CHANGE NOTICE

Date Prepared: July 8, 2011

1.	2.	3. Code Ident.	4. Change Notice No.
Barrios Technology 16441 Space Center Blvd, Suite B-100 Houston, Texas 77058	☐ Proposed ☒ Approved		DCN 002
		5. Contract No.	6. Directive No. 012751
7. Document No./Rev. SSP 30599/Revision E	8. Document Title Safety Review Process		9. SSCN No. 012751
10. Related Change No.	11. Change Title		

THIS NOTICE INFORMS RECIPIENTS THAT THE DOCUMENT IDENTIFIED BY THE NUMBER (AND REVISION LETTER) SHOWN IN BLOCK 7 HAS BEEN CHANGED. THE PAGES CHANGED BY THE CN BEING THOSE FURNISHED HEREWITH AND CARRYING THE SAME DATE AS THIS CN. THE PAGES OF THE PAGE NUMBERS AND DATES LISTED BELOW IN THE SUMMARY OF CHANGED PAGES COMBINED WITH NON-LISTED PAGES OF THE ORIGINAL ISSUE OF THE REVISION SHOWN IN BLOCK 7 CONSTITUTE THE CURRENT VERSION OF THIS SPECIFICATION.

12. DCN No.	13. Pages Changed (Indicate Deletions)	S*	A*	Date
002	Cover	S		
	Revision and History Page	S		
	v - viii	S		
	J-i – J-C-2	S		
	Order of DCN Incorporation: DCN 001, DCN 002			

14. Technical Concurrence

/s/ Vincent Berend — 07/12/11 (Date)

* “S” indicates supersedes earlier page. “A” indicates added page.

Safety Review Process

International Space Station Program

Revision E

Incorporates DCN 002
June 2009

National Aeronautics and Space Administration
International Space Station Program
Johnson Space Center
Houston, Texas Contract No.: NNJ04AA01C

REVISION AND HISTORY PAGE

REV.	DESCRIPTION	PUB. DATE
-	Baseline Issue (Reference SSCBD BB003229B EFF.)	10-93
A	Revision A (SSDBD 000085 EFF. 05-05-95)	
	No cost change – ECP 85)	6-15-95
B	Revision B (Reference per SSCD 003405, EFF. 01-07-02)	02-13-02
C	Revision C (Reference per SSCD 007558, EFF. 07-08-04)	12-05-05
D	Revision D (Reference per SSCD 009840, EFF. 10-24-06)	
	Early Released	11-01-06
	Program Released	11-16-09
E	Revision E (Reference per SSCD 011243, EFF. 07-20-09)	11-16-09
	DCN 001 (Reference per SSCD 011760, EFF. 11-06-09)	11-23-09
	DCN 002 (Reference per SSCD 012751, EFF. 05-18-11)	07-12-11

INTERNATIONAL SPACE STATION PROGRAM

SAFETY REVIEW PROCESS

LIST OF CHANGES

JUNE 2009

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

Board Name	Entry Date	Change	Paragraph(s)
SSPCB	October 1993	Baseline	All
SSPCB	June 15, 1995	Revision A	All
SSPCB	February 2000	Revision B	All
SSPCB	May 2004	Revision C	All
SSPCB	September 2006	Revision D	All
SSPCB	June 2009	Revision E	All
SSPCB	November 2009	DCN 001	
SSPCB	July 2011	DCN 002	

TABLE OF CONTENTS

APPENDIX

TABLE

FIGURE

APPENDIX J – PAYLOAD SAFETY REVIEW AND DATA SUBMITTAL REQUIREMENTS

NSTS/ISS 13830, Revision C, Payload Safety Review and Data Submittal Requirements has been placed in Appendix J to preserve the Requirements after the completion of the Shuttle Program. NO TECHNICAL CHANGES have been made to NSTS/ISS 13830, Revision C.

TABLE OF CONTENTS

Section Page

Section | Page

Section Page

SECTION 1
INTRODUCTION

Implementation of the payload safety process is the joint responsibility of the Payload Organization (PO); the flight operator, Lyndon B. Johnson Space Center (JSC); and the launch/landing site operator, John F. Kennedy Space Center (KSC).

The International Space Station (ISS) and Space Shuttle Program (SSP) safety policies and requirements for ISS and Shuttle payloads are specified in the current version of NSTS 1700.7 "Safety Policy and Requirements for Payloads Using the Space Transportation System" and the current version of the NSTS 1700.7 ISS Addendum, "Safety Policy and Requirements for Payloads Using the International Space Station." In addition, unique ground safety policies and requirements are specified in the current version of 45 SPW HB S-100/KHB 1700.7, "Space Shuttle Payload Ground Safety Handbook." These documents require the PO to conduct a systematic safety analysis and to document and submit a Safety Data Package (SDP) in support of safety reviews to be conducted by the flight operator (JSC) and the launch/landing site operator (KSC).

National Aeronautics and Space Administration (NASA) Headquarters has assigned the responsibility to review submitted payload safety documentation to the Space Shuttle and Space Station Program Directors at JSC and the Director of Safety and Mission Assurance at KSC. The JSC Payload Safety Review Panel (PSRP) will assess the payload design and flight operations; the KSC Ground Safety Review Panel (GSRP) will assess the Ground Support Equipment (GSE) design and ground operations. These two panels were formed to accomplish the following:

- Assure that PO interpretation of the safety requirements is consistent with NASA payload safety policy.
- Conduct safety reviews as appropriate during the development of the payload, associated GSE, and related operations.
- Evaluate hazard analyses and Noncompliance Reports (NCRs).
- Negotiate the resolution of safety issues involving design and operation to ensure compliance with all applicable safety requirements.
- Assess payload design features that have been implemented for controlling identified hazards and the verification approach that confirms intended system performance.
- As human spaceflight has expanded to multinational activities through the cooperation in the ISS Program (ISSP), and recognizing the responsibility and experience of the International Partner (IP) Safety Organizations, it is appropriate that the PSRP function not be limited to a single United States (U.S.) panel only. With respect to that goal, the JSC PSRP has developed understandings and agreements of internal IP payload safety methodologies and processes that meet or exceed the standards of the JSC PSRP and assure the safe implementation of the requirements dictated within this document.

SECTION 2
PURPOSE

The purpose of this document is to define the payload safety review process in order to assist the Shuttle/ISS POs in documenting compliance with the payload requirements documents specified in section 1. Specifically, this document accomplishes the following:

- Defines the safety reviews necessary to comply with the system safety requirements that are applicable to payload design, flight operations, GSE design, and ground operations for both ISS and Space Shuttle.
- Identifies the required content of the SDP.
- Describes preparation for and conduct of the safety review.
- Establishes the timeline for data submittal and establishes the depth of detail required for the various submittals.
- Explains safety review process variations.
- Defines the payload series/reflight review process.

SECTION 3
SCOPE

Data submittal requirements included herein apply to hardware being submitted to both the PSRP and the GSRP unless specified otherwise. This document outlines the minimum data submittal requirements; the PSRP and the GSRP reserve the right to request additional data as deemed necessary to support safety documentation.

The objective of the safety review process is to review the payload, GSE, and operations for adequate safety implementation. The mission success and any scientific objectives of the payload are the responsibility of the PO and are beyond the scope of this document and process.

This document does not establish design requirements.

3.1 APPLICABLE HARDWARE

This document applies, but is not limited to, the following payload hardware that flies/operates on the Space Shuttle and/or ISS during any mission phase (prelaunch, launch, ascent, on-orbit, entry, landing, or postlanding):

- New Payload Hardware
- Existing (reflown and series) Payload Hardware
- Hardware Associated with Developmental Test Objectives (DTOs), Detailed Supplemental Objectives (DSOs), Risk Mitigation Experiments (RMEs), Space Medicine Program (SMP), and Human Exploration and Development of Space Technology Demonstrations (HTDs) Experiment Hardware

The document also applies, but is not limited to, the following payload-related hardware:

- Government-Furnished Equipment (GFE)
- Airborne Support Equipment (ASE)
- GSE

3.2 EXPORT CONTROL

The PSRP complies with the United States export control laws and regulations as established by the U.S. Department of Commerce in the Export Administration Regulations (EAR) and the U.S. Department of State in the International Traffic in Arms Regulations (ITAR). The PSRP also complies with the Space Shuttle Program's export control policy in NSTS 07700 Volume V and the ISSP's export control policy in SSP 50223.

Export control factors significantly into two areas of the payload safety review process:

- Distribution of Payload Data
- Conduct of Safety Reviews

The PSRP Executive Officer serves as the primary exporter of payload data to the ISS IPs and other foreign persons in support of the payload safety review process. Payload data includes safety data packages, hazard reports, safety review presentation materials and other payload related information. Specific export control data submittal requirements for payload organizations are listed in section 4.3.1.5 of this document.

The PSRP Executive Officer takes special precautions when conducting safety reviews for payloads under export control restrictions. These precautions may include restricting attendance, limiting presentation materials, posting signs, or conducting the review in a secure facility.

SECTION 4
RESPONSIBILITIES OF THE PAYLOAD ORGANIZATION

The PO is responsible for assuring the safety of its payload and for complying with the safety requirements contained in the technical requirements documents cited in section 1. To this end, the PO must accomplish the following:

- Perform a Safety Analysis
- Identify Hazards
- Document Compliance with the Safety Requirements
- Present the Documentation to the PSRP/GSRP

4.1 SAFETY ANALYSIS

To meet the requirements of the current version of NSTS 1700.7 and NSTS 1700.7 ISS Addendum, paragraph 301, **the PO shall perform a safety analysis** of the payload and GSE. The analysis shall consider hardware design, verification, testing, and flight/ground operations. The safety analysis shall begin during the payload concept phase and shall be refined and expanded as the design matures. For situations in which payload hardware will be installed or reconfigured on-orbit or in which the payload will be on-orbit for an extended time, safety analyses shall consider the necessity of on-orbit verification/reverification of hazard controls.

4.1.1 Level of Analysis

In order to identify the hazards applicable to a payload, the PO shall conduct safety analyses both at the system and subsystem levels. Each system and subsystem shall be evaluated to determine the applicability of each technical safety requirement.

Selection of subsystem groupings varies and any convenient grouping may be used. The following is a suggested list of subsystems: biomedical, caution and warning, cryogenic, electrical, environmental control, human factors, hydraulics, materials, mechanical, optical, pressure systems, propulsion, pyrotechnics, radiation, and structures.

For hardware developed for or provided to the PO, the PO shall:

- Obtain the appropriate safety data from the supplier or conduct an independent safety analysis.
- Conduct a safety analysis of the interfaces between the subject hardware and other elements.

4.1.2 Analysis Techniques

Depending on the complexity of the payload, the PO should use established analytical techniques (e.g., preliminary hazard, sneak circuit, fault tree, operational hazard, and failure modes and effects analyses) to obtain the data necessary to complete, present, and support payload hazard reports.

4.1.3 Safety Verifications for Payloads with Catastrophic Hazard Potential (Flight Only)

The current version of NSTS/ISS 18798 specifies data requirements to document the verification program for payload systems/subsystems that have catastrophic hazard potential. An excerpt from this document is included below for convenience.

Table 4-1. - NSTS/ISS 18798

> All payload systems having catastrophic hazard potential for the orbiter or crew as a result of operations in or near the orbiter must use hardware and procedures that have been subjected to a rigorous verification program. Verification programs normally require testing to verify adequate performance margins under all environmental conditions (qualification testing) as well as demonstrating intended system performance on flight hardware. Comprehensive system-level testing on payload flight hardware supported by qualification test on protoflight or flight type hardware are the preferred verification methods. It is essential that payload system performance be verified from the input stimuli to the end function.
>
> Safety-critical system performance that cannot be verified by test shall be verified by independent parties using dissimilar analysis techniques whenever possible. Single party analytical efforts can be used to verify performance only when the methodology is widely accepted and conservative margins are applied to the results.
>
> The payload organization must focus its attention to all parts of the payload verification program and orbiter interface verification activities to assure that the sub-elements of the total verification program are integrated into a comprehensive system verification effort that confirms the intended system performance. When the use of ground test equipment (apparatus) is required to replace flight hardware functions, verification methods shall be developed by engineering personnel independent from those designing the flight system. Test requirements, procedures, and test apparatus shall be derived from intended functional requirements rather than from the design, and all items must be maintained under strict configuration control. The payload organization is responsible for developing and presenting sufficient data to the PSRP [GSRP] to substantiate that the test requirements, procedures, and test apparatus will provide an adequate simulation in substitution for the end function.

