepared and submitted for each failure as described above. The Failure Reports shall include the following as a minimum:

SSP 50146, Revision B

- a. Identification of the failed component,
- b. The date and the site location that the nonconformance/problem was detected,
- c. The situation under which the nonconformance/problem was observed and the actions taken as a result of the failure,
- d. A description of the failed component,
- e. Cause of the failure,
- f. Failure effect, or information concerning events which may be impacted as a result of the nonconformance/problem,
- g. The corrective action(s) taken to resolve the nonconformance/problem,
- h. Actions taken to prevent reoccurrence on similar hardware, and
- i. Results of testing/inspection to ensure that the nonconformance/problem was corrected.

DATA REQUIREMENT SPECIFIC FORMAT AND PREPARATION INSTRUCTIONS:
Native format is acceptable

DATA ITEM DESCRIPTION

1. DID NUMBER: U-10-QA03
2. DID TITLE Failure Reporting and Corrective Action
3. APPROVAL REQUIRED YES ____ NO X
4. INITIAL SUBMITTAL DATE: Within 5 days of occurrence
5. UPDATE FREQUENCY: Initial report; final report following satisfactory resolution of problem
6. NUMBER OF COPIES:
- 6.1 ENGLISH VERSION: 1
- 6.2 RUSSIAN VERSION: N/A
7. SOW REFERENCE N/A
8. ELECTRONIC DELIVERY REQUIRED: YES X NO ____
- 8.1 ELECTRONIC FORMAT REQUIRED: Y
9. PURPOSE: To provide a system for failures reporting and recurrence control for flight and test hardware.
10. PREPARATION INFORMATION:
- 10.1 REFERENCE DOCUMENTS: SSP 30223

10.2 DATA DESCRIPTION (CONTENTS):

A report shall be prepared and submitted for each failure encountered in accordance with SSP 30223. The Failure Reports shall include the following as a minimum:

- a. Identification of the failed component,
- b. The date and the site location that the nonconformance/problem was detected,
- c. The situation under which the nonconformance/problem was observed and the actions taken as a result of the failure,
- d. A description of the failed component,
- e. Cause of the failure,
- f. Failure effect, or information concerning events which may be impacted as a result of the nonconformance/problem,
- g. The corrective action(s) taken to resolve the nonconformance/problem,
- h. Actions taken to prevent reoccurrence on similar hardware, and
- i. Results of testing/inspection to ensure that the nonconformance/problem was corrected.

10.3 DATA REQUIREMENT SPECIFIC FORMAT AND PREPARATION
INSTRUCTIONS: Native format is acceptable

SSP 50146, Revision B

ATTACHMENT C

NASA /RSA SAFETY REVIEW PROCESS FOR ISS

ATTACHMENT C TABLE OF CONTENTS

1.0 INTRODUCTION	C-5
1.1 PURPOSE AND SCOPE	C-5
2.0 APPLICABLE DOCUMENTS	C-5
2.1 REFERENCE DOCUMENTS	C-6
3.0 RESPONSIBILITIES	C-6
4.0 ISS SAFETY REVIEW PROCESS	C-6
4.1 SAFETY ANALYSIS AND DELIVERABLES	C-6
4.2 GENERAL REVIEW PROCESS FLOW	C-7
4.3 PHASE SAFETY REVIEW MEETING	C-7
4.4 PHASE SAFETY REVIEW OBJECTIVES	C-8
4.5 PROGRAM HAZARD REPORT ACCEPTANCE	C-8
4.6 SAFETY REVIEW DATA SUBMITTALS	C-8
5.0 PHASE SAFETY REVIEW	C-10
5.1 PHASE I SAFETY REVIEW	C-10
5.1.1 PHASE I DATA REQUIREMENTS	C-10
5.1.2 PHASE I OFF-NOMINAL SITUATION/HAZARD REPORTS	C-10
5.1.3 PHASE I/II/III SAFETY REVIEW MEETING AGENDA ITEMS	C-11
5.1.4 OFF-NOMINAL SITUATION/HAZARD REPORT DISPOSITION	C-12
5.2 PHASE II SAFETY REVIEW	C-12
5.2.1 PHASE II DATA REQUIREMENTS	C-12
5.2.2 PHASE II HAZARD REPORTS	C-13
5.3 PHASE III SAFETY REVIEW	C-14
5.3.1 PHASE III DATA REQUIREMENTS	C-14
5.3.2 PHASE III HAZARD REPORTS	C-15
5.4 POST PHASE III SAFETY ACTIVITY	C-16
6.0 NONCOMPLIANCE WITH SPACE STATION REQUIREMENTS	C-17
7.0 SIMILAR EQUIPMENT	C-19

SSP 50146, Revision B

APPENDIX A: AMENDMENTS TO THE “NASA/RSA SAFETY REVIEW PROCESS FOR ISS,” APPLICABLE TO SOYUZ AND PROGRESS VEHICLES	C-20
A.1.0 INTRODUCTION	C-20
A.1.1 PURPOSE	C-20
A.1.2 SCOPE	C-20
A.2.0 SAFETY REVIEW REQUIREMENTS	C-21
A.2.1 INTERNATIONAL SPACE STATION ALPHA SAFETY REVIEWS	C-21
A.2.2 PHASE SAFETY REVIEWS	C-21
A.2.3 LEVELS OF DESCRIBING OFF-NOMINAL SITUATION/HAZARD	C-21
A.2.4 POST PHASE III SAFETY ACTIVITY	C-21
A.2.4.1 CHANGES IN THE DESIGN OR OPERATION AFFECTING THE ISS	C-22
A.2.4.2 CHANGES THAT DO NOT AFFECT THE ISS	C-22
A.2.4.3 SAFETY REVIEW FOR THE FIRST LAUNCH	C-22
APPENDIX B: INSTRUCTIONS FOR ISS HAZARD REPORT FORM	C-23
B.1 SCOPE	C-23
B.2 SUPPORT DATA	C-23
B.3 APPROVAL	C-23
FIGURE B.1 ISS HAZARD REPORT/OFF-NOMINAL SITUATION FORM	C-24
TABLE B.1: TABLE OF HAZARD CAUSE SEVERITY	C-32
TABLE B.2 TABLE OF LIKELIHOOD OF OCCURRENCE OF HAZARD CAUSES	C-33

1.0 INTRODUCTION

NASA has developed an ISS Safety Review Process to execute its responsibilities for the overall integrated safety of the ISS. That process is defined in SSP 30599. The NASA /RSA safety review process defined herein reflects the bilateral agreements between NASA and RSA which will implement the intent of the ISS Safety Review Process. Likewise, NASA has defined a set of technical safety requirements to be implemented throughout the design of the ISS. These technical requirements are defined in SSP 50021, Safety Requirements for International Space Station Alpha. As amended by bilateral NASA and RSA agreements the technical intent of the safety requirements of SSP 50021 have been incorporated into SSP 41163, Russian Segment Specification.

1.1 PURPOSE AND SCOPE

The purpose of the NASA/ RSA safety review process is to define the methodology by which ISS will review and assess the safety of the RS flight elements and support equipment that will become part of the ISS. RS elements and ground support equipment that are used at KSC are also subject to the ISS safety review process. The safety of the Russian ground elements and support equipment that are used at Russian ground and launch facilities are the responsibility of RSA and are outside the scope of this document.

This process agreement describes the responsibilities of the organizations involved in the safety review process and the phase safety review meeting requirements.

The Soyuz and Progress vehicles are existing and proven designs, and as such, the scope of the safety review for those vehicles may differ from the other elements of the RS. Appendix A of this document specifies exceptions to the safety review process that are applicable to the Russian Vehicles (Soyuz and Progress).

2.0 APPLICABLE DOCUMENTS

SSP 50094 NASA /RSA Joint Specification/Standards Document for ISS Russian Segment

SSP 41163 Russian Segment Specification

2.1 REFERENCE DOCUMENTS

SSP 30599 Safety Review Process

SSP 50021 Safety Requirements for ISS

3.0 RESPONSIBILITIES

NASA is responsible for the overall integrated safety of the ISS. To successfully implement this responsibility compliance with the safety requirements must be assured within the ISS Program by the close coordination of a well structured phase safety review process with the formal ISS design review process. This coordinated review provides the mechanisms necessary to demonstrate that all hazards have been identified and once identified have been sufficiently controlled, eliminated or reduced by appropriate design features. At the completion of the safety review process there must be assurance that the residual risks are acceptable and that all hazard controls are properly verified. In consideration of the cultural differences in the NASA and Russian approaches to safety, the ISS safety review process has been adapted to review a modified version of Russian off-nominal situations (ONSs). This approach will enhance safety in that RSA will be able to utilize a safety tool with which it has experience and still satisfy the essential elements needed for a hazards analysis.

RSA has the responsibility to actively participate in this safety review process

4.0 ISS SAFETY REVIEW PROCESS

The objective of the ISS safety program is to achieve the maximum degree of safety consistent with ISS objectives and operational requirements while complying with NASA safety policy. The goal of the safety reviews in this process is to eliminate hazards through design modifications and to assure that all hazards and their causes inherent in the design have been identified and evaluated.

For hardware launched on Russian launch vehicles, existing Russian ground and launch safety processes will be used to assure safety of launch and delivery to planned orbit. The ISS flight safety review panel will assess the safety for all phases of the ISS program after delivery to planned orbit including operations of the ISS on orbit.

For hardware launched on Space Shuttle, the ground and launch safety process is ***TBD***.

Safety reviews are conducted to verify that RS design and operations comply with the ISS safety requirements.

4.1 SAFETY ANALYSIS AND DELIVERABLES

The process for conducting a safety review was established to evaluate the results from the safety analyses. The ISS safety analyses include, as a minimum, traditional hazards analyses. Performance of hazards analyses provides a means to systematically and objectively identify

hazards and hazard causes. For assessment of the safety of RS hardware, it has been determined that a modified version of Russian ONS analysis will satisfy the intent of a traditional hazards analysis. The ONSs to be considered are those that result in unsafe conditions or consequences which may have catastrophic effects on the ISS or result in crew injury. The form to report the ONSs is a modified NASA hazard Report (HR) form. A description of data fields of the ONS/HR form is included as an attachment to this document. These ONS/HR's shall include reference to appropriate supporting attachments that will enable the safety review panel to understand and properly interpret the safety features in the RS design that are referenced in the ONS/HR. A list of ONS/HRs related to critical consequences should also be submitted to assure that they have been properly categorized. The ONS/HRs will be submitted in accordance with the bilateral NASA/ RSA data exchange agreements. The ONS/HRs will be reviewed through the milestone review process and approved prior to release.