4.2 HAZARD IDENTIFICATION

The primary objectives of the safety review process are to identify the potential hazards applicable to a payload, including its flight, GSE, and ground operations, and to assure that the hazard controls and verifications (including on-orbit verification/reverification of hazard controls where applicable) are adequate and in compliance with the safety requirements. To assist the PO in accomplishing these objectives, appropriate safety terminology has been defined in the current version of NSTS 1700.7.

Although not exhaustive, the following is a list of some previously identified flight hazard groups that have been used on hazard reports: collision, contamination, corrosion, electrical shock, explosion, fire, injury and illness, loss of orbiter entry capability, and inability to egress.

The following are basic hazard groups applicable to ground operations: structural failure of support structures and handling equipment; collision during handling; inadvertent release of corrosive, toxic, flammable, or cryogenic fluids; loss of habitable/breathable atmosphere; inadvertent activation of ordnance devices; ignition of flammable atmosphere/material; electrical shock/burns; personnel exposure to excessive levels of ionizing or nonionizing radiation; use of hazardous/incompatible GSE materials; inadvertent deployment of appendages; working under suspended loads; and rupture of composite epoxy overwrapped pressure vessels.

4.3 DOCUMENTATION OF COMPLIANCE WITH THE SAFETY REQUIREMENTS

The safety analysis results shall be documented in the SDP, which includes applicable payload hazard report forms (JSC Form 542B and JSC Form 1230) and presented to both the JSC PSRP and the KSC GSRP as described in this document. Guidelines for completing the flight hazard report forms and preparing the SDPs are found in JSC 26943, “Guidelines for the Preparation of Payload Flight Safety Data Packages and Hazard Reports for Payloads Using the Space Shuttle,” current issue.

Low hazard potential hardware may qualify as Basic (Category 1), as defined in paragraph 5.4. Submitted requirements for IP-sponsored payload meeting the Basic (Category 1) criteria are Described in paragraph 5.4.

For SDP preparation, the PO is responsible for using the current version of all applicable forms and safety documentation. The PO may verify current forms/documents by contacting the Executive Officer to the PSRP or the Chairman of the GSRP. These forms are listed in section 11.

4.3.1 Data Submittals

Although there will be some duplication of material contained in data submittals prepared for PSRP and GSRP reviews, each package serves a different purpose and must stand alone.

Data submittals, which may include SDPs and other supporting information (e.g., action item responses), should identify the flight on which the payload is manifested (if known) and be formally submitted in English to the Executive Officer, PSRP, or the Executive Secretariat, GSRP. Data should be formally transmitted under the signature of the Program Manager.

Safety review meetings are scheduled to be held approximately 45 calendar days after receipt of an acceptable SDP (i.e., an SDP that satisfies all the requirements in this document).

The SDP will be made available to the PSRP/GSRP members and various other NASA/contractor technical and administrative personnel who support the Panels. For ISS payloads, this may include International Partner representatives to the PSRP.

Payload safety data must be submitted electronically via the Internet using the Payload Safety Data Management System (DMS) located at the following URL:

http://psrp.jsc.nasa.gov

The DMS System Administrator (tel. 281-335-2446) can provide information on acceptable software applications, electronic addresses, detailed login instructions, and system procedures. POs may also access the DMS via a hyperlink at the top of the Payload Safety homepage located at the following URL:

http://wwwsrqa.jsc.nasa.gov/pce

POs must obtain approval from the PSRP Executive Officer or Executive Secretariat, GSRP to submit flight or ground safety data, respectively, by alternate means or to submit supplementary data in hard copy format. Hard copy submittals must be single-sided and sequentially paginated from the cover sheet to the last page of the package.

Once the SDP has been electronically submitted, the PO must send the transmittal letters, document signature pages, and signed original Hazard Reports (HRs) to the appropriate Panel contact:

Executive Officer, PSRP
NASA Lyndon B. Johnson Space Center
Mail Code NE12
2101 NASA Parkway
Houston, TX 77058-3696

Executive Secretary, GSRP
NASA John F. Kennedy Space Center
Mail Code SA-C3
Kennedy Space Center, FL 32899-0001

4.3.1.1 Submittal of Proprietary Data

If proprietary data are submitted in the SDP, the transmittal letter must include the following statement:

> This payload safety data package contains proprietary data on the following pages: [list the appropriate page numbers]. [Insert name of the payload organization] acknowledges awareness and acceptance of the GSRP and the PSRP's policies and methods of processing proprietary data. [Insert name of the payload organization] also will provide any additional protective measures it deems necessary over and above that provided by the panels during meetings.

The transmittal letter and the first page of the SDP must identify the specific pages that contain proprietary information. Insert the word "PROPRIETARY" at the top and bottom of each page that contains proprietary data. The word "PROPRIETARY" shall be in all capital letters in a large font size and style that is easily discernible from the rest of the text.

In addition to the proper submittal of proprietary information, the PO should be aware of the following while attending PSRP/GSRP safety reviews, Technical Interchange Meetings (TIMs), and action item closure meetings:

- PSRP/GSRP meetings are not conducted in secure facilities. Thus, when it is necessary to recess meetings (e.g., lunch and breaks), the POs will be responsible for protecting any proprietary data distributed during the meeting (other than that logged and distributed by NASA as part of the SDP).
- If any proprietary data are to be presented or discussed during the meeting, prior to the meeting the PO will notify the PSRP Executive Officer/GSRP Chairman who will then make arrangements to monitor attendance, close the doors, and post a sign noting that access to the meeting is controlled.
- The PO will be responsible for retrieval and disposition of any proprietary material distributed at the meeting (other than that logged and distributed by NASA as part of the SDP), with the exception that two copies of proprietary material distributed by the PO at the meeting will be retained by the PSRP/GSRP in a protected file.

When the PSRP/GSRP receives proprietary data included in the SDPs, such data will be handled in a manner that will protect the interests of the PO. These procedures include tracking distributed materials, protecting files, and restricting reproduction. In order to exercise reasonable care in protecting proprietary data in connection with the payload safety review process, NASA will ensure that proprietary data are distributed only to persons who have a need to review such data in support of panel functions. Furthermore, distributed data that is returned to the PSRP Executive Officer/GSRP Chairman after use will be destroyed via the NASA secure disposal process.

The protection of material marked "PROPRIETARY" creates an added burden on the PSRP/GSRP review support system, so the PO should mark only those items that are proprietary. The PO should coordinate with the PSRP Executive Officer/GSRP Chairman to explore such alternatives as providing the proprietary material in a separate package when it is a very small portion of the overall SDP. If a separate, proprietary briefing package (not contained in the SDP) is to be presented to the PSRP/GSRP during the review, the PO shall provide at least 20 copies of such material for distribution at the review.

If the PO discovers that some portion of the SDP marked "PROPRIETARY" is no longer considered such, the PO must inform the PSRP Executive Officer and/or the GSRP Chairman in writing.

4.3.1.2 Submittal of Copyrighted Data

Payload organizations are hereby informed that payload documentation submitted to NASA must be reproduced and distributed to the members of the PSRP/GSRP and to associated technical support personnel. Accordingly, copyrighted data shall not be included in the submitted documentation unless the PO 1) identifies such copyrighted data, and 2) grants to the Government, or acquires on behalf of the Government, a license to reproduce and distribute the data to these necessary recipients.

4.3.1.3 Submittal of Translated Data

For all documents submitted by the PO to the PSRP/GSRP that have been translated into English, the English translation shall be the official document.

4.3.1.4 Submittal of Toxicological Data for SSP and ISS Payloads (Flight Only)

The Shuttle/ISS payload safety review process requires biomedical safety assessments of potentially hazardous materials, such as chemicals, microorganisms, and radioisotopes. In order for these assessments to be available for the safety reviews, the JSC Toxicology Group requires POs to submit test sample data substantially in advance of the safety reviews. See JSC 27472, "Requirements for Submission of Test Sample-Materials Data for Shuttle Payload Safety Evaluations," current issue, for the timeline and data requirements for these early submittals. The PO must attach both the data submitted to JSC Toxicology Group and the JSC response (when available) to the applicable hazard report that is a part of the SDP. Should toxicology submittals involve proprietary data, see section 4.3.1.1.

4.3.1.5 Submittal of Export Control Data (Flight Only)

The export control data requirements in sections 4.3.1.5.1 and 4.3.1.5.2 apply to U.S. payload organizations only. In the event an IP SDP requires an international review, the IP PO shall distribute the data to the other ISS IP organizations.

4.3.1.5.1 ISS Payloads

Distribution of ISS payload safety data packages to the ISS IPs is a standard part of the payload safety review process.

The PO must identify the export control classification of the SDP payload data in its transmittal letter. The first page of the SDP must also identify the export control classification of the data.

The PSRP Executive Officer will not distribute an SDP with an unknown export control classification to the IPs. Safety reviews may be delayed or cancelled for ISS payloads with unresolved export control issues.

The PO's safety review presentation materials must have the same export control classification as the SDP submitted for review or a less restrictive export control classification.

4.3.1.5.2 Shuttle Payloads

Distribution of Shuttle payload safety data packages to the ISS IPs is not a standard part of the payload safety review process.

Shuttle payload safety data packages are not distributed to the IPs unless the PSRP identifies a specific need to do so. If a need is identified, the PSRP Executive Officer will work with the PO and the SSPs export control resources to obtain the export control classification of the SDP.

The PO may include the export control classification of the SDP payload data in its transmittal letter and on the first page of the SDP, if the classification is known prior to SDP submittal.

4.3.2 Hazard Reports

The purpose of the hazard reports is to document the PO's safety assessment in a manner that reflects how the payload design demonstrates compliance with the safety requirements. The hazard reports are used as a method to systematically assess compliance with the safety requirements.

The flight SDP submittal must contain all flight hazard reports; the ground SDP submittal must contain all ground hazard reports. Each hazard report must be signed and dated by the payload program manager prior to submittal. Hazard reports shall be prepared on JSC Form 542B, JSC Form 542B-1, or JSC Form 1230 (see section 11) or an equivalent form that contains all information required on the JSC forms. Section 7, organized by area of design, identifies minimum support data for flight hazard reports. JSC 26943 contains guidelines for preparing payload flight hazard reports.

Following any technical discussion, the PSRP/GSRP Chairman will provide a disposition for each hazard report. This disposition may take one of the following forms: 1) approved as written, 2) approved with modification, 3) approved with an action to be performed by the PO and/or PSRP/GSRP, and 4) not approved.

The PO is responsible for retaining and maintaining the original hazard reports after approval.

4.4 SAFETY REVIEW PRESENTATION

The PO should be prepared to present information submitted in the SDP to the appropriate safety panel during scheduled reviews (see sections 6.1.1 and 6.1.2). During reviews, the PO should provide briefing chart handouts sufficient for the number of people expected to attend the review.

SECTION 5
SAFETY REVIEW OVERVIEW

5.1 LOCATION

Safety reviews for payload design and flight operations are usually conducted at JSC. The safety reviews for GSE design and ground operations will normally be conducted at KSC. The PO shall coordinate the timing of the PSRP reviews with the PSRP Executive Officer. The PO shall coordinate the timing and location of the GSRP reviews with the GSRP Chairman.

5.2 INITIAL CONTACT MEETING

The PO may receive initial contact safety briefings by the JSC and KSC safety representatives. The JSC briefing, normally held during the first integration meeting at JSC, should be scheduled by contacting the Payload Integration Manager (PIM) at JSC. For ISS payloads, contact the ISS PIM. The KSC briefing is usually held in conjunction with the first Ground Operations Working Group (GOWG) meeting, which is scheduled through the assigned payload representative at KSC.