4.2 GENERAL REVIEW PROCESS FLOW

The phase safety review schedule is based upon the schedule of the major program milestone reviews. Phase safety reviews are scheduled for each stage on the Engineering Master Schedule (EMS). The ISS safety review meeting nomenclature to be used to identify the level of review is referred to as Phase I, II, and III, and corresponds to preliminary design review, critical design review, and design certification review. Three reviews are normally conducted for each stage. The depth and number of reviews is dependent on the complexity, technical maturity, and hazard potential of the equipment, and may be modified by the safety review panel in conjunction with RSA prior to the review.

Prior to all safety reviews with the ISS flight safety review panel, the RS AIT leads will review all safety assessments to assure that appropriate management accountability and to identify issues which need to be treated prior to the safety review. These issues will be reviewed by the safety panel as they are identified.

The content of each phase safety review (i.e., data requirements, content of the safety review meeting, and disposition of the HR/ONSs) is provided in section 5.0. The safety data are submitted 45 days prior to the review. Upon completion of the safety review the panel chairman will provide any major issues/items that could not be resolved within the panel to the ISS Program Manager.

NOTE: ISS payloads furnished by RSA, NASA or other IP for use in/on the RS elements or in other modules of the ISS are not reviewed by the ISS flight safety review panel as all experiments and payloads must be reviewed by a separate ISS payload safety review panel. The ISS flight safety review will only review the experiment rack to module integration.

4.3 PHASE SAFETY REVIEW MEETING

The minimum agenda for a phase safety review is defined in paragraphs 5.1.3. More than one stage may be reviewed at a single review. All actions generated at the review will be logged and tracked by a common action tracking system for ISS. A single set of actions and minutes are generated and sent to attendees.

4.4 PHASE SAFETY REVIEW OBJECTIVES.

The phase I safety review is the first formal meeting of the safety review panel in which the safety of RS equipment and operations will be addressed. The purpose of the meeting is to present to the panel the results of the safety assessments performed by RSA and report the results at the program design reviews. The panels will focus on: assuring that all hazards/ONSs and hazards/ONS causes inherent in the design have been identified; evaluating the means employed to control the hazard/ONS; and assessing the preliminary methods identified to verify all hazard/ONS controls.

The purpose of the phase II safety review is to assess the stage / increment design and operations to assure that all appropriate hazard/ONS controls have been implemented and that the means of verifying them has been identified in detail. The safety assessment shall be completed such that (1) all system level, assembly, operational, and interface hazards/ONSs and hazard/ONS causes have been identified; (2) a means for eliminating reducing or controlling the hazard/ONS has been defined and implemented; and (3) specific verification methods have been finalized and integrated with other ISS partners.

The purpose of the phase III safety reviews is to assess the stage/design and operation and to bring ONS/HRs to closure status in preparation for program management acceptance and mission stage/increment safety certification.

By the phase III safety review, the safety analysis and safety verification activities should be complete for the stage/increment to allow safety certification.

4.5 PROGRAM HAZARD REPORT ACCEPTANCE

Approval and closure of all ONS/HRs will be made through the ISS safety review panel. Signing of the individual ONS/HRs by the ISS flight safety review panel at the conclusion of the phase safety review signifies that the ONS/HR is at the maturity of the level of the review and that the safety review panel concurs with/approves the hazard/ONS data contained therein.

4.6 SAFETY REVIEW DATA SUBMITTALS

The required safety review data shall be submitted 45 days prior to the scheduled safety review meeting. The safety data required for each phase safety review is to be submitted to the following individual:

Launch Package Russian Segment Integrated Product
Team Manager
International Space Station Program Office
Mail code OB
NASA/JSC
Houston, TX 77058

SSP 50146, Revision B

A signed original of each ONS/HR must be available to the safety review panel for signature at the time of each review. Only one copy of each deliverable must be sent to the addressee.

5.0 PHASE SAFETY REVIEW

5.1 PHASE I SAFETY REVIEW

The phase safety review is the first formal meeting between the ISS contractors, International Partner organizations, and the ISS safety review panel. The focus of the meeting is on identifying hazards/ONSs and hazard/ONS causes inherent in the preliminary design, evaluating the means of eliminating, reducing, or controlling the hazard/ONS and establishing a preliminary method for safety verification. NOTE: Where the text in section 5 refers to "hazard," the term "hazard/ONS" may be substituted.

5.1.1 PHASE I DATA REQUIREMENTS

- a. Deleted
- b. Flight System Design and Operations
 1. Description of the system, element, or support equipment and associated operations, including baseline description of on-orbit assembly, on-orbit operations, and start-up sequence. Description of the stage configurations including conceptual description of on-orbit assembly and manned operations.
 2. Summary descriptions, schematics/block diagrams of safety-critical subsystems and their operations, including schematics and block diagrams with safety features, inhibits, etc., identified.
 3. Deleted
 4. Flight ONSs and appropriate support data (see paragraph 5.1.2).
 5. A summary listing of safety-critical services provided by other ISS segments or the Orbiter and used to control and/or monitor hazards.

5.1.2 PHASE I OFF-NOMINAL SITUATION/HAZARD REPORTS

A Phase I ONS shall be prepared for each hazard identified as a result of the safety analysis on the preliminary design and operations.

The responsible safety manager shall sign and date each ONS before submittal into the process.

Critical procedures/processes, which require special monitored verification, shall be identified in preliminary fashion. For hazards controlled by "design to minimum risk," the following is a suggested set of support data. If the following data is provided to other NASA/RSA technical review teams, it need not be resubmitted to the safety review panel. No additional reports will be required if joint technical teams have reviewed the design and conclude that the data exchange is sufficient. However, appropriate references to the submittal of the data and to the joint technical

team which reviewed the data should be stated on the ONS/HR. The following is a list of selected subsystems that can be treated as “design to minimum risk.”

- a. Unpressurized Structures.
 - 1. Fracture Summary Report in accordance with SSP 50094.
- b. Pressurized Systems.
 - 1. Fracture Summary Report in accordance with SSP 50094.
 - 2. Summary of results of verification tests/analyses.
- c. Pyrotechnic Devices:
 - 1. Summary of results of verification test/analyses.
- d. Materials:
 - 1. Flammability assessment.
 - 2. JSC Form 44, if required - update.
- e. Components and elements of mechanisms in critical applications.
 - 1. Summary of verification results.

5.1.3 PHASE I/II/III SAFETY REVIEW MEETING AGENDA ITEMS

The agenda for each of the safety meetings shall consist of the following:

- a. Title of meeting.
- b. Introduction.
- c. Purpose of meeting.
- d. Status of pre-review activities, as applicable.
- e. A design and operations overview, including a description of all safety-critical subsystems.
- f. Detailed presentation of ONS/HRs (and NCRs if applicable).
- g. A summary of safety-related failures (or problem reports), accidents, and significant technical issues.
- h. Presentations of any proposed nonconformances.

SSP 50146, Revision B

- i. Status of safety review meeting action items.
- j. Panel's disposition of ONS/HRs in accordance with paragraph 5.1.4.
- k. Verification tracking log status (phase III).
- l. Concluding remarks.

5.1.4 OFF-NOMINAL SITUATION/HAZARD REPORT DISPOSITION

After a technical discussion is held, the panel chairs provide a disposition of the ONS/HRs. Action items are assigned by panel chairs and the list of action items signed by the panel chairmen. The disposition may take one of these forms:

- a. Recommend approval as written.
- b. Recommend approval with changes.
- c. Recommend approval with an action to be performed by the responsible organization.
- d. Recommend disapproval with an action to be performed by the responsible organization.

5.2 PHASE II SAFETY REVIEW

The purpose of the Phase II safety review is to present to the panels the updated ONS/HRs that reflect the completed design and operations of RS equipment. The HR/ONSs shall be completed such that (1) hazards/ONSs and hazard/ONS causes have been identified, (2) a means for eliminating, reducing, or controlling the hazard/ONS has been defined and implemented, and (3) specific safety verification methods (i.e., test plans, analysis, and inspection requirements, etc.) have been finalized. Interfaces to be assessed shall include those between the Russian Segment and the USOS and among the various elements and distributed systems that comprise the Russian elements of the stage configuration. Newly identified hazards/ONSs shall be documented in additional ONS/HRs.

5.2.1 PHASE II DATA REQUIREMENTS

The following data is required for the Phase II safety review:

- a. DELETED
- b. Flight System Design and Operations.
 - 1. Updated Contractor End Item or Space Station Control Center (SSCC) description, mission scenario. Individual increment phase descriptions as well as assembly, and nominal operations descriptions.

2. Updated schematics and block diagrams of safety-critical subsystems and their operation with safety features and inhibits. (Defined electrical schematics must clearly indicate the required number of inhibits or controls to establish their independence).
3. Status of action items assigned during Phase I safety review.
4. Updated summary listing of critical services provided by other IP segments or the Orbiter that are used to control and/or monitor hazards.
5. Engineering drawings of safety critical subsystems
6. ONS/HRs and appropriate support data (see paragraph 5.2.2).
7. A list of safety-related failures and accidents.
8. A list of hazardous procedures (excluding ground processing).

5.2.2 PHASE II HAZARD REPORTS

The Phase II ONS/HRs shall be prepared by updating hazards/ONSs identified, providing new hazards/ONSs to reflect the completed equipment design and flight/ground operating procedures. If the equipment design is changed from Phase I to Phase II such that a Phase I ONS/HR may be deleted, a brief statement of rationale for deleting the report shall be presented in the Phase II assessment report.

All current changes to the ONS/HRs are to be identified by a bar in the right-hand margin. The submitting organization's safety manager shall sign and date each ONS/HR before submittal.

All critical procedures/processes must be addressed, including the plan for verification. For hazards controlled by "design to minimum risk," the following is a suggested set of support data in addition to that provided for phase I. If the following data is provided to other NASA/RSA technical review teams, it need not be resubmitted to the safety review panel. No additional reports will be required if joint technical teams have reviewed the design and conclude that the data exchange is sufficient. However, appropriate references to the submittal of the data and to the joint technical team which reviewed the data should be stated on the ONS/HR. The following is a list of selected subsystems that can be treated as "design to minimum risk."

- a. Unpressurized Structures.
 1. Fracture Summary Report in accordance with SSP 50094.
 2. Summary of design loads derivation leading to critical load cases.
 3. Math model verification plan.
- b. Pressurized Systems.

1. Fracture Summary Report in accordance with SSP 50094.
 2. Summary of results of verification tests/analyses.
 3. Qualification and acceptance test plan.
- c. Pyrotechnic Devices:
1. Summary of results of verification test/analyses.
- d. Materials:
1. Flammability assessment.
 2. JSC Form 44, if required - update.
 3. Fluids compatibility analysis.
- e. Components and elements of mechanisms in critical applications.
1. Summary of verification results.

5.3 PHASE III SAFETY REVIEW

The purpose of the Phase III safety review is to obtain approval of the completed ONS/HRs and the remainder of the safety compliance data. The Phase III review provides the final assessment of equipment and operational compliance with SSP 41163 safety requirements.

5.3.1 PHASE III DATA REQUIREMENTS

The following data is required for the Phase III safety review:

- a. DELETED
- b. Flight System Design and Operation
 1. TBD PYROTECHNIC DATA.
 2. Final Contractor End Item or Space Station Control Center (SSCC) description, mission scenario. Individual increment phase descriptions as well as assembly, and nominal operations descriptions.
 3. A final summary listing of safety-critical services provided by other IPs or the Orbiter and an explanation of services used to control and/or monitor hazards.
 4. Final schematics and block diagrams of safety-critical subsystems and their operation.
 5. HRs and appropriate support data (see paragraph 5.3.2).
 6. Engineering drawings of safety critical subsystems when specifically requested.

7. Listing of waiver/deviation requests to safety related requirements. A signed copy of each approved waiver and deviation shall be included. (See paragraphs 6.0).
8. A summary of all safety related failures and accidents.
9. Closure of action items assigned during the Phase II safety review.
10. ISS Safety Verification Tracking Log (for flight hardware only) in accordance with Appendix C.

5.3.2 PHASE III HAZARD REPORTS

The Phase III ONS/HRs shall reflect the as-built design and operations of the equipment design and operation. Ideally, by Phase III, all safety analysis efforts are completed. The RSA shall update the Phase II ONS/HRs to (1) reflect this final equipment design and operations, and (2) document the status and results of all completed verification work. All open verifications must be listed on a safety verification tracking log. This log allows the panel chairmen to sign the ONS/HRs indicating completion of the safety analyses, but with the understanding that approval for flight will be withheld until all verification activity is complete. Approval for flight will not be withheld for open verification activities that are part of nominal on-orbit activation activities, but failure to successfully accomplish these activities on orbit may constrain subsequent on-orbit operations. Open ground and flight verifications that have been identified as a constraint against ground processing must be closed before the applicable ground operation can be performed.

Instructions for completion of Phase III ONS/HR forms are contained in Appendix B. All changes to the ONS/HRs since Phase II should be indicated by a bar in the right-hand margin. The applicable safety manager (RSA, RSC-E or KhSC) and program manager shall sign and date each ONS/HR before submittal to the panel. For hazards controlled by “design to minimum risk,” the following is a suggested set of support data in addition to that provided for phase I and II. If the following data is provided to other NASA/RSA technical review teams, it need not be resubmitted to the safety review panel. No additional reports will be required if joint technical teams have reviewed the design and conclude that the data exchange is sufficient. However, appropriate references to the submittal of the data and to the joint technical team which reviewed the data should be stated on the ONS/HR. The following is a list of selected subsystems that can be treated as “design to minimum risk.”

- a. Unpressurized Structures.
 1. Fracture Summary Report in accordance with SSP 50094.
 2. Summary of design loads derivation leading to critical load cases.
 3. Math model verification plan.
- b. Pressurized Systems.
 1. Fracture Summary Report in accordance with SSP 50094.

SSP 50146, Revision B

2. Summary of results of verification tests/analyses.
 3. Qualification and acceptance test plan.
- c. Pyrotechnic Devices:
1. Summary of results of verification test/analyses.
- d. Materials:
1. Flammability assessment.
 2. JSC Form 44, if required - update.
 3. Fluids compatibility analysis.
- e. Components and elements of mechanisms in critical applications.
1. Summary of verification results.

5.4 POST PHASE III SAFETY ACTIVITY

When changes to the design or operation of a stage are required subsequent to the Phase III safety review but prior to launch, the ISS participants shall assess those changes for possible safety implications, including their effect on all interfaces. The assessment shall be forwarded to the panel for approval. New or revised ONS/HRs and support data shall be prepared where applicable and also submitted for review. If the safety of the stage is affected, the need for a Delta safety review is determined by the safety panel chairmen.

6.0 NONCOMPLIANCE WITH SPACE STATION REQUIREMENTS

Elements of the RS shall meet all the applicable safety requirements or obtain specific approval for each case of noncompliance. The applicable safety requirements for the RS are those requirements of SSP 41163 Russian Segment Specification paragraph 3.3.6 and other than 3.3.6 safety requirements.

When the design of RS hardware or its operations do not comply with an applicable safety requirement, a safety noncompliance report (NCR) form,(see attachment), shall be submitted to obtain approval of the noncompliance condition. This form shall be signed by the RS safety manager and other RS managers as appropriate.

After submittal by RSA, the NCR shall be initially reviewed and concurred in by the SRP, Safety IPT, and Safety and Mission Assurance IPT. The concurred in NCR will be forwarded to SSIPT to obtain ISS Program Manager approval as a request for a waiver or deviation in accordance with Bilateral NASA/RSA configuration management requirements.

Note: RSA will participate in the NCR process for USOS NCR's by their participation in the ISS Safety Review Panel. In addition, NCR's that are approved by the Safety Review Panel will, in most cases, result in a waiver or deviation which will be processed in accordance with Bilateral NASA/RSA configuration management requirements.

SSP 50146, Revision B

ISS SAFETY NONCOMPLIANCE REPORT

TITLE:

Enter a brief title and tracking number for the NCR.

SYSTEM/ELEMENT:

Specify the segment, system, and /or end item that relates to the hardware to which the NCR is applicable.

APPLICABLE SAFETY REQUIREMENT:

Specify the applicable safety requirements that relate to the NCR. These are the requirements from SSP 41163

DESCRIPTION OF NONCOMPLIANCE:

Describe the specific design feature or operational capability of the hardware that does not meet the safety requirements. Clearly correlate the noncompliance condition to the safety requirement.

HAZARD OR HAZARD CAUSE:

Describe the hazard or hazard cause that relates to the noncompliance. A brief description with a reference to an ISS hazard report for additional detail is preferred.

REASON REQUIREMENT CAN NOT BE FULFILLED:

Describe the technical reasons why the requirement can not be met.

RATIONALE FOR ACCEPTANCE:

Describe the rationale for acceptance of the noncompliance condition. Rationale demonstrating safety features of the design Rationale that mitigates the safety risks such as results of testing, / analysis, or inspections shall be specified. Other relevant information that may be provided as appropriate includes time of exposure to the hazard, factors that may limit the severity of the hazard, or factors that may limit the probability of occurrence.

Cost and schedule impacts for design changes that may be necessary to correct the noncompliance condition may be included if known.

SUBMITTED BY:

ORGANIZATION: _____ DATE _____

CONCURRENCE:

ISS SAFETY REVIEW PANEL _____ DATE _____

APPROVAL:

ISS PROGRAM MANAGER _____ DATE _____

7.0 SIMILAR EQUIPMENT

"Similar Equipment" is hardware/software which is of the same or similar design to hardware/software which has been previously certified by the flight safety review panel for its safety. Variances to the basic procedures of paragraph 5.0 have been developed for similar equipment to eliminate unnecessary duplication of effort from previously accomplished safety activity.

The user of the similar equipment(i.e., NASA or RSA) is responsible for the safety of the similar equipment and associated interfaces. To fulfill this responsibility, the user shall assess the previously approved safety data of the similar equipment for applicability to the new application and make all appropriate changes. The number and depth of the phase safety reviews to be conducted to assess similar equipment should be discussed at an early safety review meeting.

The following unique data for the similar equipment shall be submitted:

- a. Identification of all similar equipment to be used and the baseline safety analyses.
- b. Assessment of each similar equipment to indicate that the proposed use is the same as that analyzed and documented.
- c. New or revised ONS/HRs, additional data, and identification of deleted ONS/HRs. Identification and assessment of changes in hardware/software and operations which have safety impact.
- d. An assessment of the safety verification methods contained in the baseline safety analysis to determine which verification must be re-accomplished.
- e. A list and description of safety noncompliances including the acceptance rationale for each.
- f. Assessment of all failures and anomalies during previous usage of the similar element with corrective action taken and rationale for extended use.
- i. Unique flight article data required by paragraph 5.3.1, item b.1.
- j. Ionizing radiation data sheet for each source (JSC Form 44) as applicable.

APPENDIX A: Amendments to the “NASA/RSA Safety Review Process for ISS,” applicable to Soyuz and Progress Vehicles

A.1.0 INTRODUCTION

This Appendix lists specific deviations to the "NASA/RSA Safety Review Process for ISS," applicable to the existing designs of the Soyuz and Progress vehicles.

A.1.1 PURPOSE

Because the Soyuz and Progress are existing vehicles, differences in the applicability of the Safety Review Process defined in the "NASA/RSA Safety Review Process for ISS," exist. These differences are detailed in this Appendix, and the appendix will become a part of "NASA/RSA Safety Review Process for ISS".

A.1.2 SCOPE

The "NASA/RSA Safety Review Process for ISS" applies to the entire RS, including the Soyuz and Progress; however, exceptions to this process are required for these vehicles. This Appendix describes exceptions to the "NASA/RSA Safety Review Process for ISS" and applies only to the Soyuz and Progress vehicles that are existing designs and will be used as a part of the ISS.

A.2.0 SAFETY REVIEW REQUIREMENTS

A.2.1 INTERNATIONAL SPACE STATION ALPHA SAFETY REVIEWS

The following three paragraphs modify the scope of the safety review for the Soyuz and Progress vehicles. It is agreed to modify paragraph 4.0 in the "NASA/RSA Safety Review Process for ISS" for the Soyuz and Progress only.

The objective of the ISS safety program is to achieve the maximum degree of safety consistent with ISS objectives and operational requirements. The goal of the safety reviews in this process is to eliminate hazards and to assure that all hazards and their causes inherent in the design have been identified and evaluated. For existing RS Russian Vehicles (Soyuz and Progress) NASA and RSA shall implement the Safety Review Process defined in the "NASA/RSA Safety Review Process for ISS" with the following reduced scope:

- a. Hazards to the ISS caused by any ISS vehicle that is temporarily in the proximity of or docked to the ISS must be identified and controlled. This excludes hazards associated with autonomous flight of these vehicles (i.e., launch operations, orbit insertion, deorbit, and landing, etc.).
- b. Hazards resulting from the inability of the vehicles to perform critical ISS functions.

A.2.2 PHASE SAFETY REVIEWS

For the Soyuz and Progress, three formal reviews have been scheduled to assess functional capabilities.

A.2.3 LEVELS OF DESCRIBING OFF-NOMINAL SITUATION/HAZARD

The level of describing the ONS/Hazard and level of subsystem analysis are determined by the ONS/Hazard category, either Catastrophic or Critical, and the complexity of the system.

A.2.4 POST PHASE III SAFETY ACTIVITY

The results of the Phase III safety review are documented by the Safety Review Panel and presented to Program Management.