The briefing includes an overview of the technical and system safety requirements to be met by the PO, plus instructions for conducting the safety reviews. The PO should provide a schedule of payload milestones and request a phase 0 or phase I safety review when the payload design concept has been developed.

5.3 TYPES OF MEETINGS

Safety reviews may take place in person, via teleconference, or by correspondence. Review meetings may be formal or out-of-board as deemed appropriate by the Panel Chairman.

- Formal Meeting: Formal meetings constitute a gathering of the safety review panel, representatives of the PO, and the appropriate supporting technical staff.
- Out-of-Board Meeting: Out-of-board meetings do not require the full safety panel. Attendees may include the Panel Chairman, Safety representative(s), representatives of the PO, and others necessary to address the issues that may be involved.
- Safety TIM: The review panel and/or associated technical staff may convene upon request in order to assist in interpreting safety requirements or to coordinate safety analyses/issues prior to safety reviews. Requests for flight safety TIMs should be coordinated with the PSRP Executive Officer. Requests for Ground Safety TIMs should be coordinated with the GSRP Chairman. Material to be addressed during the TIM should be provided 14 calendar days prior to the TIM.
- Splinter Meetings: Splinter meetings may be held concurrently with a safety review to discuss detailed technical concerns.

5.4 PAYLOAD CATEGORIES

Traditional payload safety compliance assessment is accomplished using a phased safety review process (phases 0, I, II, III) that corresponds to the hardware conceptual, preliminary, and critical design review phases and verification/validation of the payload (see section 6). Successful completion of each safety phase is documented by SDP/HR submittals to and approval by the PSRP/GSRP.

To streamline this process, the PSRP has implemented procedures and data requirements to minimize formal PSRP review time for payloads with routine hazards/standard controls/verifications. This allows the PSRP to concentrate review time on payload systems with the highest hazard potential, "must-work" functions, and/or nonstandard controls and verification methods. POs may document routine hazards and standard controls and verifications on the JSC Form 1230, "Flight Payload Standardized Hazard Control Report."

Based on the phase I SDP, new payloads are categorized by the PSRP into one of three categories of complexity (basic, intermediate, or complex) with respect to hazard potential as shown in Table 5-1 below. The review process is then tailored to the complexity of the payload design and adequacy of documentation. In addition, the process permits all payloads to document standard hazards that have standard controls and verifications on JSC Form 1230, which may be approved by the PSRP without a formal PSRP meeting. Details concerning basic and intermediate categories are contained in sections 5.4.1 and 5.4.2, respectively. Complex payloads use the review process detailed in section 6. Reflown and series payloads use the review process outlined in section 9.

For IP-sponsored payloads, an additional simplified safety review process has been developed that facilitates increased IP cooperation, a decreased level of documentation required for submittal to the PSRP, and agreements on how to process payload hardware that represents the lowest risk for ISS stowage and/or operations. Only IP-sponsored hardware items that qualify as low hazard potential may use this simplified process. All other hardware items must use the process as dictated within table 5-1.

The definition of the simplified safety review process termed Basic (Category 1) is based on the constraints as listed within the JSC Form 907. Those payloads which do not meet the constraints of the Basic (Category 1) shall be classified as Category 2.

Table 5-1. - PAYLOAD CATEGORIES

Payload Category	Defined Hazards
Basic (1230) Basic (Category 1)	The only hazards identified are "standard" as specified on the JSC Form 1230. The appropriate hazard controls are found on JSC Form 1230. **<u>OR</u>** The only hazards identified are "standard" as constrained by the JSC Form 907. This use of this payload category is restricted to IP safety organizations that have committed to the May 2006, Multilateral Safety and Mission Assurance Panel (MSMAP) simplified payload safety process agreement and documentation of compliance to appropriate hazard controls is accepted upon submission of JSC Form 906.
Intermediate	1) The payload has "unique" hazards (i.e., hazards not found on the JSC Form 1230) but has controls and verification methods that have been historically accepted by the PSRP **<u>OR</u>** 2) The payload has "standard" hazards (i.e., hazards identified on the JSC Form 1230) but uses controls and verification methods other than those identified on the JSC Form 1230.
Complex	The payload has unique hazards with hazard controls that are: a. Active "must work" functions, such as electromechanical or pyrotechnic separation systems or actuators/mechanisms providing structural load paths, **<u>OR</u>** b. Nonstandard or have nonstandard verification methods that depart from historically accepted techniques, **<u>OR</u>** c. Operationally complex requiring flight or ground personnel intervention to assist in controlling the hazard.

If, after a payload category has been assigned, the PO a) identifies previously undefined hazards or b) implements design changes that may create new hazards, the PO must submit a revised SDP, which may result in a reclassification of the payload category.

5.4.1 <u>Review Process for Basic Payloads (Flight Only)</u>

Basic (1230) payloads (see Table 5-1, above) have a very low level of complexity, which may allow the payload to complete the safety process out of board. However, the PO will submit an SDP that will document the applicable hazards, controls, and verifications. Submittal will follow the standard procedure detailed in section 4.3.1, and approval may be obtained without a meeting. The following data are required for the simplified SDP for hardware design and flight operations:

- Brief description of the hardware design and flight operations with schematics and block diagrams, as appropriate
- Summary of the safety analysis results that documents compliance with the design, verification, and applicable on-orbit verification/reverification requirements for the identified standard hazards
- Documentation of all applicable hazards, controls, and verifications on hazard report(s) (e.g., JSC Form 1230/Form 542)
- Certificate of Payload Safety Compliance (JSC Form 1114A) signed by the Program Manager or Flight Safety Certificate (JSC Form 906)

  Basic (Category 1) payloads (see Table 5-1, above) also have a very low level of complexity and require only a subset of the data set as noted above for Basic (1230). This classification is reserved for IP-sponsored items (items that have been reviewed and approved by an IP safety organization that is part of the multilateral agreement), and as such, the IP only needs to send the following set of documentation to the PSRP:

- Completed JSC Form 906

  In addition to submitting this data, the IP will include the hardware in their Certification of Flight Readiness (CoFR) endorsement inputs for the relevant flight or stage. SDPs generated from IP safety analyses shall be maintained by the sponsoring IP for potential audit by the PSRP. Any partner may request a copy of the complete safety data package for review, if necessary. Should this request be made, the sponsoring IP is required to provide the package within two weeks of the request.

5.4.2 Review Process for Intermediate Payloads (Flight Only)

In addition to the standard hazards found in Basic payloads, the Intermediate payload has unique hazards that have standard controls and verification methods (including applicable on-orbit verifications/reverifications) that have been historically accepted by the PSRP. Intermediate category payloads should require one or two reviews of the unique hazards, but the basic hazards may be addressed on a Form 1230/Form 906 and approved out of board/accepted. The PSRP will determine the need for a second review for unique hazards at the completion of the first review. The determination will be based primarily upon the completeness and quality of the unique hazard reports. Requirements for SDP submittal are the same as those stated in section 4.3.1.

5.5 SCHEDULE OF REVIEWS/PHASES

The schedule for formal phase 0, I, and II payload safety reviews generally relates to the payload development schedule. Phase 0 is held during the concept phase or at the start of payload design. Phase I is near the Preliminary Design Review (PDR); phase II is near the Critical Design Review (CDR). The PO should set the review schedule to obtain maximum benefit to payload development based on the results of the safety reviews.

ISS payloads may include multiple major systems or components, each working to a unique schedule. These may be individually baselined and categorized (see section 5.4), which allows them to progress through the payload safety process in accordance with their own schedule (see section 8.2).

Phase III is associated with completion of payload safety verifications and/or the start of ground processing. When establishing a timeline for phase III, the PO should allow enough time to close potential issues that may result from a phase III review. The timing and completion of the phase III review and safety certification are critical to the launch schedule. The flight and ground phase III completion requirements restated below are in the current version of NSTS 1700.7 and NSTS 1700.7 ISS Addendum and apply to all payloads:

> The JSC and KSC Phase III safety review and ground safety certification must be completed 30 days prior to delivery of the payload, ASE, and GSE to the launch site…

If any verification items remain open on the flight hazard reports, the PO must provide rationale to support the safety of starting ground processing with these items open. The rationale is to be submitted to both the PSRP and GSRP. The PSRP will review the rationale and provide concurrence to the GSRP.

To schedule KSC Ground safety reviews, contact the GSRP Chairman; to schedule JSC Flight safety reviews, contact the PSRP Executive Officer (see section 4.3.1).

5.6 SAFETY REVIEW COMPLETION

5.6.1 Documentation of Phase Completion

During a formal meeting, the Panel Chairman will make an official announcement that the safety phase is complete or incomplete (open). This announcement will be recorded and distributed by the PSRP/GSRP in the official meeting minutes. Incomplete phases are usually attributable to overdue/open action items or unsigned (open) hazard reports. The PSRP/GSRP will issue official correspondence to document closure of open action items/signature of open hazard reports that occurs after the phase review. The correspondence that closes the last open action item/hazard report for that phase will include a statement that the safety phase is considered complete.

For out-of-board reviews, safety review process completion will be documented by formal correspondence.

5.6.2 Completion Criteria for Phase I, II, and III

Successful completion of phase I and II reviews is accomplished by obtaining approval (Panel Chairman’s signature) of hazard reports at the appropriate phase level and closure of applicable phase I/II action items.

After submission of all required data, the criteria for successful completion of the safety review process at the phase III level for both flight and ground reviews are as follows:

- All payload hazard reports are signed by the payload Program Manager and the Panel Chairman at the phase III level.
- All NCRs are approved.
- Safety review action items are formally closed in the safety review meeting minutes or documented closed in separate correspondence.
- A signed Certificate of Ground Payload Safety Compliance provided to the GSRP (for phase III ground safety).

Approval of the phase III safety data by the PSRP and GSRP is with the understanding that the data represent the actual design and operations of the payload. Should safety issues arise after the safety process is complete, the safety panels reserve the right to request additional data deemed necessary to reassess the payload.

5.6.3 Completion Criteria for Series/Reflight

The criteria for successful completion of a series or reflight safety review is that all data required by section 9, Reflown and Series Payload Hardware, have been submitted and approved.

5.7 POST PHASE III SAFETY ACTIVITY

5.7.1 Certificate of Flight Payload Safety Compliance/Flight Safety Certificate

A safety assessment must be conducted to determine the payload's safe operational life and safe design life, as defined on the Certificate of Payload Safety Compliance (JSC Form 1114A - NSTS 1700.7B, section 306, figure 3) or the Flight Safety Certificate (JSC Form 906).

The PO must present a signed Certificate of flight Payload Safety Compliance or final Flight Safety Certificate to the PSRP Executive Officer no later than 10 days prior to the Flight Readiness Review (FRR) or ISS Stage Operations Readiness Review (SORR) , whichever occurs first.

5.7.2 Configuration Control

When changes to the design, configuration, or operations of the payload are required subsequent to phase III, the PO shall assess those changes for possible safety implications, including the effect on all interfaces. The assessment shall be forwarded to the PSRP/GSRP for review and approval. If the change has ground safety implications, it must be reviewed with the KSC panel prior to proceeding with ground processing. New or revised hazard reports and support data shall be prepared where applicable and submitted for approval as indicated in section 4.3.1. The need for delta phase III safety reviews will be determined by the PSRP/GSRP Chairman. Satisfactory completion of these activities is mandatory prior to the start of affected ground activities or launch.

Any test failures, anomalies, or accidents involving payload flight hardware or software that occurs between the completion of phase III and launch must be promptly reported to the PSRP/GSRP. Safety impacts, if any, should be identified.

5.7.3 Verification Tracking Log

Open verification items must be tracked on a flight or ground safety Verification Tracking Log (VTL) (see section 11).

- Flight Safety: From Phase III until L-60 days, the PO shall update and provide the VTL to the PSRP Executive Officer once a month. From L-60 days until launch, the PO shall provide a weekly update to the VTL. All VTL open items must be closed no later than 4 p.m. Central time on the last business day prior to launch. Items that cannot be closed at this time will require the transmission of a facsimile closing the open VTL items to the Mission Evaluation Room (MER) at NASA JSC no later than L-6 hours. Contact the PSRP Executive Officer for MER delivery instructions.

- Ground Safety: The initial submittal of the ground safety VTL is required with the phase III ground SDP. Following the completion of the phase III review, the ground safety VTL shall be updated monthly prior to hardware arrival at KSC. If there are open flight verifications that are constraints to ground processing, the PO must also include those items of the flight VTL. After the delivery of the payload, ASE, or GSE to the launch site, the safety VTL(s) shall be updated at least weekly. More frequent updates to the safety VTL(s) may be required if the open items must be closed to allow work to continue.

5.7.4 Documentation of Safety Process Completion

Final flight safety approval is documented by the PSRP Chairmans signature on the CoFR for the planned flight. The CoFR will include IP certification of completion of the safety review of Category 1 (Basic) items and will be provided as part of CoFR inputs to the PSRP.

Final ground safety approval is documented by a letter from the KSC Director, Safety Assurance to the KSC Director, Customer Service Space Station and Shuttle Payloads Processing stating that the Ground Safety Review Process has been completed and the payload may begin ground processing.

SECTION 6
SAFETY PROCESS

6.1 GENERAL

6.1.1 Preparation

In preparation for a phase safety review, the PO will submit an SDP as indicated in section 4.3.1. If phase reviews are combined (e.g., a phase I/II review), the SDP shall include the data requirements that apply to all the appropriate phases. The depth and number of the planned reviews are dependent on the complexity, technical maturity, and hazard potential of the payload, and may be modified by the Panel Chairman in conjunction with the PO.

The PO should provide sufficient technical support personnel to answer questions posed by the PSRP/GSRP in support of the agenda items.

Listed below are general agenda topics for safety review meetings. These insure that the safety review meetings proceed smoothly and contain the necessary information to facilitate the review.

6.1.2 General Meeting Agenda Guidelines

The PO should coordinate all meeting agenda with the PSRP Executive Officer or the GSRP Chairman prior to the safety review meeting and provide the final agenda in advance. The fundamental elements of all Safety Review Meeting Agenda are as follows:

a. Introduction of the Meeting and Participants by the JSC Safety Reliability and Quality Assurance (SR&QA) Payload Safety Engineer (PSE).

b. Opening Remarks by Chairman and the Payload Program Manager.

c. Discussion of Pre-Review Activity Led by the PSE.

d. Program-level Overview (including areas of responsibility).

e. Program Milestone Schedule: Provide the Program Milestone Schedule, including, but not limited to,

   (1) design stages and reviews,

   (2) hardware/software build status,

   (3) testing and verification activities,

   (4) delivery, integration, and launch activities, and

   (5) safety review dates.

f. Mission Objectives, including overview of mission objectives and general criteria for a successful mission.

g. System/Subsystem Technical Presentation Overview, including enough information to allow the PSRP/GSRP to gain a general technical understanding of the systems involved in the payload operations. Highlight any design changes since the previous safety reviews.

h. Operations Overview, describing planned operations and known contingencies. Plan to discuss detailed operations that relate to payload safety in conjunction with the appropriate hazard report presentation. Highlight any operations changes made to the operations that impact the safety of the payload since the previous review.

i. Safety Assessment Summary, including safety assessments performed to identify hazards, any failures or anomalies that occurred after development testing, and the corrective actions. Present responses to agreements and formal action items, including a summary of open action items and associated plans for closure. Provide sufficient information to demonstrate that a comprehensive hazard analysis has been performed. Provide an overview of hazards and how they relate to the hazard reports, and discuss safety-related items that are not reflected in the hazard reports.

j. Phase-specific Topics: Additional, phase-specific topics for the agenda should be drawn from the data that are required to be included in the SDP for that phase (see sections 6.2.1, 6.3.1, 6.4.1, and 6.5.1). If not included as one of the general agenda topics, these data should be addressed as separate agenda items.

k. Hazard Report Presentation: Unless otherwise agreed to by the PSRP/GSRP, present all hazard reports in full, associated noncompliance reports/waivers/deviations, previously assigned action items/agreements that involved modification of hazard reports, and associated action item/agreement responses.

l. Action Item Review: Both the PO and the PSRP/GSRP will review and agree to actions and due dates assigned during the course of the safety review to ensure that there are no misunderstandings. These action items will be printed and signed during the review.

m. Closing Comments Payload Program Manager and Panel.

6.2 PHASE 0 SAFETY REVIEW

The optional phase 0 safety review is provided as a service to the PO. The objectives of the meeting are to:

- Assist the PO in identifying hazards, hazard causes, and applicable safety requirements early in the development of the payload.
- Adequately describe the hazard potential.
- Answer questions regarding the interpretation of the safety requirements or the implementation procedures of this document.
- Provide guidance to the PO for preparing the safety data required for subsequent safety reviews.

6.2.1 Phase 0 Data Requirements

The following data are required for the phase 0 SDP and must be submitted as stated in paragraph 4.3.1:

a. For payload design and flight operations:

(1) Conceptual payload description (including subsystems) and mission scenario.

(2) Description of safety-critical subsystems and their operations.

(3) Flight hazard reports (JSC Form 542B/Form 1230).

b. For GSE design and ground operations:

(1) Conceptual payload description and brief mission scenario.

(2) Conceptual GSE description and operations, and description of payload design that is safety critical during ground operations.

(3) Ground operations scenario.

(4) Ground hazard reports (JSC Form 542B).

The description of the payload and its operation must be of sufficient detail to permit identification of all subsystems that may create hazards. Emphasis should be given to those subsystems that store, transfer, or release energy. The descriptions of the safety-critical subsystems must be of sufficient detail to identify the hazards in terms consistent with the conceptual design. In addition, the PO shall address tentative plans for any flight operation (e.g., extravehicular activity, reverification of hazard controls) or ground operation that would require personnel certification to perform hazardous procedures.

6.2.2 Phase 0 Hazard Reports

The purpose of a phase 0 hazard report is to document and scope the specific hazards identified. It is intended to be a working document for discussion and critique at the phase 0 safety review and will not require signatures. A hazard report must be prepared for each unique hazard identified in the safety analysis. The hazards contained on the phase 0 hazard report must reflect the payload conceptual design and operations existing at the time of the phase 0 review. For phase 0, the PO may identify hazard controls, verification methods, or status of verifications.

6.3 PHASE I SAFETY REVIEW

The purpose of the phase I safety review is to obtain PSRP/GSRP approval of the updated safety analysis that reflects the preliminary design and operations scenario of the payload. At this point, the PO shall present a refined safety analysis that identifies all hazards and hazard causes inherent in the preliminary design; evaluates all hazards for means of eliminating, reducing, or controlling the risk; and establishes preliminary safety verification and on-orbit verification/reverification methods. The PO shall provide a preliminary identification of the payload interfaces and of the hazards presented by these interfaces.

6.3.1 Phase I Data Requirements

The following data are required for the phase I SDP and must be submitted as stated in paragraph 4.3.1:

a. For payload design and flight operations:

(1) Updated payload description (including subsystems) and mission scenario.

(2) Updated descriptions of safety-critical subsystems and their operations, including schematics and block diagrams with safety features, inhibits, and controls identified. Identify any safety-critical subsystems that are computer controlled, and identify the functional architecture associated with that computer control.

(3) Updated and additional flight hazard reports (e.g., JSC Form 542B/JSC Form 1230) including appropriate support data (see section 7). For payloads that have catastrophic hazard potential, document the verification program outlined in NSTS/ISS 18798.

(4) A summary list (in the payload description) of orbiter- and/or ISS program-provided critical services, and an explanation (in the appropriate hazard reports) of the orbiter and/or ISS services used to control and/or monitor payload hazards (NSTS 1700.7 and NSTS 1700.7 ISS Addendum, current version).

(5) For ISS payloads, a presentation of the Fire Detection and Suppression (FDS) implementation approach. For sub-rack payloads, the PO shall address the integrated system approach (using sub-rack services and/or ISS services) to fully define the FDS implementation strategy. In addition, submit JSC Form 1428 to document methods and verifications used to detect and suppress a fire event for each payload volume.

(6) Discussion of design features supporting verification/reverification of hazard controls on-orbit and associated constraints.

(7) A tabulated list of tentative toxic materials and support data per JSC 27472 (see section 4.3.1.4).

(8) A list of all battery types, their uses, manufacturer, and applications.

(9) A preliminary description of all pyrotechnic devices and their functions.

(10) Preliminary on-orbit maintenance safety assessment as outlined in NSTS/ISS 18798.

(11) A preliminary life safety assessment. Provide an updated list of payload hardware items that could create a hazardous condition if they were to remain in service past their certification (design and/or operational) expiration date. Include a description of the failure mode and potential hazard created, and identify the safe operational life and safe design life for each item along with sufficient supporting verification data.

b. For GSE design and ground operations:

(1) Updated payload description and brief mission scenario.

(2) Updated descriptions of GSE, payload subsystems that present a potential hazard during ground processing, and their ground operations. Schematics and block diagrams with safety features and inhibits identified should be included. Design data for hazardous systems (pressure, lifting, etc.) shall be summarized in a matrix. Contact the GSRP Chairman for sample formats.

(3) Updated ground operations scenario including postflight ground operations at the primary, alternate, and contingency landing site. The scenario should highlight unique payload requirements at the launch pad, such as continuous power through a T-0 umbilical.

(4) Updated ground hazard reports (JSC Form 542B) including appropriate support data.

(5) Ordnance data required by the current version of KHB 1700.7, Appendix D.

(6) Estimated KSC on-dock arrival date.

6.3.2 Phase I Hazard Reports

The PO shall prepare phase I hazard reports for each hazard identified as a result of the safety analysis for the preliminary design and operations scenario of the payload. Hazard reports shall be added to or deleted from those agreed to during phase 0 to reflect the updated safety analysis. Rationale for deleting a hazard agreed upon at phase 0 shall be presented during the phase I review.

For phase I, the PO shall identify hazard controls for each hazard cause identified at phase 0. A direct correlation between each hazard cause and the corresponding hazard control(s) must be clearly shown on the report. Sufficient supporting information detailing each hazard control must be provided.

Verifications should include the types of tests, analyses, inspections, or procedures to be used to verify each hazard control, including all orbiter- or ISS-provided services or interfaces, both prelaunch and on-orbit. A direct correlation between each verification method and the corresponding hazard control must be clearly shown on the report. Each verification item should be independent and have a designator that allows for individual tracking of verification status.

Manufacturing/assembly procedures/processes that are critical in controlling hazards that cannot or will not be verified by subsequent inspection or test must be verified during the manufacturing/assembly process. An independent verifier, as specified by the PO, shall attest to proper completion of the procedure/process. Critical procedures/processes, which require special monitored verification (Mandatory Inspection Points [MIPs]), shall be identified in preliminary fashion (NSTS 1700.7 and NSTS 1700.7 ISS Addendum, current version).

If available, the PO should provide a tentative schedule for completion of each verification task and correlate with the integration schedule.

6.4 PHASE II SAFETY REVIEW

The purpose of the phase II safety review is to obtain panel approval of the updated SDP that reflects the CDR-level design and operations scenario of the payload. The phase II safety analysis identifies all hazards and hazard causes; defines and documents implementation of a means for eliminating, reducing, or controlling the risks; and documents finalized, specific safety verification and on-orbit verification/reverification methods (test plans, analysis, and inspection requirements, etc.). Payload interfaces, mission and ground operations, procedures, and timelines that were not addressed during the phase I safety review shall be assessed for safety hazards. The payload interfaces to be assessed shall include those between the Shuttle and/or ISS and the payload and among the various components that make up the payload (the spacecraft, upper stages, space platforms, pallets, experiments, ASE, ancillary flight equipment, GSE, KSC Facilities, GFE, etc.). Newly identified hazards shall be documented in additional hazard reports. For this review, the PO should provide the estimated KSC on-dock arrival date.