A.2.4.1 CHANGES IN THE DESIGN OR OPERATION AFFECTING THE ISS

When changes to the design or operation of the vehicle are required subsequent to the Phase III safety review, the designing organization shall assess those changes for possible negative safety implications, including their effect on all interfaces. When this assessment shows hazardous effects in the scope defined in paragraph 2.1 of this appendix, the assessment shall be forwarded to the panel for approval. The data on changes to the design and operation of a vehicle affecting safety reports shall be submitted after approval of the modifications by the designing organization authorities, but no later than 180 days prior to launch of the first modified vehicle. New or revised ONS/HRs and support data shall be prepared where applicable and also submitted for review. If the safety of the vehicle is negatively affected, the need for a additional safety review is determined by the safety review panel chairmen.

A.2.4.2 CHANGES THAT DO NOT AFFECT THE ISS

When changes to the design or operation of the stage are required subsequent to the Phase III safety review, the designing organization shall assess those changes for possible safety implications, including their effect on all interfaces. When this assessment shows no hazardous effects on the ISS, submittal of additional hazard reports to the ISS Safety Review Panel are not necessary.

A.2.4.3 SAFETY REVIEW FOR THE FIRST LAUNCH

The safety review process will be held only for the first launch of the Soyuz and Progress vehicles. Subsequent launches of Soyuz and Progress vehicles will be assessed for flight readiness according to normal RSC-Energia processes. If significant modifications to the Soyuz or Progress vehicles are made after the first or subsequent launches, paragraphs 2.4.1 and 2.4.2 above will be applied.

APPENDIX B: INSTRUCTIONS FOR ISS HAZARD REPORT FORM

B.1 SCOPE

The information required to complete a ISS Hazard Report form is defined herein. The ISS Hazard Report Form (Figure B.1) and hazard report legend will be used as the standard form for all ISS equipment. ISS IPs may use an equivalent form as long as the form contains the same content fields as the ISS form.

B.2 SUPPORT DATA

Each HR should stand alone. Data required to understand the hazard, the hazard controls, and the safety verification methods should be attached to the report. Examples of such data include block diagrams, descriptions of the applicable flight/support system and its operation, a listing of the sequence of events, a list of critical procedures/processes that require special verification, and summaries of proposed tests or test results. When functional diagrams or schematics are supplied, the pertinent information shall be clearly identified (e.g., controls, inhibits, monitors, etc.).

B.3 APPROVAL

The ISS HRs will be approved in accordance with paragraph 4.5. The appropriate management personnel must sign and date the hazard report to signify agreement with the content prior to its submittal to the safety panel. During the phase safety review, the safety review panels will evaluate each HR. The panel chairman will provide a disposition for each HR.

SSP 50146, Revision B

FIGURE B.1 ISS HAZARD REPORT/OFF-NOMINAL SITUATION FORM

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:

7. REMARKS:

SSP 50146, Revision B

8. SUBMITTAL CONCURRENCE:**(a) Russian Segment:**

Safety ManagerDate

Program Manager

9. APPROVAL:**(a) Safety Review Panel**

Panel ChairmanDate

Panel ChairmanDate

(b) For Phase III (ONLY)

NASA Manager, Space Station ProgramDate

SSP 50146, Revision B

Hazard Report Number Cause 1

1. HAZARD CAUSE DESCRIPTION:

SEVERITY: LIKELIHOOD: (Phase II/III)

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:

5. MISSION PHASE(S):☐ Launch Processing: (KSC launch only)☐ Launch: (KSC launch only)☐ 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. REFERENCE:

10. POINT OF CONTACT:

Name:

Telephone:

Hazard Report Number

SSP 50146, Revision B

Cause 2**1. HAZARD CAUSE DESCRIPTION:****SEVERITY: LIKELIHOOD: (Phase II/III)****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:

5. MISSION PHASE(S):☐ Launch Processing: (KSC launch only)☐ Launch: (KSC launch only)☐ 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. REFERENCE:****10. POINT OF CONTACT:****Name:****Telephone:**

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 ISS 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) and II (Critical) as referenced in RS Specification, SSP 41163 and Table B.1 below.

TABLE B.1: Table of Hazard Cause Severity

Catastrophic	I	Any condition which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the orbiter, ISS or major ground facility. Loss of ISS: Loss of the ISS is to be limited to those conditions resulting from failures or damages to elements in the critical path of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.
Critical	II	Any condition which may cause a non-disabling personnel injury, severe occupational illness; loss of a ISS 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 ISS 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.

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 B.2, Likelihood of Occurrence. This field is applicable to Phase II and III only.

TABLE B.2 TABLE OF LIKELIHOOD OF OCCURRENCE OF HAZARD CAUSES

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.

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. For Phase I identify the types of tests, analyses, or procedures (e.g., vibration testing, fracture analysis) to be used to verify the hazard control.

For Phase II update each method to refer to specific test (or analysis) procedures and summary of criteria to be used.

For Phase III all safety verifications should be completed. The verification method is updated to reflect any changes made after the CDR review.

4. SAFETY REQUIREMENT(S): Identify the requirements in SSP 41163 that will be addressed by this cause. Other engineering design requirements used for controls shall also be identified.

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.

SSP 50146, Revision B

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

Launch covers the time period from T-0 through orbital insertion (KSC launch only).

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 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, from the on-orbit stage, through final disposal of the elements.

6. PROGRAM STAGES: Using the ISS 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. REFERENCE: Provide numbers of reference documents used to support the hazard cause, if any reference documents are available.

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

APPENDIX C: Instructions for Developing a Safety Verification Tracking Log (Applicable to Phase III only)

C.1 SCOPE

This appendix describes the usage of the ISS safety verification tracking log (Figure C.1), and provides instructions for its completion.

C.2 USAGE

The verification tracking log is used to formally document and status the work that is not completed at the time the final safety assessment report is prepared. (All completed verification work is documented on the appropriate hazard reports.) These verification requirements will be acted on in accordance with the process described in the Program Master Verification Plan. If all activities associated with the safety analyses (other than the open verification) are completed, the panel chairmen may sign the hazard reports indicating panel acceptance of the safety work, but with the understanding that final approval of the hazard is not complete until the HR is baselined and all applicable verification activity is completed. Items requiring on-orbit verification will be incorporated in approved assembly and checkout procedures. The procedure numbers will be referenced in the Log.

C.3 INSTRUCTIONS

Instructions for the completion of the ISS Safety Verification Tracking Log are as follows:

- a. Title - the title is used to identify whether the tracking log is for a mission or a specific equipment verification.
- b. Page - the specific page number followed by the total number of pages.
- c. Element - the name of the element, experiment, etc.
- d. Date - date completed or updated.
- e. Log Number - an alphanumeric designation used to identify and track each verification item. These designations will be assigned by the project organization when the log is first submitted.
- f. Hazard Report Number - the number of the hazard report containing the verification item.
- g. Description Verification Number - The number from the applicable hazard report (Safety Verification Method block) for the specific verification item.
- h. Description - the specific verification remaining open. Procedures will be identified by number and title.
- i. Operation(s) Constrained - the specific operation(s) that this verification is a constraint against. Closure of this verification item must be accomplished before the listed, operation(s) can be performed.
- j. Independent Verification Required (Yes/No) - The need (yes/no) for an independent verification of the specific item.
- k. Scheduled Date - the planned date for completion of the verification.
- l. Completion Date - the date this verification was completed.
- m. Method of Closure/Comments/Verification Completion Notice (VCN)- the method by which this open verification has been confirmed closed, and additional information or remarks.

SSP 50146, Revision B

Figure To be provided.

Figure C.1 Safety Verification Tracking Log

APPENDIX D: ABBREVIATIONS AND ACRONYMS

AIT	Analysis and Integration Team
CR	Change Request
EMS	Engineering Master Schedule
e.g.	Example
etc.	Etceteras
HR	Hazard Report
IP	International Partner
ISS	International Space Station Alpha
JSC	Johnson Space Center
KSC	Kennedy Space Center
NASA	National Aeronautical and Space Administration
ONS	Off-Nominal Situation
RS	Russian Segment
RSA	Russian Space Agency
S&MA	Safety and Mission Assurance
SSCB	Space Station Control Board
SSCC	Space Station Control Center
SSP	Space Station Program
TBD	To Be Determined
USOS	United States On-orbit Segment
VCN	Verification Completion Notice

SSP 50146, Revision B

ATTACHMENT D

NASA/RSA GENERAL PRINCIPLES AND REQUIREMENTS FOR ISS CARGO SAFETY

ATTACHMENT D**NASA/RSA GENERAL PRINCIPLES AND REQUIREMENTS
FOR ISS CARGO SAFETY*****Table of Contents***

	<u>Page</u>
D.1 Purpose	D-3
D.2 Scope	D-3
D.3 General principles of the procedure for conducting a cargo safety analysis	D-6
D.4 Contents of ISS cargo flight safety certificates	D-9
Figure 1. Safety Certificates	D-4
Figure 2. ISS Cargo Operations	D-5

ATTACHMENT D**NASA/ROSAVIAKOSMOS GENERAL PRINCIPLES AND REQUIREMENTS
FOR ISS CARGO SAFETY****D.1 Purpose**

This document states Rosaviakosmos and NASA's agreement on the procedure for developing the necessary cargo safety documents, on the methods for performing safety reviews, on the technical safety requirements and on the accepted format of safety documents.

D.2 Scope

D.2.1 This document applies only to NASA cargo transported on Russian transport vehicles, NASA cargo stowed or operated on the ISS Russian Segment, Russian cargo transported on the Shuttle in pressurized compartments or in the payload bay, and Russian cargo stowed and operated on ISS.

D.2.2 The term "cargo" refers to all types of hardware stowed on a transport vehicle or module but not needed for its functionality, e.g. hardware transferred, stowed and operated on or removed from ISS. "Cargo" also relates to hardware items removed from service systems of the modules to be stowed, disposed of, or returned to the ground. Cargo items include scientific equipment (experiments), logistics, crew psychological support items, tools, spare instruments and assemblies, etc. Waste is also classified as cargo, and a definition and categorization of waste items are contained in document SSP 50481 "Management Plan for Waste Collection and Disposal".

Functionally, ISS cargo is subdivided into experiments and logistics cargo (MTO). Experiments include scientific and engineering devices and assemblies, ancillary devices, support systems, equipment for engineering tests, etc. Logistics cargo (MTO) encompasses resupply cargo, module service system spare parts (ЗИП), repair equipment, containers with consumables, etc.

Hardware components removed from vehicle systems for stowage, disposal or return become cargo after disassembly is complete.

The cargo ceases to be considered cargo after it is returned to Earth or is deorbited.

Logistics cargo is no longer cargo after it is used or included as a component of the module's service systems or structure.

The manifest (SSP 54101 Annex 1) identifies the list of cargo items for a specific transport vehicle.