6.4.1 Phase II Data Requirements

The following data are required from the PO for phase II and must be submitted as stated in paragraph 4.3.1:

a. For payload design and flight operations:

(1) Updated payload description (including subsystems) and mission scenario.

(2) Updated descriptions of safety-critical subsystems and their operations, including schematics and block diagrams with safety features and inhibits identified. Provide electrical schematics that clearly identify the required number of independent inhibits, controls, and monitoring provisions. Present a summary of the test and analytical efforts required to verify the intended performance of all safety-critical hardware.

For a computer-based control system that is used to prevent critical/catastrophic hazards, provide the following data/descriptions:

Functional architecture

Expected interactions

Results of unexpected interactions

Protections for common cause failures

Development process for databases, hardware, software, and hardware/software

(3) Updated and additional flight hazard reports (e.g., JSC Form 542B/JSC Form 1230), including appropriate support data (see section 7). For payloads that have catastrophic hazard potential, document the verification program outlined in NSTS/ISS 18798.

(4) Updated summary list and explanation of orbiter- and/or ISS-provided critical services.

(5) For ISS payloads, an update of the FDS implementation approach. Include information on use of forced air flow, wire derating, circuit protection, materials usage, parameter monitoring (fan speeds, temperatures, current, etc.) and responses to an out-of-limit condition, and suppression approach. For sub-rack payloads, the PO shall address the integrated system approach (using sub-rack services and/or ISS services) to fully define the FDS implementation strategy. Updated JSC Form 1428 to reflect specific test (or analysis) procedures to be used along with the schedule for completion of FDS verification tests, analyses, or inspections.

(6) Verification methods associated with hazard controls that require on-orbit verification and/or reverification and the applicable approach (include rationale, constraints, and detailed methodology.)

(7) An updated tabulated list of planned toxic materials and support data per JSC 27472 (see section 4.3.1.4). Updates should include changes in test materials, changes in test conditions, and any alternate test materials.

(8) Updated list of all battery types, their uses, manufacturer, and applications.

(9) A list of all pyrotechnic devices, their functions, chemical composition, critical components inspection plan, verification plan, and aging degradation evaluation plan.

(10) List of hazard controls that require crew procedures and/or training.

(11) A record of test failures, anomalies, and accidents involving qualification or potential flight hardware. Include a safety assessment for items which may affect safety.

(12) The status of all action items assigned to the PO during phase I.

(13) Detailed on-orbit maintenance safety assessment as outlined in NSTS/ISS 18798. Identify maintenance activities, safe access areas, and reverification of safety critical features.

(14) Update life safety assessment. Provide an updated list of payload hardware items that could create a hazardous condition if they were to remain in service past their certification (design and/or operational) expiration date. Include a description of the failure mode and potential hazard created, and identify the safe operational life and safe design life for each item along with sufficient supporting verification data.

b. For GSE design and ground operations:

(1) Updated payload description and brief mission scenario.

(2) Updated descriptions and matrices of the GSE, the payload subsystems that present a potential hazard during ground processing, and their ground operations. Include updated schematics and block diagrams with safety features and inhibits identified. Electrical schematics must show all payload/GSE grounding.

(3) Updated ground operations scenario, including postflight ground operations at the primary, alternate, and contingency landing sites.

(4) Updated and additional ground hazard reports (JSC Form 542B), including appropriate support data.

(5) Updated ordnance data required by the current version of KHB 1700.7, Appendix D.

(6) Updated KSC on-dock delivery date.

(7) Specific engineering drawings and stress analyses of subsystems when requested by the GSRP Chairman.

(8) A list of safety-related failures and mishaps that have occurred.

(9) The status of all action items assigned to the PO during phase I.

(10) A list of technical operating procedures that will be used at KSC with a preliminary designation as to which ones are considered hazardous.

6.4.2 <u>Phase II Hazard Reports</u>

The PO shall prepare the phase II hazard reports by revising the phase I hazard reports to reflect the completed payload design and flight/ground operating procedures. If the payload design changes from phase I to phase II so that a phase I hazard report may be deleted, present a brief statement of rationale for deleting the report in the phase II SDP. The GSRP/PSRP will disposition the hazard reports.

Address all critical procedures/processes, including the plan for verification. Verifications shall refer to specific test (or analysis) procedures and summarize pass/fail criteria to be used. Specify the schedule for the completion of each specific verification test, analysis, or inspection.

6.5 PHASE III SAFETY REVIEW

The purpose of the phase III safety review is to obtain PSRP/GSRP approval of the SDP and safety compliance data that reflects the safety verification findings. The focus of this review is to assess safety verification testing and analysis results. If verifications critical for establishing the acceptability of the fundamental design of the payload for safety are not completed prior to the phase III review, then subsequent reviews may be required prior to hazard report approval. All verifications that are open at the time of the phase III SDP submittal must be included on the safety VTL. Items listed on the VTL should be planned open work items, such as ground processing at KSC.

6.5.1 <u>Phase III Data Requirements</u>

The following data are required for the phase III SDP and must be submitted as stated in paragraph 4.3.1:

a. For payload design and flight operations:

(1) Final as-built payload description (including subsystems) and mission scenario.

(2) Updated descriptions that define the final configuration of the safety-critical subsystems and their operations, including schematics and block diagrams with the as-built payload safety features and independent inhibits, controls, and monitoring provisions identified. Address applicable features and constraints relating to on-orbit verification/reverification of hazard controls.

For a computer-based control system that is used to prevent critical/catastrophic hazards, provide verifications for the following:

Functional architecture

Expected interactions

Results of unexpected interactions

Protections for common cause failures

Flight article databases, hardware, software, and hardware/software operate as designed

(3) Updated (and additional, if required) flight hazard reports, including support data that reflect the final configuration of the as-built payload and planned use. For payloads that have catastrophic hazard potential, document the verification program outlined in NSTS/ISS 18798.

(4) Final summary list and explanation of orbiter- and/or ISS-provided critical services.

(5) For ISS payloads, a finalized FDS implementation approach. Include information on use of forced air flow, wire derating, circuit protection, materials usage, parameter monitoring (fan speeds, temperatures, current, etc.) and responses to an out-of-limit condition. For sub-rack payloads, the PO shall address the final integrated system approach (using sub-rack services and/or ISS services) to fully define the FDS implementation strategy. Final JSC Form 1428 to summarize the results of the completed tests, analyses, and/or inspections and refer to particular test reports by document number, title, and date.

(6) Updated (and additional, if required) verification methods associated with hazard controls that require on-orbit verification and/or reverification and the applicable approach (include rationale, constraints, and detailed methodology).

(7) A final tabulated list of toxic materials and support data per JSC 27472 (see section 4.3.1.4), including additions and changes in test materials, changes in test conditions, and any alternate test materials.

(8) A final list of all battery types, their uses, manufacturer, and applications.

(9) A final list of all pyrotechnic devices installed or to be installed on the payload. The list will identify for each cartridge the function to be performed, the part number, the lot number, and the serial number.

(10) Updated list of hazard controls that require crew procedures and /or training.

(11) An updated record of test failures, anomalies, and accidents involving qualification or potential flight hardware or baselined flight software if the software is used for hazard control. Include a safety assessment for items which may affect safety.

(12) The status of all action items assigned to the PO through phase II.

(13) Payload Flight Safety VTL (JSC Form 764).

(14) Identification of flight safety noncompliances. Flight safety NCRs must be approved as either a waiver or a deviation before the phase III safety review can be completed. A signed copy of each approved safety waiver and/or deviation shall be included in the phase III SDP attached to the appropriate hazard report.

(15) Final/updated on-orbit maintenance safety assessment as outlined in NSTS/ISS 18798.

(16) Final/updated life safety assessment. Provide a final listing of payload hardware items that could create a hazardous condition if they were to remain in service past their certification (design and/or operational) expiration date. Include a description of the failure mode and potential hazard created, and identify the safe operational life and safe design life for each item along with sufficient supporting verification data. Processing of final signed Certificate of Flight Payload Safety Compliance for Flight Safety Certificate shall be in accordance with section 5.7.1.

b. For GSE design and ground operations:

(1) Final as-built payload description and brief mission scenario.

(2) Updated descriptions and matrices defining the final configuration of the GSE, the payload subsystems that are potentially hazardous during ground processing, and their ground operations. Include updated schematics and block diagrams with the as-built safety features and inhibits identified.

(3) Updated and finalized ground operations scenario, including postflight ground operations at the primary, alternate, and contingency landing sites.

(4) Updated and additional ground hazard reports, including support data that reflect the final configuration of the as-built GSE and planned payload/GSE use.

(5) Updated and finalized ordnance data required by the current version of KHB 1700.7, Appendix D.

(6) Updated and finalized KSC on-dock delivery date.

(7) Specific engineering drawings and stress analyses of subsystems when requested by the GSRP Chairman.

(8) A summary and safety assessment of all safety-related failures and accidents applicable to payload processing, test, and checkout. Identify impact to the Space Shuttle, other payloads, and facilities.

(9) The status of all action items assigned to the PO through phase II.

(10) Finalized list of technical operating procedures that will be used at KSC with the hazardous procedures clearly identified. The list shall also state the proposed first use of the procedure at KSC.

(11) Verification that each payload flight system pressure vessel has a pressure vessel logbook that shows pressurization history, fluid exposure, and other applicable data. This verification should account for the planned testing at KSC.

(12) Payload Ground Safety VTL, if required.

(13) Certificate of Payload Safety Compliance (JSC Form 1114A) signed by the PO program manager for GSE design and ground operations.

(14) Procedural hazard control matrix that identifies hazard control criteria within the associated work-authorization documents for all procedural hazards. Contact GSRP Chairman for format.

(15) Identification of ground safety noncompliances. Ground safety noncompliances must be approved as either a waiver or a deviation before the phase III safety review can be completed. A signed copy of each approved waiver/deviation shall be included in the phase III SDP (see section 10).

6.5.2 Phase III Hazard Reports

The phase III hazard reports shall reflect the final, as-built design and operations of the payload and GSE. If the payload or GSE design is changed from phase II to phase III, so that a phase II hazard report may be deleted, provide in the phase III SDP a brief statement of rationale for deleting the report. By phase III, all safety analysis efforts should be completed. Verifications completed by phase III shall be indicated as such on the hazard report and shall refer to particular test reports, analyses reports, and/or inspection records by document number, title, and date. Additional information that may be required to support phase III verification closure includes the results of the completed tests, methods of verification, analyses, and/or inspections. Copies of the appropriate ground safety verification documentation shall be provided with the ground phase III hazard reports. This verification documentation shall consist of those items agreed to by the Payload Organization and the GSRP.

For those hazards controlled by the design-for-minimum-risk approach (per the current version of NSTS 1700.7, paragraph 200.2), in addition to data provided for phases I and II, the PO must provide additional data listed in section 7 of this document.

For payload systems having catastrophic hazard potential for the vehicle or crew as a result of operations in or near the vehicle, see paragraph 4.1.3.

6.5.3 Verification Tracking Log

All flight safety verifications that are still incomplete at Phase III, must be "closed" on the hazard report and transferred to the flight safety VTL for further tracking. This log will allow the PSRP Chairman to sign the hazard reports, indicating completion of the safety analysis, but with the understanding that approval for flight will be withheld until all flight verification activity is completed.

Similarly, all open ground verifications must be listed on the ground safety VTL. This log will allow the GSRP Chairman to sign the hazard reports, indicating completion of the ground safety analysis. Open ground verifications and open flight verifications that have been identified as a constraint against payload processing must be closed before the applicable ground operation can be performed.

SECTION 7
SUPPORTING TECHNICAL DATA SUBMITTALS

The information in this section applies to flight safety only, except for the data identified in sections 7.5 and 7.6, which applies to both flight and ground safety.

To further define the general data requirements in section 6, this section addresses SDP data submittals related to various technical disciplines to support hazard reports. Hazard reports (JSC Form 542 and Form 1230) must be supported by the minimum set of data as outlined below. Each such hazard report shall clearly identify the supporting data. This supporting data shall be submitted in one of the following manners: a) attached to the hazard report, b) as part of the SDP, or c) submitted to the PSRP Executive Officer/GSRP Chairman. This official submittal path is not intended to preclude direct technical coordination between the PO and the appropriate JSC/KSC technical disciplines.

Technical areas of design, such as structures, pressure vessels, and pressurized lines, fittings, and components are typically Design-For-Minimum-Risk (DFMR) areas of design. The data submittal requirements in sections 7.1 and 7.2 are the minimum DFMR requirements for those particular design areas. The remainder of section 7 contains the minimum data submittals required by the PSRP for either DFMR or failure tolerant designs.

7.1 STRUCTURES

7.1.1 Phase I

- Proposed Structural Verification Plan in accordance with NSTS 14046, “Payload Verification Requirements” and/or SSP 52005 “ISS Payload Flight Equipment Requirements and Guidelines for Safety Critical Structures.”
- Verification plans for structural integrity of payloads stowed or installed on ISS.
- Fracture Control Plan (FCP)
- If applicable, identify use of JSC-25863 Fracture Control Plan for JSC Flight Hardware (current revision) in the Safety Data Package and in the Fracture Control Summary Report.
- Damage Control Plan for all fracture critical and low-risk composite structures.
- Methodology for assurance of fastener integrity.

7.1.2 Phase II

- Final structural verification plan, including: 1) summary of design loads derivation leading to critical load cases, and 2) math model verification plan.
- Fracture control status (including parts categorization).
- Identification of Material Usage Agreements (MUAs) and Stress Corrosion Cracking Control Certifying Organization and point of contact information for structural materials, the failure of which would cause a hazard (including, but not limited to, stress corrosion, hydrogen embrittlement, and materials compatibility).
- For payloads stowed or installed on ISS, provide summary of verification approach to meet ISS on-orbit load requirements including crew-induced loads for the on-orbit stowed or installed configurations.

7.1.3 Phase III

- Structural Verification Report that provides a summary of verification tests/analyses/inspections results.
- Fracture control summary report.
- New/approved MUAs as defined in phase II.
- Documentation of compliance with fastener integrity program.
- For payloads that will be stowed or installed on ISS, provide summary of verification tests/analyses/inspection results to meet ISS on-orbit load requirements including crew-induced loads for the on-orbit stowed or installed configurations.
- Final Stress Corrosion Cracking Control Certification Compliance for structural materials.
- Final Loads Analysis Summary.

7.2 PRESSURIZED SYSTEMS (vessels, lines, fittings, components)

7.2.1 Phase I

- Preliminary pressurized system schematic and operating parameters (e.g., temperature, pressure and other environmental conditions).
- Preliminary summary of the derivation of system Maximum Design Pressures (MDPs) per NSTS 1700.7 and NSTS 1700.7 ISS Addendum.
- Preliminary list of all system working fluids, their complete chemical composition, amounts, potential hazards (e.g., flammability, explosion, corrosion, toxicity) and hazard category (e.g., catastrophic, critical, nonhazard).
- Summary of pressure vessel(s) design and qualification approach.
- Damage control plan and stress rupture life assessment (Composite Overwrapped Pressure Vessels (COPVs) only).
- Fracture Control Plan.
- Preliminary table to show compliance with pressure systems safety requirements with columns for: 1) Item - (lines and fittings, components, or pressure vessel), 2) Ultimate strength (design burst pressure), 3) system MDPs, 4) Safety Factor - (design burst pressure divided by MDP), 5) Safety Factor required by ‘1700, 6) Proof Factor (Maximum Test Pressure divided by MDP), 7) Leak rate method used for hazardous materials and 8) Containment integrity required (maximum allowed leak rate). If the Proof Factor will be less that 1.5 X MDP provide an explanation. See Appendix C, Table 1 (EXAMPLE), Pressure System Compliance.
- Proposed pressurized system(s) verification approach for controls to ensure pressure integrity.
- For fluids whose leakage is hazardous also include: Proposed pressurized system(s) verification approach including controls to prevent leakage (e.g., levels of containment, Design for DFMR).

- For the DFMR approach to protect against leakage that may cause a catastrophic hazard include: 1) identification of mechanical fitting and leakage certification approach for wetted areas. Consider all environments where leakage is hazardous (e.g., in the Shuttle Payload Bay (PLB)) and 2) preliminary identification of fusion and bi-metallic joints within the system.

7.2.2 Phase II

- Complete and updated pressurized system schematic(s) and operating parameters, addressing all pressurized hardware.
- Complete summary of the derivation of system MDP(s) per NSTS 1700.7 and NSTS 1700.7 ISS Addendum.
- Complete table of pressurized system hardware, MDP(s), proof pressure, ultimate pressure, resulting proof and ultimate safety factors and method of determining the safety factors (e.g., test, analysis, vendor data) should be fully disclosed except for information not yet available with respect to “Proof Factor (Maximum Test Pressure)” and “Leak rate method used for hazardous materials”.
- Updated list of all system working fluids, their complete chemical composition, amounts, identified hazards and hazard category. Status on pressure vessel(s) design and qualification.
- Fracture control status.
- Identification of MUAs on pressurized system materials the failure of which would cause a hazard (including, but not limited to, stress corrosion, hydrogen embrittlement, and materials compatibility [including working and cleaning fluids]).
- Final pressurized system(s) verification approach for controls to ensure pressure integrity including a summary of qualification and acceptance test plans and analyses.
- For fluids whose leakage is hazardous include: Final pressurized system(s) verification approach including controls to prevent leakage (e.g., levels of containment, DFMR). Include a summary of qualification and acceptance test plans and analyses.
- For the DFMR approach to protect against leakage that may cause a catastrophic hazard include: 1) summary of certification test plans and analyses to prevent leakage of wetted mechanical fittings, 2) identification of system fusion joints and their method of Nondestructive Evaluation (NDE). Identification of system bi-metallic joint(s), manufacturer and certification data, and 3) complete list of wetted materials and their compatibility rating with system and cleaning fluids. Define credible single barrier failures which may release fluid into a volume that is not normally wetted and provide a summary of maximum worst case temperatures which were considered.

7.2.3 Phase III

- Final pressurized system schematic(s) and operating parameters, addressing all pressurized hardware.
- Final MDP derivation summary and table of pressurized system hardware, including the “Proof Factor (Maximum Test Pressure)” and “Leak rate method for hazardous materials”.

- Final list of all system working fluids, their complete chemical composition, amounts, hazards and categories.
- Certification of pressure vessel(s) design, including qualification and acceptance test results.
- Fracture control summary report.
- New/approved MUAs as defined in phase II.
- For safe life and limited life pressure vessels, document existence of a Pressure Log, including log number.
- Summary of results from verification tests/analyses/inspections for controls to ensure pressure integrity.
- For fluids whose leakage is hazardous also include: Summary of results from verification tests/analyses/inspections for controls to prevent leakage.
- For the DFMR approach to protect against leakage that may cause a catastrophic hazard include: 1) summary of results from certification tests and analyses on wetted mechanical fittings, 2) final list of system fusion joints and results from NDE. Final list of system bi-metallic joint(s), manufacturer(s) and certification data, 3) final list of wetted materials and their compatibility rating with system and cleaning fluids.

7.3 PYROTECHNIC DEVICES

7.3.1 Phase I

- List of pyrotechnic devices and the functions performed.

7.3.2 Phase II

- Detailed drawings of devices.
- Chemical composition of any booster charge(s).
- Inspection plan(s) for critical components.
- Plan for evaluation of aging degradation.
- Verification plan summary, including acceptance and qualification approach(s) (including margin demonstration), in accordance with NSTS 08060, "System Pyrotechnic Specifications."

7.3.3 Phase III

- Summary of verification tests/analyses/inspections results.

7.4 MATERIAL FLAMMABILITY, TOXICITY, AND COMPATIBILITY

7.4.1 Phase I

- Approach used to assure materials compatibility and crew safety.

- A tabulated list of tentative toxic materials and support data per JSC 27472, “Requirements for Submission of Test-Sample Materials Data for Shuttle Payload Safety Evaluations” (see also section 4.3.1.4).

7.4.2 Phase II

- Materials compatibility status.
- Toxicological evaluation of test sample materials in accordance with JSC 27472.
- Offgassing test plan.
- Preliminary flammability assessment.
- Provide certifying organization point of contact information for Offgassing and Flammability.

7.4.3 Phase III

- Final materials compatibility status.
- Update to toxicological evaluation of test sample materials in accordance with JSC 27472.
- Flammability Assessment in accordance with JSC-29353, “Flammability Configuration Analysis for Spacecraft Applications.”
- Provide Certification for Offgassing and Flammability Compliance per document JSC-29353.

7.5 IONIZING RADIATION

7.5.1 Phase I

PSRP:
- Ionizing Radiation Source Data Sheet (JSC Form 44). To initiate the JSC Form 44 process, use the following web link for obtaining and submitting the JSC Form 44: http://srag.jsc.nasa.gov/form44/form44link.cfm.

GSRP:
- Forms in accordance with KNPR 1860.1, “KSC Ionizing Radiation Protection Program,” if required.

7.5.2 Phase II

PSRP:
- New/Updated JSC Form 44 must be submitted and obtained at the following web link: http://srag.jsc.nasa.gov/form44/form44link.cfm.

GSRP:
- Forms in accordance with KNPR 1860.1, “KSC Ionizing Radiation Protection Program,” if required.

7.5.3 Phase III

PSRP:
- Approved JSC Form 44.

GSRP:

- Forms in accordance with KNPR1860.1, “KSC Ionizing Radiation Protection Program,” if required.OP

7.6a NON-IONIZING RADIATION

7.6.a1 Phase I

PSRP:

- List of equipment that generates non-ionizing radiation (RF transmitters, light sources, etc.).

- Proposed Electromagnetic Interference (EMI)/Electromagnetic Compatibility (EMC) Test Plan, for Conducted Emissions (CE), Radiated Emissions (RE), Conducted Susceptibility (CS), and Radiated Susceptibility (RS); applicable tests as determined by the hardware’s intended application and criticality.

GSRP:

- Forms in accordance with KNPR1860.2, “KSC Non-ionizing Radiation Protection Program,” if required.

7.6.a2 Phase II

PSRP:

- Updated list of equipment that generates non-ionizing radiation, including expected nominal operational characteristics of all non-ionizing radiation sources.

- Final EMI/EMC Test Plan, for CE, RE, CS, and RS: applicable tests as determined by the hardware’s intended application and criticality.

GSRP

- Forms in accordance with KNPR1860.2, “KSC Non-ionizing Radiation Protection Program,” if required.

7.6.a3 Phase III

PSRP:

- Final list of equipment that generates non-ionizing radiation, including actual nominal operational characteristics of all non-ionizing radiation sources.

- Submit final report of Electromagnetic Effects Panel (EMEP) approval of relevant EMI/EMC test results, including any Tailoring Agreements (TIAs) approved by the EMEP.

GSRP:

- Forms in accordance with KNPR1860.2, “KSC Non-ionizing Radiation Protection Program,” if required.

7.6b NON-IONIZING RADIATION - LASERS

7.6.b1 Phase I

PSRP:

- Identify each laser, its operating location, and its complete beam path.

- Identify the laser hazard classification per ANSI Z136.1.
- Identify each laser's operating characteristics (wavelength(s), (Continuous Wave) (CW)/pulsed).
- For CW lasers, provide average and peak powers.
- For pulsed lasers, provide pulse shape and energy characteristics and repetition frequency.
- Provide the laser manufacturer's specification sheet, if available.
- Identify each laser's transmission characteristics (beam diameter and beam divergence at accessible apertures, intensity profile) (class 1M, 2M, 3R, 3B and 4 only). Preliminary Nominal Ocular Hazard Distance (NOHD) and/or Nominal Hazard Zone (NHZ) analysis including a list of assumptions used in the analysis (window transmission factors, maximum exposure durations, atmospheric attenuation, reflections, etc.) (class 1M, 2M, 3R, 3B and 4 only) as defined by the ANSI Z136.1.
- Preliminary description of controls and inhibits to contain laser beam or prevent inadvertent laser operation and/or crew exposure (interlocks, barriers, beam stops, etc.)
- Preliminary list of crew protective equipment (goggles, etc,), if required for hazard control.