A diagram of operations performed with ISS cargo is presented in Figure 2-1.

D.2.3 Cargo safety is reviewed through Safety Data Packages (SDPs)

The basic required elements of a safety data package are:

- Safety Certificate (except for NASA experiments stowed or operated in the Russian Segment)
- Standardized Hazard Control Report for experiments and Category 1 Cargo Hazard List for other cargo
- Unique Hazard Reports (for cargo in category 2)
- Additional Information Required For Safety Review Panels, on Design and Flight Operations, etc.

The certificate indicating that the given cargo meets safety standards is the final document confirming cargo safety.

The scope of Safety Certificates is shown in Figure 2-2.

ISS CARGO OPERATIONS

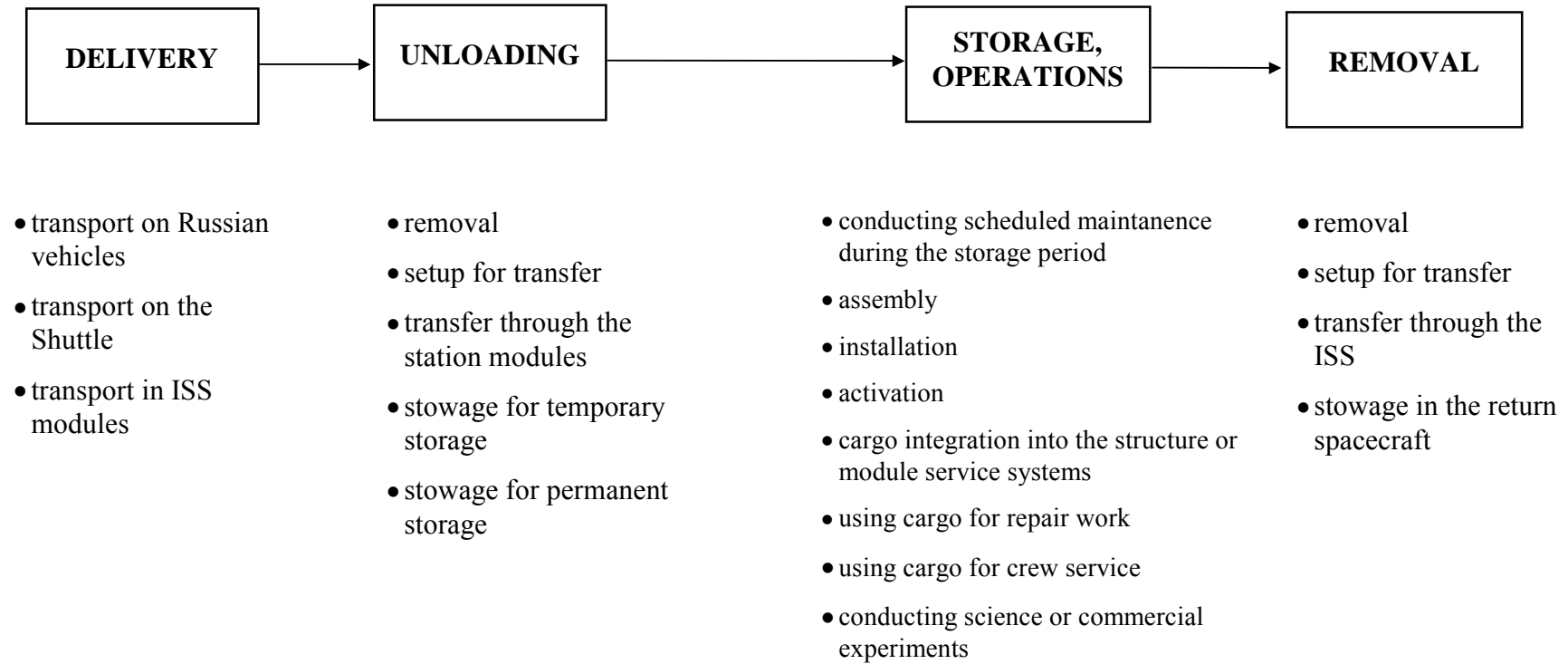


Figure 2-1

Figure 2-2. Safety Certificates

1. Safety certificate is required in order to stow cargo in a transport vehicle or to transfer to Station.
2. Reflight hardware safety is confirmed by a reflight letter referencing a previously issued certificate.
3. Phase 1 (NASA/Mir) transportation safety certificates may be used as a basis for reflight safety assessment for the ISS Program if initial assessment conditions are still valid.
4. Safety assessment of experiments includes operations.

?	Purpose [type] of cargo	Transport certificate addresses			Operation certificate addresses	
		<ul style="list-style-type: none"> • Stowage • Flight to station 	<ul style="list-style-type: none"> • Unloading • Stowage on station 	<ul style="list-style-type: none"> • Return • Disposal 	<ul style="list-style-type: none"> • Stowage • Installation • Disassembly 	<ul style="list-style-type: none"> • Station operations
1	Resupply & outfitting items	Y	Y	Y	Y	Y/N*
2	Spare parts, tools and accessories	Y	Y	Y	N **	Y/N*
3	Consumables for hardware	Y	Y	Y	Y	Y/N
4	Repair hardware and tools	Y	Y	Y	Y	Y
5	Experiments and consumables	Y	Y	Y	Y	Y
6	Objects and consumables for crew use	Y	Y	Y	Y/N	Y
7	Waste			Y***	Y***	

* The safety of the cargo as a part of the module is reviewed in module Hazard Reports. Modified or newly-designed resupply and outfitting items, spares, tools and accessories will require new or modified module Hazard Reports or SDPs.

** Operations is responsible for the necessary crew procedures.

*** For waste placed according to SSP 50481 into certified containers, a separate safety certificate is not required. Waste which does require safety certification shall be certified for transportation and for stowage if needed.

D.3 General principles of the procedure for conducting a cargo safety analysis

D.3.1 The responsibility of the partners for safety reviews of station modules is examined in detail in Section 2 of the main document. In addition to the main document, this document defines the responsibility of the U.S. and Russian sides when analyzing cargo safety, in accordance with which:

D.3.1.1 The term “Safety Panel” used in this Attachment refers to the NASA Payload Safety Review Panel (PSRP), Station Safety Review Panel (SRP)/Safety and Mission Assurance Review Team (SMART), Ground Safety Review Panel (GSRP), or the RSC Energia Safety Panel, as appropriate.

D.3.1.2 The RSC Energia Safety Panel conducts safety reviews of U.S. cargo being transported on Russian transport vehicles, and U.S. cargo to be stowed and/or operated on the Russian Segment. The Safety Panel shall review the Safety Data Packages and return comments to the supplying side in a timely manner to support any necessary modifications. The RSC Energia Safety Panel reviews the safety for the Russian Segment of US experiments conducted on the US Segment. The RSC Energia Safety Panel also reviews an integrated safety analysis of the transfer, stowage and operation within the ISS Russian Segment of cargo delivered by transport vehicle. Usage of cargo items on the Russian Segment may be implemented only after approval by RSC Energia.

D.3.1.3 NASA Safety Panels conduct safety reviews of Russian cargo being transported on the Shuttle and Russian cargo being operated or stored on the ISS. The Safety Panel shall review the Safety Data Packages and return comments to the supplying side in a timely manner to support any necessary modifications. The panels also take into account the results of the RSC Energia Safety Panel’s review of NASA SDPs for cargo to be stowed or used on the Russian Segment. Experiment safety is reviewed by the PSRP, while the SRP reviews the safety of the remaining cargo. These safety panels inform the Russian side about the decisions made as a result of comments presented by the Russian side. These panels also review integrated safety analyses of the transfer, stowage and operation within the ISS of cargo delivered by transport vehicle.

D.3.1.4 The sides provide each other, in the Safety Data Packages, hazard controls associated with cargo elements during translation, stowage and operations both internal and external to the module.

D.3.1.5 In view of the fact that ISS common air parameters are primarily maintained by the Russian Segment Life Support Systems, the estimated offgassing load for the complete hardware complement shall be submitted by the U.S. side to the Russian side of the Joint Environmental Team by L-3 months.

D.3.1.6 Safety review of the design of ground support equipment and ground processing operations for cargo prelaunch processing and post landing processing that occurs at launch and landing processing sites is addressed in Attachment TBD.

D.3.2 Rosaviakosmos and NASA management have given the JARSWG the task of managing communications in support of the safety review process, and the coordination and implementation of actions in support of the Safety process.

D.3.3 The cargo safety analysis and the volume of information presented for this analysis are dependent upon the cargo complexity and hazard level. Detailed requirements for data submittals and reviews for experiments are levied in Revision C of NSTS/ISS 13830 sections 6 and 7 (and TBD sections).

D.3.3.1 Cargo, except for U.S. experiments, is subdivided into two categories depending upon the potential hazards (for flight only); separately-delivered hardware for U.S. experiments is also divided into the given categories:

Cargo category definitions

Category 1 – Cargo items in this category typically present lower risks with well understood hazards and hazard controls. Cargo is certified as Category 1 cargo if it has potential hazards only in the areas indicated on the Category 1 Cargo Hazard List, JSC Form 907 or for experiments the Standardized Hazard Report, JSC Form 1230R. The following constraints also apply to Category 1 cargo:

1. The cargo may not have an electrical interface with the electrical power distribution system of the receiving side’s segment/vehicle.

SSP 50146, Revision B

2. The cargo may not contain software which could create a hazard via interface with the onboard control software.
3. The cargo may not contain biological or toxic substances or alcohol.

The safety of Category 1 cargo is certified by a Category 1 safety certificate (JSC Form 906). The certificate is signed by the cargo developer/curator, the JARSWG Co-chair, and the Program Manager of the supplying side (or his designee).

Additionally developed documents are: Category 1 Cargo Hazard List (JSC Form 907, see paragraph D.4.6) or, for Russian experiments, Standardized Hazard Control Report (JSC Form 1230R). The following documents are sent to the receiving side: certificate (JSC Form 906) and Standardized Hazard Control Report (JSC Form 1230R).

If the receiving side agrees that all applicable hazards are addressed, the Category 1 certificate, and JSC Form 1230R for Russian experiments, is approved and the receiving side informs the supplying side in written form.

Category 2 – Cargo items in this category typically present a moderate or high risk and have unique hazards, which are outside the scope of JSC Form 907 or for Russian experiments the Standardized Hazard Report, JSC Form 1230R. These hazards are documented in unique hazard reports.

Experiment items of this category will follow the process documented in NSTS/ISS 13830 Revision C, section 5. The first safety review for cargo items in this category is required at the Design Review stage as a minimum. The number of phase reviews required depends upon the complexity of the cargo. When possible, such reviews will be conducted via telecon.

The safety of Category 2 cargo is certified by issuing a Category 2 safety certificate (JSC Form 906). The certificate is signed by the cargo developer/curator, the JARSWG Co-Chair, and the Program Manager (or his designee) of the supplying side.