GSRP:
- Forms in accordance with KNPR 1860.2, "KSC Non-ionizing Radiation Protection Program," if required.

7.6.b2 Phase II

PSRP:
- Final NOHD/NHZ analysis (class 1M, 2M, 3R, 3B and 4 only) as defined by the ANSI Z136.1.
- Final description of controls and inhibits to contain laser beam or prevent inadvertent laser operation and/or crew exposure.
- Final list of crew protective equipment (goggles, etc,), if required hazard control.
- Test plan for verifying operating and transmission characteristics of laser (class 1M, 2M, 3R, 3B and 4 only)

GSRP:
- Forms in accordance with KNPR 1860.2, "KSC Non-ionizing Radiation Protection Program," if required.

7.6.b3 Phase III

PSRP:
- Summary of verifications and test results

GSRP:
- Forms in accordance with KNPR 1860.2, "KSC Non-ionizing Radiation Protection Program," if required.

7.7 PAYLOAD COMMANDING

7.7.1 Phase I

- List of hazardous commands and implementation.

7.7.2 Phase II

- Updated list of hazardous commands and detailed implementation plan.

7.7.3 Phase III

- Verification of implementation plan.

7.8a ELECTRICAL (POWER, BONDING AND GROUNDING) SUBSYSTEMS

7.8.a1 Phase I

- Preliminary power distribution schematic(s) showing wire sizing and circuit protection.
- Preliminary bonding and grounding diagram/plan.

7.8.a2 Phase II

- Updated power distribution schematic(s) showing wire sizing and circuit protection.
- Final bonding and grounding diagram.

7.8.a3 Phase III

- As-built power distribution schematic(s) that show wire sizing and circuit protection.
- Summary of verification tests/analyses/inspection results for bonding and grounding.

7.8b AVIONICS CONTROL

7.8.b1 Phase I

- Preliminary diagram of safety-critical subsystems, that indicate inhibits, controls, and monitors.
- Preliminary verification approach for electrical safety-critical subsystems.
- Identify any usage of orbiter and/or ISS electrical service to control a hazard.

7.8.b2 Phase II

- Updated schematics of safety-critical subsystems that indicate inhibits, controls, monitors, and Orbiter interfaces.
- Verification approach (test pass/fail criteria) for each avionics leg of the hazard control/monitor subsystem, including test location (e.g., cargo integration test equipment stand [CITE], orbiter, payload rack checkout unit [PRCU], other) procedures, and test apparatus used in substantiating end function.

- Provide a "payload hazard event table" listing the subsystem interface connector, pin number, payload function nomenclature, and whether the pin is command, monitor, or power.

7.8.b3 Phase III

- As-built schematics of safety-critical subsystems that indicate inhibits, controls, monitors, and Orbiter interfaces.
- Summary of test results and summary of test procedures, including payload organization testing and/or fully integrated testing (e.g., CITE, orbiter, PRCU, or other).
- As-built/final "payload hazard event table."

7.8.c COMPUTER SYSTEMS (Avionics)

This section applies only to payload computer systems (as defined in SSP 50038 Appendix C) used to control hazardous functions.

7.8.c1 Phase I

- Identify computer system hazard controls.
- Describe the function(s) controlled by computer systems that prevent a hazard from occurring or control a hazardous function.
- Provide a block diagram of the Computer-Based Control System (CBCS) with all inhibits to a hazard identified and describe how the inhibits independently control the hazard, including clear identification of control paths or other independent inhibit CBCS control methods.
- Provide design features for CBCSs planned to control multiple inhibits to a hazard (i.e. designed to be greater than zero-fault tolerant).
- Describe the development process (including verification) of software/hardware and computer based control.

7.8.c2 Phase II

- Describe the independence of computer and non-computer methods of hazard control and update block diagrams that detail the control of inhibits to a hazard.
- Update the description of computer system hazard controls, and the function(s) controlled by computer systems that prevent a hazard from occurring or control a hazardous function, including design features for CBCSs controlling multiple inhibits to a hazard and designed to be greater than zero-fault tolerant.
- Summarize the functional testing of the software/hardware, and describe the verification approach for the computer based hazard control system.

7.8.c3 Phase III

- Provide a summary of results of computer based hazard control verification activity, including summaries of any failures/errors of the baselined flight software used for hazard control.

- Update CBCS hazard control diagrams to show independence of inhibits, and provide verification details for CBCS that controls multiple inhibits to a hazardous function that confirms fault tolerance of CBCS and independence of inhibits.

7.9 MECHANISMS IN CRITICAL APPLICATIONS

7.9.1a <u>Phase 0</u>

- Provide a draft Mechanical Systems Verification Plan (MSVP) approach.
- Where applicable simple mechanisms and/or design for minimum risk mechanisms design approaches are used, a request for approval shall be submitted to the Mechanical Systems Working Group (MSWG).

7.9.1b <u>Phase I</u>

- Preliminary MSVP identifying safety-critical mechanisms and design approach for each mechanism.
- Identification of areas of applicability of holding or operating force or torque margin requirements and planned verification approach (test or analysis).
- Formally request approval from the MSWG to pursue a simple mechanism approach, and/or to pursue a DFMR approach to any safety-critical mechanisms, prior to Phase 1 SDP submittal.
- Provide a Fault Tolerance Matrix for Fault Tolerant Mechanisms.
- Provide a tolerance analysis with tolerance stackup and thermal effects for all safety-critical mechanisms.
- Fracture Control Plan.

7.9.2 <u>Phase II</u>

- Final MSVP includes updates of critical procedures and processes to meet safety requirements using either a) failure tolerant approach or b) DFMR approach that required compliance with JSC letter MA0-00-057.
- Include fault-tolerance analysis for the safety-critical mechanisms explaining the independent success legs in place to meet fault-tolerance requirements and, if using DFMR approach, a completed matrix, detailing how each requirement in the MA2-00-057 Mechanical Systems Safety letter is or will be met for each mechanism relying upon a DFMR designation as a success leg.
- A complete discussion of the verification approach, including qualification and acceptance tests and analyses, for each critical mechanism operation or feature is required for the MSVP.
- List of MIPs.
- Fracture control status (including parts categorization).

7.9.3 Phase III

- Provide Mechanical Systems Verification Report (MSVR) that describes the verifications performed on all safety-critical mechanisms previously described in the MSVP and the results of those verification activities, and include any trade/special studies supporting mechanisms hazard reports.
- Fracture control summary report.

7.10 SOLID ROCKET MOTORS

7.10.1 Phase I

- Preliminary schematic showing electrical inhibits, controls and monitoring provisions to prevent premature firing.
- Preliminary characteristics of the Solid Rocket Motor (SRM).
- Preliminary SRM case Fracture Control Plan, preliminary SRM qualification plan with a history of the related, family of, rocket motors and propellants history.

7.10.2 Phase II

- Updated schematic showing electrical inhibits, controls, and monitoring provisions to prevent premature firing, including power sources, inhibit control command sources and static control devices. Independence of inhibits shall be clearly depicted.
- Updated characteristics of SRM, including motor manufacturer, total mass and type of propellant, propellant formulation/ingredients, motor/propellant explosive classification, and case description.
- Cutaway diagram of the initiator.
- Diagram of the safe-and-arm device, indicating design and operation.
- SRM case Fracture Control Plan.
- SRM qualification plan showing qualification analysis, qualification testing, and qualification of SRMs inspection to be used for acceptance of the SRMs with a history of the related, family of, rocket motors and propellants history.

7.10.3 Phase III

- Final schematic showing electrical inhibits, controls, and monitoring provisions to prevent premature firing, including power sources, inhibit control command sources, and static control devices. Independence of inhibits shall be clearly depicted.
- Final characteristics of SRM, including motor manufacturer, total mass and type of propellant, propellant formulation/ingredients, motor/propellant explosive classification and case description.
- A table listing the inhibits, when last cycled (actuated), and the final pre-launch state.
- Final cutaway diagram of the initiator.

- Updated diagram of the safe-and-arm device, indicating design and operation.
- SRM case fracture control summary.
- SRM qualification analysis summary, qualification testing summary (number of motor hot firings and family of motors operational performance), SRM NDE acceptance inspection summary with a history of the related, family of, rocket motors and propellants history.

7.11 BATTERIES

7.11.1 Phase I

- Preliminary list of type and number of cells and batteries, cell size (capacity), battery configuration, cell/battery chemistry, cell/battery manufacturer, model number(s), voltage, capacity, details of on-orbit operations, and documentation of anomalies.
- State whether on-orbit cell/battery charging is intended.
- Provide a copy of EP Form 03, as submitted to JSC-EP5 Battery Office, for each cell/battery model.

7.11.2 Phase II

- Updated list of type and number of cells and batteries, cell size (capacity), battery configuration, cell/battery chemistry, cell/battery manufacturer, and model number(s) and charging circuit.
- Electrical power diagram detailing cell/battery circuit diagram including charging circuit showing compliance with NSTS 1700.7 and NSTS 1700.7 ISS Addendum. See requirements in JSC 20793, “Crewed Space Vehicle Battery Safety Requirements.”
- Charging characteristics and procedures, e.g., pulse charging, charge rate, trickle charge rate, and method of charge termination.
- Describe on-orbit operations including charging, discharging, battery replacement, stowage and disposal procedures. Provide design details and a diagram for battery boxes that indicates materials of construction, absorbent material, venting provisions, minimization of hydrogen accumulation from aqueous electrolyte batteries, protective coatings on battery box interiors and on exposed cell terminals, and cell physical retention techniques.
- Verification plan, including qualification and acceptance tests.
- Diagram of charging devices, characteristics, and implementation procedures.
- Fracture control approach for battery cells where leakage causes a catastrophic hazard and for nickel-hydrogen batteries. (Refer to section 7.2 for data submittal on fracture critical pressurized components or pressure vessels).
- Update EP Form 03 for each cell/battery model (as submitted to EP5/Battery Office).

7.11.3 Phase III

- Final list of type and number of cells and batteries, cell size/battery configuration (capacity), cell/battery chemistry, cell manufacturer, and model number(s).

- Final circuit diagrams, including safety circuitry and charging circuit showing compliance with NSTS 1700.7 and NSTS 1700.7 ISS Addendum. See requirements in JSC 20793, “Crewed Space Vehicle Battery Safety Requirements.”
- Final on-orbit operations including charging and discharging, battery replacement, stowage and disposal procedures.
- As-built diagram/drawings for battery boxes that indicates materials of construction, absorbent material, venting provisions, minimization of hydrogen accumulation from aqueous electrolyte batteries, protective coatings on battery box interior and on exposed cell terminals, and cell physical retention techniques.
- Results of verification tests, analyses, and inspections.
- Fracture Control Summary Report for NiH_2, battery cells. Approved EP Form 03 for each cell/battery model.

7.12 FLUID PROPULSION SYSTEMS

7.12.1 Phase I

- Preliminary propulsion system schematic(s) and operating parameters (e.g., temperature, pressure, other environmental conditions, number of thrusters).
- Preliminary summary of the derivation of system MDP(s) per NSTS 1700.7 and NSTS 1700.7 ISS Addendum.
- Preliminary list of all system working fluids, their complete chemical composition, amounts, potential hazards (e.g., flammability, explosion, corrosion, toxicity) and hazard category (e.g., catastrophic, critical, non-hazard).
- Summary of pressure vessel(s) design and qualification approach.
- Fracture Control Plan.
- Safe distance assessment and planned thrust level(s) used to determine it.
- Preliminary schematic(s) showing flow control devices, their electrical inhibits and monitoring provisions to prevent premature firing. Proposed verification approach for controls to prevent premature firing.
- Proposed propulsion system(s) verification approach for controls to ensure pressure integrity.
- For fluids whose leakage is hazardous also include: Proposed propulsion system(s) verification approach including controls to prevent leakage. To protect against leakage that may cause a catastrophic hazard include: 1) identification of mechanical fitting and leakage certification approach for wetted areas. Consider all environments where leakage is hazardous (e.g., in the Shuttle PLB), 2) preliminary identification of fusion and bi-metallic joints within the system.
- For fluids whose leakage is hazardous also include proposed propulsion system(s) containment integrity (including controls) to prevent hazardous fluid leakage, and verification (leak test) method.