Additionally developed documents are: Category 1 Cargo Hazard List (JSC Form 907, see paragraph D.4.6) or, for Russian experiments, Standardized Hazard Control Report (JSC Form 1230R). The following documents are sent to the receiving side: certificate (JSC Form 906), Standardized Hazard Control Report (JSC Form 1230R) and any applicable unique Hazard Reports, signed by the supplying side. Unique Hazard Reports are approved by the Safety Review Panel of the receiving side and the receiving side informs the supplying side in written form.

TBR: Active and Especially Hazardous Cargo; NASA considers that it is necessary to develop criteria for Active and Especially Hazardous Cargo and to develop a process for it similar to Attachment C of SSP 50146.

D.3.3.2 All U.S. experiment cargo will follow the process as documented in NSTS/ISS 13830 Revision C. Technical requirements shall be in accordance with documents listed in Table 3.8-2 for operation on the Russian Segment.

D.3.3.3 If necessary, certain Experiment hardware can be certified separately from the experiment for transport and stowage, with the understanding that an SDP will be provided which contains an integrated operational safety assessment for the entire experiment.

D.3.4. The cargo developer (curator) is responsible for cargo safety and determines the cargo category. The JARSWG, or the NASA or RSC Energia Safety Panels, can request additional clarification information and/or change the cargo category based upon an analysis of the data presented.

D.3.5.1 Cargo safety data packages are to be submitted to the Safety Panel not later than four months prior to the launch of the vehicle or module (TBR for Category 2 cargo). The review of the SDPs should be completed one month prior to the delivery of the cargo to KSC or Baikonur.

D.3.5.2 Any cargo which does not meet the stated deadlines (expedited cargo) requires Program level approval with the participation of the JARSWG, and the JCCT when required, to be processed.

SSP 50146, Revision B

D.3.6. If the cargo being transported is hardware whose safety for ISS operations as part of a module was already reviewed and approved by the Safety Panel, then a safety data package is issued for transportation, stowage and installation/removal of such cargo.

D.3.7.1 Non-experiment cargo which is delivered to the ISS on the same transport vehicle repeatedly or is operated on ISS more than once and has not undergone any basic changes (in design, layout, etc.) is considered reflight cargo and is covered by a safety data package issued previously and approved by the Safety Panel. A reflight certification letter will be used to document acceptability of the given cargo as reflight cargo, specifying part numbers, nomenclature, and previous certification.

Cargo which is delivered to the ISS on the same transport vehicle repeatedly or is operated on ISS more than once and, as it was modified, underwent changes impacting its safety, is considered reflight cargo and is covered by a safety data package issued previously and approved by the Safety Panel, and a safety data package is issued covering the modification/correction with regard to the review of the new hazards.

D.3.7.2 Experiments which are delivered to the ISS on the same transport vehicle more than once and/or are operated on ISS more than once are considered reflight experiments and are covered by a safety data package issued previously and approved by the Safety Panel. If significant changes are made to the safety acceptance rationale contained in the original safety data package, an update to the safety data package will be required. A reflight assessment must be provided prior to reuse; NSTS/ISS 13830C, Section 9, identifies the information required. For those experiments that fall under the classification of category 1 as defined in section D.3.3.1, and for category 2 experiment resupply items which don't themselves require unique Hazard Reports, the minimum reflight data submittal for acceptance shall include the following:

1. Experiment name/nomenclature and list of hardware that is to be flown
2. Flight upon which the hardware is to be delivered
3. Confirmation that there have been no changes to the hardware, its configuration, or its procedures
4. Confirmation that there have been no anomalies with the use of the hardware.

D.3.8 Cargo technical safety requirements are set forth in the documents listed in the following table.

Table 3.8-1 List of applicable documents

№	Document Number	Title
1	SSP 41162	Segment Specification For The United States On-Orbit
2	SSP 41163	ISS Russian Segment Specification
3	SSP 50128	Specification of Technical Requirements for the FGB
4	SSP 50094	NASA/RSA Joint Specifications Standards Document for the ISS Russian Segment
5	NSTS 1700.7B Addendum for ISS	Addendum "Safety Policy and Requirements For Payloads Using the International Space Station"
6	NSTS 1700.7B	Safety Policy and Requirements For Payloads Using the Space Transportation System
7	II32928-103	Requirements for International Partner Cargoes Transported on Russian Progress and Soyuz Vehicles
8	II32958-106	Requirements for International Partner Cargoes Delivered To the ISS Russian Segment
9	SSP 50260	ISS Medical Operations Requirements Document (MORD)
10	Materials Agreement	Agreement On The Safe Utilization of Materials In Cargoes To Be Delivered To ISS By Any Vehicle And Transferred To ISS For Stowage And/Or Operation

Applicability of the documents for safety certification of the cargo is given in the table below.

Table 3.8-2

SSP 50146, Revision B

Document	Russian cargo			US cargo	
	Transportation	Operation and stowage		Transportation	Operation and stowage
	On Shuttle	On RS	On US OS	On Progress, Soyuz	On RS
1. SSP 41162 US OS Spec			+		+
2. SSP 41163 RS OS Spec		+	+		+
3. SSP 50128 FGB Spec		+	+		+
4. SSP 50094 Joint NASA/RSA Standards		+	+		+
5. NSTS 1700.7B ISS Addendum			+		+
6. NSTS 1700.7B	+				
7. П32928-103 Rqmts for IP Cargoes Transported on Russian Vehicles				+	
8. П32958-106 Rqmts for IP Cargoes delivered to ISS RS		+			TBR Russian Side Position +
9. SSP 50260 (MORD)		+	+		+
10. Materials agreement		+	+		+

* - In addition to meeting unilateral RS requirements, Russian cargo will meet necessary unique USOS interface requirements.

** - In addition to meeting unilateral USOS requirements, US cargo will meet necessary unique RS interface requirements.

*** - For non Russian-produced cargo

In the event of conflicting requirements in these documents, the issue will be reviewed by the JARSWG and Safety Review Panels.

Table 3.8-2 will be revised after common ISS safety requirements are developed. It is the U.S. side's position that an outstanding issue in this table is the applicability of the current or a future version of NSTS 1700.7B ISS Addendum to Russian experiments in the Russian Segment.

D.3.8.2 Cargo Safety Process Document:

NSTS/ISS 13830 Revision C "Payload Safety Review and Data Submittal Requirements"

D.3.9 Cargo certified for stowage or operation on only one ISS segment can be transferred and used on the other ISS segment once new integrated hazard analyses have been approved by the appropriate safety panel and the segment owner.

D.3.10 Cargo stowage in a cargo vehicle and its transfer to a module to be stowed and operated is performed only if the safety certificate is approved or the hardware is yellow-tagged either for stowage or for restricted operation. The process of attaching and removing yellow tags is TBD.

D.3.11 The side responsible for cargo which is defined by the manifest (Annex 1 to SSP54101 "Increment Definition and Requirements Document (IDRD)") submits a safety data package on the entire article, including all of its components acquired from the other side.

D.4 Contents of ISS cargo flight safety certificates

SSP 50146, Revision B

D.4.1 Document name:

ISS Cargo Flight Safety Certificate

D.4.2 All cargo/experiment safety certificates are developed in a mutually concurred format. The mutually concurred forms are contained in each side's internal documentation and contain the following sections:

ISS Cargo/Experiment Flight Safety Certificate (reference JSC Form 906)	
Section	Title and contents of section
I	Name and designator of Cargo This section shall identify all cargo items being certified.
II	Description This section contains a description of the cargo and flight operations.
III	Cargo Category Category 1 or 2
IV	Applicability This section indicates the scope of application of the certificate. For example, the given certificate applies only to cargo transport on the Shuttle. For an experiment example, this certificate is applicable to the phase when the experiment is conducted on-board ISS and for the delivery of the equipment on the Shuttle Orbiter.
V	Responsibility This section states that the cargo meets the requirements of the applicable documents.
VI	Conclusion/Certification This confirms that the design and flight operations involving the cargo are safe. There are no deviations from the safety requirements. (If there are any, they are listed.) Results of hazard analyses are attached when required.

SSP 50146, Revision B

D.4.3 Requirements for numbering flight safety certificates for ISS cargo

D.4.3.1 Safety certificates are issued for the transport and ISS operations phases. All ISS cargo safety certificates are assigned a letter-digit designator (number) using the following system:

Numbering system requirements for flight safety certificates for ISS cargo

Requirements for numbering ISS Non-experiment Cargo Safety Certificates	Requirements for numbering ISS Experiment Safety Certificates.
<p>Safety certificates are issued for the transport and ISS operations phases. All ISS cargo safety certificates are assigned a letter-digit designator (number) using the following system:</p> <ul style="list-style-type: none"> a) designator of the transport vehicle (mission number), e.g. STS#, #P, #R b) after a slash, the designator of the space agency owner (of the certificate): “RSA” or “NASA” c) after a slash, the designator of the flight phase: TR – transport, including transfer, stowage, deorbit and return OP – operation, including storage and operation on the station d) the category of cargo complexity (1 or 2) e) after a slash, a three-digit number denoting the serial number of the certificate. There is one numerical sequence for all flight phases and cargo categories, for each mission. 	<p>Safety certificates are issued for the phase when the experiment is conducted on-board ISS and also cover the hardware transportation phase. Each ISS experiment safety certificate is assigned a designator (number) using the following system:</p> <ul style="list-style-type: none"> a) designation of the experiment within a program (e.g., MBI No. – for medical and biological experiments) b) after a slash, the designator of the space agency which approves the experiment for use on the ISS (certificate): “RSA” or “NASA” c) the category of the experiment complexity (1 or 2) d) after a slash, the number of the Expedition when the experiment is performed within the ISS program (e.g., ISS1 means that the experiment is conducted during Expedition 1) e) after a slash, a three-digit number designating the number of the certificate within that specific Expedition.

D.4.3.2 Examples of ISS cargo certificate numbering

Certificate 3P/NASA/TR2/015 indicates the following:

- a) 3P – cargo being delivered to the ISS on Progress Mission 3P;
- b) NASA – developed by NASA;
- c) TR2 – the cargo is to be transported and is category 2;
- d) 015 – serial number of the certificate for cargo delivered to the ISS on Progress Mission 3P.

Certificate STS-96/RSA/OP1/007 indicates:

- a) STS-96 – Cargo being delivered to the ISS on the Shuttle STS-96;
- b) RSA – developed by Rosaviakosmos;
- c) OP1 – the cargo is operated on the station and is category 1;
- d) 007 – serial number for the certificate for cargo being delivered to the ISS on STS-96.

D.4.3.3 Examples of ISS experiment certificate numbering

Certificate MBI-5/RSA-1/ISS1/003 indicates:

- a) MBI-5 - unique experiment name;
- b) RSA-1 – Rosaviakosmos experiment, category 1;
- c) ISS1 - experiment is conducted (and certificate is valid) during ISS increment 1;
- d) 003 - certificate serial number.

Certificate RBO-2/RSA-1/ISS1/005 indicates:

- a) RBO-2 unique experiment name;
- b) RSA-1 – Rosaviakosmos experiment, category 1;
- c) ISS1 - experiment is conducted (and certificate is valid) during ISS increment 1;
- d) 005 - certificate serial number.

D.4.4 Language of the Safety Data Submittals

D.4.4.1 All safety data packages provided to the NASA Safety Panels for review are written in Russian. These will be translated into English by NASA-provided personnel and submitted to the Safety Panels.

D.4.4.2 All safety data packages provided to the RSC Energia Safety Panel are written in Russian except for Experiment SDPs and SDPs on US cargoes to be stowed and/or operated on the ISS Russian Segment. SDPs on these cargoes and experiments will be submitted to RSC Energia in English with a brief summary in Russian.

D.4.5 Issuance of safety data packages for the transport and operation phases

The cargo developer may issue separate data packages for the transport and ISS operations phases as well as an integrated safety data package.

When an integrated data package is issued, the letter designator for the stage (TR or OP) is not included in the certificate number.

For example: the certificate for transport and operations 3P/NASA/2/015 indicates the following:

- a) 3P – cargo delivered to the ISS on Progress Mission 3P;
- b) NASA – the cargo was developed by NASA;
- c) 2 – the cargo is category 2;
- d) 015 – serial number of the certificate for the cargo to be delivered on Progress Mission 3P and operated on the ISS.

D.4.6 Following are the Safety Certificate Form (form JF906) and the Category 1 Cargo Hazard List (form JF907)

SSP 50146, Revision B

ISS CARGO ☐ / EXPERIMENT ☐
FLIGHT SAFETY CERTIFICATE
 CERTIFICATE NUMBER

I. NAME AND PART NUMBER:**II. DESCRIPTION:****III. CARGO CATEGORY:**

- ☐ 1
☐ 2

IV. APPLICABILITY:

<i>RUSSIAN CARGO</i>	<i>US CARGO</i>
<input type="checkbox"/> Operation on USOS	<input type="checkbox"/> Operation on Russian Segment
<input type="checkbox"/> Operation on Russian Segment	<input type="checkbox"/> Stowage on Russian Segment
<input type="checkbox"/> Stowage on USOS	<input type="checkbox"/> Transportation on Progress
<input type="checkbox"/> Stowage on Russian Segment	<input type="checkbox"/> Transportation on Soyuz
<input type="checkbox"/> Transportation on Shuttle	<input type="checkbox"/> Transportation on Russian Module

V. RESPONSIBILITY:

The cargo complies with the safety requirements of the following documents:

- ☐ SSP 50094 "NASA/RSA Joint Specifications Standards Document for the ISS Russian Segment"
- ☐ SSP 41163 "Russian Segment Specification"
- ☐ SSP 50128 "Specification of Technical Requirements for the FGB"
- ☐ ПЗ2958-106 "Technical Requirements for Foreign Partner Hardware to be Stored and Operated on the ISS Russian Segment"
- ☐ ПЗ2928-103 "Requirements for International Partner Cargoes Transported on Russian Progress and Soyuz Vehicles"
- ☐ NSTS 1700.7B "Safety Policy and Requirements for Payloads using the Space Transportation System"
- ☐ NSTS 1700.7B ISS Addendum "Safety Policy and Requirements for Payloads using the International Space Station"
- ☐ SSP 41162 "Segment Specification for the USOS"
- ☐ SSP 50260 "ISS Medical Operations Requirements Document" (MORD)
- ☐ "Agreement on Safe Utilization of Materials in Cargoes To Be Delivered to ISS By Any Vehicle and Transferred to ISS for Stowage and/or Operation"
- ☐ ANSI Z136.1-1993 Class 1, 2, or 3a (lasers)

VI. CONCLUSION/CERTIFICATON:

- ☐ Category 1:

The listed cargo/experiment has potential hazards only in the areas specified in JSC Form 1231 "Experiment Standard Hazard Report Form" for experiments or JSC Form 907 "Category 1 Cargo Hazard List" for other cargo, and necessary controls for those hazards are implemented and verified. The cargo/experiment is safe for transportation and/or use as indicated in Section IV of this Certificate.

- ☐ Category 2:

The listed cargo/experiment has potential hazards in the areas specified in JSC Form 1231 "Experiment Standard Hazard Report Form" for experiments or JSC Form 907 "Category 1 Cargo Hazard List" for other cargo, and unique hazards which are beyond the scope of Category 1 cargo. The Unique Hazard Reports are attached. All necessary controls for hazards are implemented and verified. The cargo/experiment is safe for transportation and/or use as indicated in Section IV of this Certificate.

VII. APPROVAL:

SSP 50146, Revision B

	Signature	Date
Project Manager		
JARSWG Co-Chairman		
ISS Program Manager		

JSC Form 906 (Rev February 28, 2002) Previous editions are obsolete. (MS Word October 2001)

CATEGORY 1 CARGO HAZARD LIST

- ☐ 1. Structural Failure.
 - ☐ a. During transportation, the cargo is not structurally mounted.
 - ☐ b. The cargo meets the kick load requirement if structurally mounted inside ISS.
 - ☐ c. The cargo is not externally mounted.
- ☐ 2. Structural Failure of Sealed or Vented Containers.
 - ☐ a. The cargo does not contain any substance that would cause a hazard if released (e.g. gases, liquids or particles).
 - ☐ b. The cargo will not create a hazard in the event of depressurization or re-pressurization of the surrounding volume.
- ☐ 3. Hazardous Sharp Edges, Snags, Burrs, Pinch Points, Appendage Entrapments.
 - ☐ a. The cargo is free of the listed deficiencies.
 - ☐ b. The cargo contains functional sharp edges (e.g. scissors) and pinch points (e.g. clamps) that are controlled through handling procedures and crew training.
- ☐ 4. Shatterable Materials.
 - ☐ a. The cargo contains shatterable materials that are provided with structural protection to prevent fragments from entering the habitable environment.
 - ☐ b. The cargo contains photographic, optoelectric, or TV lenses and has special covers to protect them when not in use (stowed).
- ☐ 5. Flammability.
 - ☐ a. The cargo meets the supplying side's standards for flammability of materials.
 - ☐ b. The cargo contains neither ignition sources nor self-igniting materials.
- ☐ 6. Materials Offgassing.
 - ☐ a. The cargo does not exceed agreed-to standards ("Agreement on The Safe Utilization of Materials in Cargoes To Be Delivered to ISS By Any Vehicle and Transferred to ISS for Stowage and/or Operation.")
- ☐ 7. Non-ionizing Radiation (non-transmitters).
 - ☐ a. The cargo radiated emissions are within the acceptable levels for the applicable ISS segment or transport vehicle.
 - ☐ b. Deviation requires approval of the receiving side.
 - ☐ c. The deviation has been approved.
- ☐ 8. Lasers.
 - ☐ a. Beams are totally contained over the complete power range.
 - ☐ b. Lasers meet ANSI Z136.1-1993 for Class 1, 2, or 3a lasers (power measured at source.)
- ☐ 9. Battery Failure.
 - ☐ a. The cargo contains batteries of the following types: Alkaline-MnO₂, Carbon-Zn, or Zn-Air in sizes D or smaller, with:
 - ☐ 1. Six or fewer cells either all in parallel or all in series (series-parallel combinations require a unique hazard report)
 - ☐ 2. No potential charge source
 - ☐ 3. A vented container
 - ☐ b. The cargo contains batteries of the following types: Li-CFx, Li-Iodine, Li-MnO₂, Ni-Cd, Ni-MH, or Ag-Zn, with:
 - ☐ 1. Capacity of 200 mAh or less
 - ☐ 2. No more than 2 cells per common circuit
- ☐ 10. Touch Temperature.

SSP 50146, Revision B

- ☐ a. No single failure will cause exceedance of touch temperature limits ($=0^{\circ}\text{C}$ or $=45^{\circ}\text{C}$)
- ☐ 11. Rotating Equipment
 - ☐ a. The cargo contains small fans or low-energy rotating machinery such as small electric motors but release of debris is precluded by design.
- ☐ 12. Noise
 - ☐ a. The cargo does not generate noise or meets ISS noise requirements.
- ☐ 13. Cleanliness/Microbiological Contaminants
 - ☐ a. The cargo has been maintained clean since assembly/testing.
 - ☐ b. The surface of the cargo or its packaging must be disinfected.
- ☐ 14. The cargo does not have an electrical interface with the electrical power distribution system of the receiving side's segment /vehicle.
- ☐ 15. The cargo does not contain software that could create a hazard via interface with onboard control software.
- ☐ 16. The cargo does not contain biological or toxic substances or alcohol.

SSP 50146, Revision B

Appendix E of SSP 50146 – Bilateral Safety and Mission Assurance Requirements

**NASA/ROSAVIAKOSMOS/ESA TRI-LATERAL REQUIREMENTS FOR IMPLEMENTATION
OF THE SAFETY AND MISSION ASSURANCE PROCESSES FOR THE ATV
AND ISS RS**

Version 1

June 12, 2003

National Aeronautics and Space Administration
Johnson Space Center

European Space Agency

Rosaviakosmos

SSP 50146, Revision B

**NASA/ROSAVIAKOSMOS/ESA TRI-LATERAL REQUIREMENTS FOR IMPLEMENTATION
OF THE SAFETY AND MISSION ASSURANCE PROCESSES FOR THE ATV
AND ISS RS**

June 12, 2003

Approved by:

Original signed by
James W. Wade/ NASA
Manager, Safety and Mission Assurance
& Program Risk

Original signed by
Pavel Vorobiev/ RSC-E Deputy Director,
ISS Program;
Co-Chairman ,
ISS Joint Safety Working Group

Original signed by
Sergei Sharygin
Rosaviakosmos

Original signed by
Richard Chase/ ESA
ATV Safety and Product Assurance Manager

SSP 50146, Revision B

**NASA/ROSAVIAKOSMOS/ESA TRI-LATERAL REQUIREMENTS FOR IMPLEMENTATION
OF THE SAFETY AND MISSION ASSURANCE PROCESSES FOR THE ATV
AND ISS RS**

June 12, 2003

Concurrence

Concurred by:

	OE
Kelle Pido	
ISS S&MA	Org.

	Date
<i>Original signed by</i>	
Signature	

	OE
Gregg Baumer	
Chairman, Safety Review Panel	Org.

	Date
<i>Original signed by</i>	
Signature	

	NT
Donald W. Totton	
Chairman, SMART	Org.

	Date
<i>Original signed by</i>	
Signature	

	MA
Axel M. Larsen	
Chairman, PSRP	Org.

	Date
<i>Original signed by</i>	
Signature	

	RSC-E
Alexander Didenko	
Head, ISS Safety, Reliability & Quality Assurance	Org.

	Date
<i>Original signed by</i>	
Signature	

1.0 Introduction

The ATV is an automated transfer vehicle built by ESA to serve as an ISS cargo transfer vehicle, an ISS reboost vehicle and an ISS RS refueling vehicle. In addition, the ATV will be loaded with ISS waste, which will be disposed of during ATV destructive re-entry at the end of its mission. The ATV will dock to the Russian Segment of the ISS, and while attached becomes part of an integrated ISS fulfilling the requirements on RS ISS integrations. The safety of the ATV must be assessed during its free-flight operations in the vicinity of the ISS, and during the ATV attached phase. This appendix will document the trilaterally agreed aspects of performing and reviewing ATV/ ISS-RS interaction related safety assessments. It also addresses the overall ISS safety assessment process as it pertains to ATV.

1.1 Purpose

The purpose of this appendix is to define the roles and responsibilities of each organization through the ISS Safety Process for the ATV basic Vehicle integration. This appendix will also identify the data exchanges necessary to support ATV related safety reviews. This document identifies the applicable Safety Requirements for the review of the ATV and ISS Safety review process for ATV Cargo will be established in separate multilateral agreements documented in TBD.

1.2 Scope

The safety of the stand-alone ATV and the ATV integrated with the ISS will be assessed consistent with the processes and responsibilities outlined in the NASA/RSA Memorandum of Understanding Concerning Cooperation on the Civil International Space Station (NASA/RSA MOU) and the NASA/ESA Memorandum of Understanding Concerning Cooperation on the Civil International Space Station (NASA/ESA MOU).

In addition, provisions for data exchanges necessary to support ATV assessments and reviews documented in this appendix have been defined in the ESA/Rosaviakosmos/RSC-E ATV Integration Contract, the Alenia/RSC-E contract for procurement of Russian Systems and the ATV Bilateral Data Exchange, Lists and Schedules (BDEALS).

1.3 Program Requirement References

Where applicable, the following documents contain design requirements that will be used as the basis for assessing ATV safety. Contradiction in document requirements will be resolved by mutual agreement of the Trilateral Safety Organizations.

SSP 50439, ESA Segment Specification for the Automated Transfer Vehicle (ATV)
 SSP 50129, International Space Station (ISS) to Automated Transfer Vehicle (ATV) Interface Requirements Document (IRD)
 SSP 41163, Russian Segment Specification

The requirements of SSP 50094, NASA/RSA Joint Specifications Standards Document for ISS Russian Segments Rev. A, 03/10/00, are applicable to RSC-E. Any requirements contained in this document, which are applicable to the ESA ATV, have been reflected in SSP 50129, ATV to ISS IRD, or SSP 50439, ATV Segment Spec.

2.0 Safety Assurance Program Features

SSP 50146, Revision B

2.1 Tasks and Responsibilities

The responsibilities of NASA, RSC-E and ESA are described in Figure 2.

Hardware presenting a hazard to the partner's segment or the ISS in general shall be jointly reviewed by the safety process per SSP 30599.

2.1.1 NASA Tasks and Responsibilities

NASA shall assess overall safety of ISS during joint ISS/ATV operations during the free flying and attached modes.

NASA or its prime contractor shall perform the Integrated Stage safety assessment of the ATV as an integrated element with the ISS.

2.1.2 Rosaviakosmos Tasks and Responsibilities

RSC-E shall perform the integrated ATV/RS ISS safety assessment and generate hazard reports to be reviewed by the NASA SRP. RSC-E will use their own safety assessment methodology and hazard report format for these documents in accordance with Appendix C of SSP 50146.

RSC-E shall identify to both NASA and ESA which safety-related technical data are needed from ESA in order to perform the ATV/RS ISS safety assessment.

RSC-E shall provide relevant safety-related equipment technical data to Alenia for Russian equipment (i.e. RDS, RFS, RECS) onboard ATV in accordance with contractual requirements.

RSC-E shall support the NASA Safety Panels (SRP) on all ATV related integrated assessments.

2.1.3 ESA Tasks and Responsibilities

ESA shall ensure ATV design and integrated ATV/ISS operations (attached and free flying) meets ISS Program safety and ISS RS requirements.

ESA shall perform ATV stand-alone (including all Russian hardware which is integrated on the ATV) safety assessments and generate hazard reports. ESA will use its own safety assessment methodology and hazard report format for these documents.

ESA shall provide ATV safety-related technical data to NASA and RSC-E to allow performance of Integrated ATV/ISS safety assessments.

ESA shall provide relevant safety data to RSC-E for European equipment onboard the Service Module (LRR, PCE)

ESA shall support all the NASA Safety Panels (SRP) reviews of ATV related assessments in accordance with SSP 30599.

2.2 Safety Review Requirements

Figure 1 ATV Safety Review Cycle depicts the flow of data and the participating parties for the ATV through the complete three-phase safety review process. All of which supports the ATV stage CoFR, as called for in the ISS COFR Process document, SSP 50108.

2.2.1 Safety Review Process

SSP 50146, Revision B

The ATV shall be subjected to the requirements of SSP 30599 Safety Review Process for International Space Station Program and this document.

2.3 Safety Activities

2.3.1 Agreements on Safety Activities

2.3.1.1 Matrix for Comparison of ATV and ISS RS requirements -

As stated above, ESA will use the ESA Segment Spec SSP 50439 for ATV HR's; RSC-E will use the Russian Segment Spec 41163 ISS RS Integrated HR's. For hazard reports on Russian hardware provided to ESA, ESA will utilize ESA requirements, but refer to Russian requirements if appropriate.

2.3.1.2 NASA, RSC-E and ESA will review and concur on list of hazards applicable when the ATV is in proximity to and attached to ISS.

2.3.1.3 ESA will support the ATV/ISS RS Integrated HRs review process at the SRP. RSC-E will support the ATV stand-alone HRs review process at the SRP.

2.3.2 Safety Analysis

2.3.2.1 Input Data Exchange

Data exchanges for the purpose of preparing the appropriate documents (e.g. HR) and analysis will be identified by ESA and RSC-E. Delivery of this data will be determined by both ESA and RSC-E in order to support the appropriate Safety Review Panels or Technical Interchange Meetings (TIM).

The appropriate lead organization will be responsible for timely delivery of all review data to support any Safety review activity. The delivery of the review data shall be in accordance the guidelines established in SSP 30599 Safety Review Process for International Space Station Program (i.e., 45 days prior to scheduled review).

2.3.2.2 Coordination

NASA, ESA and RSC-E will concur on the schedule for exchanging and reviewing information for the ATV at the NASA Safety Reviews.

Figure 1 ATV Safety Review Cycle

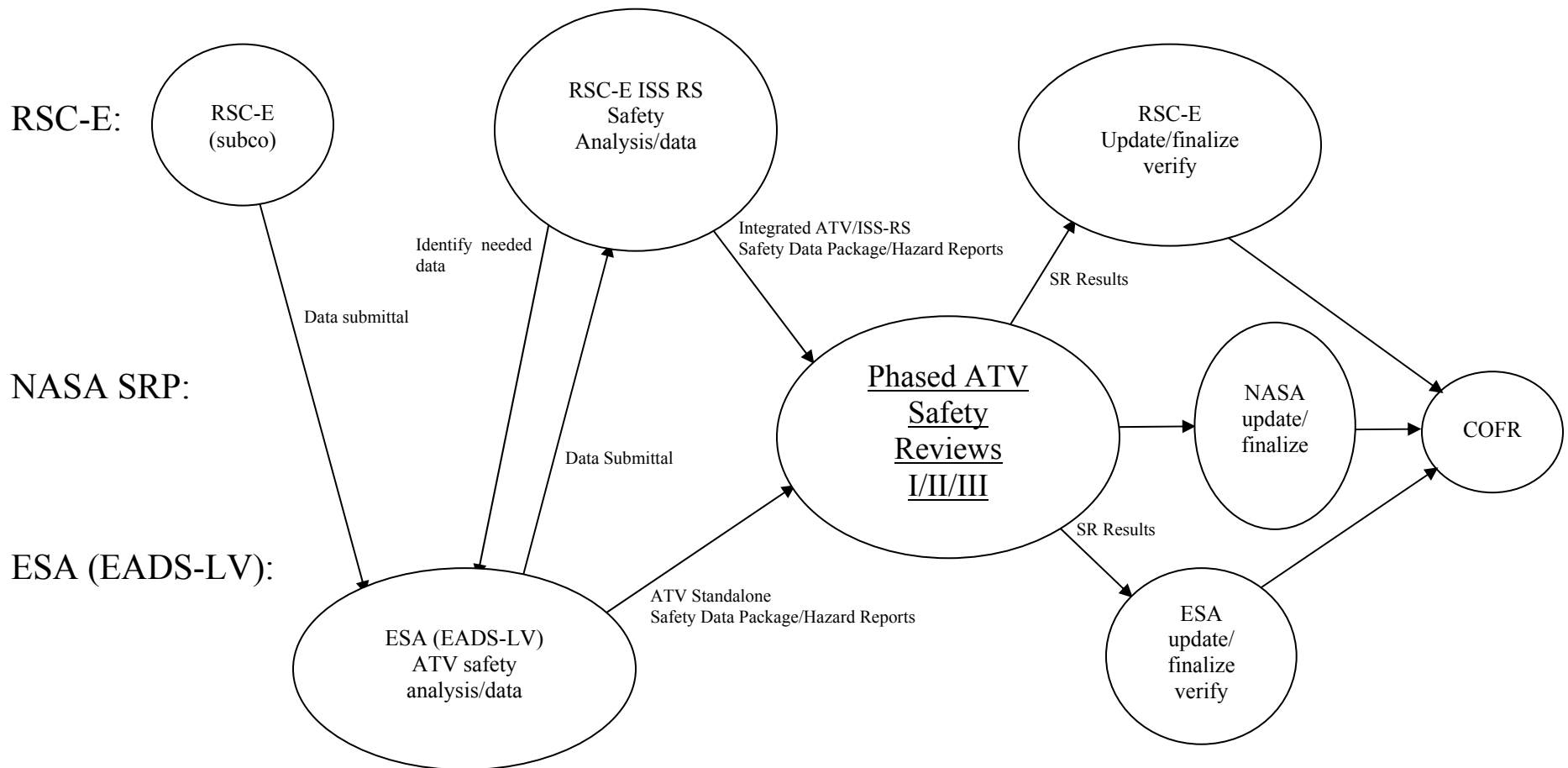


Figure 2 Trilateral Safety Roles and Responsibilities