- Since fluid propulsion systems are normally pressure systems, the data requirements for 7.2 Pressure Systems are also applicable to 7.12 Fluid Propulsion Systems.

7.12.2 Phase II

- Complete and updated propulsion system schematic(s) and operating parameters, addressing all pressurized hardware.
- Complete summary of the derivation of system MDP(s) per NSTS 1700.7 and NSTS 1700.7 ISS Addendum. Complete table of propulsion system hardware, MDP(s), proof pressure, ultimate pressure, resulting proof and ultimate safety factors, and method of determining the safety factors (e.g., test, analysis, vendor data).
- Updated list of all system working fluids, their complete chemical composition, amounts, identified hazards, and hazard category.
- Status on pressure vessel(s) design and qualification.
- Fracture control status.
- Identification of MUAs on propulsion system materials the failure of which would cause a hazard (including, but not limited to, stress corrosion, hydrogen embrittlement, and materials compatibility [including working and cleaning fluids]).
- Updated safe distance assessment and planned thrust level(s) used to determine it.
- Updated schematic(s) showing flow control devices, and their electrical inhibits and monitoring provisions to prevent premature firing. Independence of inhibits shall be clearly depicted. Provide cut-away diagrams of the flow control devices. Final verification approach for controls to prevent premature firing.
- Final propulsion system(s) verification approach for controls to ensure pressure integrity, including a summary of qualification and acceptance test plans and analyses.
- For fluids whose leakage is hazardous also include: Final propulsion system(s) verification approach, including controls to prevent leakage. Include a summary of qualification and acceptance test plans and analyses.
- To protect against leakage that may cause a catastrophic hazard, include: 1) summary of certification test plans and analyses to prevent leakage of wetted mechanical fittings, 2) identification of system fusion joints and their method of NDE. Identification of system bi-metallic joint(s), manufacturer, and certification data, 3) complete list of wetted materials and their compatibility rating with system and cleaning fluids. Define credible single barrier failures which may release fluid into a volume that is not normally wetted and provide a summary of maximum worst case temperatures considered.
- Since fluid propulsion systems are pressure systems, the data requirements for 7.2 Pressure Systems are also applicable to 7.12 Fluid Propulsion Systems.

7.12.3 Phase III

- Final propulsion system schematic(s) and operating parameters, addressing all pressurized hardware.
- Final MDP derivation summary and table of propulsion system hardware.

- Final list of all system working fluids, their complete chemical composition, amounts, hazards, and categories.
- Certification of pressure vessel(s) design, including qualification and acceptance test results.
- Fracture control summary report.
- New/approved MUAs as defined in phase II.
- For safe life and limited life pressure vessels, document existence of a Pressure Log, including log number.
- Final safe distance assessment.
- Final schematic(s) showing flow control devices, and their electrical inhibits and monitoring provisions to prevent premature firing. Summary of results from verification tests/analyses/inspections for controls to prevent premature firing.
- Summary of results from verification tests/analyses/inspections for controls to ensure pressure integrity.
- For fluids whose leakage is hazardous also include: Summary of results from verification tests/analyses/inspections for controls to prevent leakage. To protect against leakage that may cause a catastrophic hazard, include: 1) summary of results from certification tests and analyses on wetted mechanical fittings, 2) final list of system fusion joints and results from NDE. Final list of system bi-metallic joint(s), manufacturer(s), and certification data, 3) final list of wetted materials and their compatibility rating with system and cleaning fluids.
- Since fluid propulsion systems are pressure systems, the data requirements for 7.2 Pressure Systems are also applicable to 7.12 Fluid Propulsion Systems.

7.13 SEALED CONTAINERS (STRUCTURES)

7.13.1 Phase I

- List the name of each sealed container.
- Provide preliminary identification of MDP, fluid(s), materials of construction for container enclosure, stored energy due to pressure, and environmental conditions.
- Confirm/show sealed container meets design requirements per NASA-STD-5003 or NASA-STD-5019, for sealed containers, respectively.

7.13.2 Phase II

- List the name of each sealed container and verify that information furnished at Phase I is still valid. If not, identify and explain changes.
- Provide preliminary summary of analyses and tests for each sealed container as required by pressure ratings and verification methods.

7.13.3 Phase III

- List the name of each sealed container and verify that information furnished at Phase II is still valid. If not, identify and explain changes.

- Provide final identification of MDP, fluid(s), materials of construction for container enclosure, stored energy due to pressure, and environmental conditions.
- Provide final acceptance rationale for each sealed container including a summary of any required analyses and tests.

7.14 EXTRAVEHICULAR ACTIVITIES

7.14.1 Phase I

- Identification of potential Extravehicular Activities (EVAs) including scheduled, unscheduled, and contingency including maintenance and retrieval. State which EVAs/EVA tasks are for mission success and which are intended as a hazard control.
- Preliminary safety assessment of payload hazards related to ISS/NSTS environment. (Reference: SSP50021, NSTS 1700.7B, NSTS 1700.7B ISS Addendum and JSC-28918).
- Description of hardware affect on ISS/NSTS floating potential.
- Description of EVA safety design features. (Reference: SSP50021, NSTS 1700.7B, NSTS 1700.7B ISS Addendum and JSC-28918).

7.14.2 Phase II

- Clarification of EVAs including scheduled, unscheduled, and contingency, identifying all EVA operational controls.
- Update description and verification approach (including qualification and acceptance test/analysis/inspections) used to address hazards related to EVA Payload and ISS/NSTS environments. (Reference: SSP50021, NSTS 1700.7B, NSTS 1700.7B ISS Addendum and JSC-28918)
- Update description of EVA hardware design features’ affect on ISS/NSTS floating potential; if the hardware impacts the ISS/NSTS floating potential, evidence of coordination with the space environments group must be provided.
- Supporting verification data to demonstrate compliance with applicable Interface Control Documents (ICDs).
- Updated description of EVA design features. (Reference: SSP50021, NSTS 1700.7B, NSTS 1700.7B ISS Addendum and JSC-28918)

7.14.3 Phase III

- Results of verification test, analyses, fit checks, and inspections.
- Final design information of any design features which may affect ISS/NSTS floating potential or create electrical shocks.
- Final verification data to demonstrate compliance to applicable ICDs.
- All safety non-compliance reports for external hardware shall have a concurrence signature from the EVA analysis integration team.

7.15 BIOLOGICAL MATERIALS

7.15.1 Phase I

- The Payload Organization shall provide a JSC form 713, "Inflight Biohazardous Materials Approval Form" via http://microbiology.jsc.nasa.gov/microbrb.htm per JSC-63828, "Biosafety Review Board Operations and Requirements Document".

7.15.2 Phase II

- The Payload Organization shall provide an updated JSC form 713, "Inflight Biohazardous Materials Approval Form" via http://microbiology.jsc.nasa.gov/microbrb.htm per JSC-63828, "Biosafety Review Board Operations and Requirements Document".

7.15.3 Phase III

- The Payload Organization shall provide a final JSC form 713, "Inflight Biohazardous Materials Approval Form" via http://microbiology.jsc.nasa.gov/microbrb.htm per JSC-63828, "Biosafety Review Board Operations and Requirements Document".

SECTION 8
VARIATIONS OF THE SAFETY REVIEW PROCESS

This section identifies variations of the safety review process described in section 6.

8.1 VARIATIONS FOR INTEGRATED MULTIPAYLOAD CARGO COMPLEMENTS

An integrated, multipayload cargo complement usually is an assembly of experiments mounted on or in a dedicated carrier, rack(s), module, or the orbiter or ISS. When an integrated, multipayload cargo complement has payload elements that are in various stages of development, the mission manager, who is responsible for integrating the payload into the orbiter or ISS, should submit separate SDPs for individual payload elements or appropriate groups for separate review.

The complete payload complement (all experiments and the carrier, rack, module, etc.), however, must be addressed together at an integrated phase III safety review. Hazards associated with the interaction between 1) two or more experiments, or 2) an experiment and the carrier, orbiter, or ISS must be addressed in an integrated hazard report and presented at phase III.

Many payloads will serve as "hosts" that provide services for experiments and other payloads. Developers that plan to extend host services to client experiments or payloads must document the adequacy of services that control hazards in a hazard report. Any limits or restrictions to the provided safety service must be clearly specified. The hazard report may reference a user's guide or Interface Control Document (ICD) as verification of hazard controls. Verifications apply to the overall design and include the specific verifications that assure that required services are present for each client experiment or payload. On-orbit verifications/reverifications must also be included.

8.2 VARIATIONS FOR ISS PAYLOADS

Since ISS payloads are subject to differing development schedules, mobility of hardware on-orbit, potential on-orbit upgrades/modifications, and extended lifetimes, a modular data documentation and review strategy is encouraged. For payloads with multiple independent or unique systems, SDPs should be a compilation of payload system-level assessments that documents safety compliance of payload hardware and operations for each payload system. SDPs should have chapters for each of these systems and shall contain an integrated safety analysis at the rack or carrier level. Assessment will include on-orbit verification/reverification of hazard controls where applicable. Cumulative and unique integrated hazards should constitute the final SDP chapter. The rack integrator will perform integrated assessments for payloads co-manifested in a rack. The process defined in section 5, if applicable, allows a payload to progress through the payload safety process in accordance with its own schedule.

8.2.1 <u>On-orbit Reconfigured Payloads</u>

On-orbit reconfigured payloads are defined as payloads that while on-orbit either 1) will be physically reconfigured by modular substitution/addition, or 2) will experience a change in planned use or manifested location.

Safety assessments will be subject to the series/reflown hardware process detailed in section 9 and will address on-orbit verification/reverification of hazard controls.

8.2.2 Payloads Returning to Earth

Return payloads are defined as payloads or elements of payloads that are manifested for return from ISS on the STS.

Payloads that were launched on the Space Shuttle, transferred to the ISS, and later will be returned on the Space Shuttle must address all hazards for Space Shuttle delivery and transfer to ISS, ISS integration and operations, ISS deintegration, transfer to the Space Shuttle, and Space Shuttle return in the initial phase I/II/III safety data packages and hazard reports. If there have been changes to the payload hardware, safety assessments will be subject to the series/reflown hardware process detailed in section 9 and will address on-orbit verification/reverification of hazard controls and waste materials.

Payloads or hardware that were not launched on the Space Shuttle but will return on the Space Shuttle must meet the requirements of NSTS 1700.7B, NSTS1700.7B ISS Addendum, and KHB 1700.7. Safety assessments will be subject to the series/reflight reflown hardware process detailed in NSTS/ISS 13830C, section 9 and will address on-orbit verification/reverification of hazard controls. The analysis will identify hazard controls that must be verified while on-orbit; integrated hazards; and postlanding hazards or hazardous operations that occur at the primary, alternate, and contingency landing sites.

8.3 VARIATIONS FOR SSP PAYLOADS

Where a payload design has not met a specific requirement in NSTS 1700.7b but can demonstrate it achieves an acceptable level of safety, the SSP may at its discretion direct the PO to process an Accepted Risk Hazard Report (ARHR) in lieu of an NCR. The PO will receive direction to proceed with the ARHR approach through their normal interactions with the PSRP and will utilize the existing Space Shuttle ARHR classification and process as noted within section 10.1.1.

SECTION 9
REFLOWN AND SERIES PAYLOAD HARDWARE

Reflown hardware is defined as payloads or elements of payloads that have flown on the Space Shuttle or ISS and are manifested for reflight. Series flight hardware is defined as payloads or elements of payloads that are of the same or similar design as previously flown hardware (NSTS 1700.7 and NSTS 1700.7 ISS Addendum, current version). “Series” is not an applicable category for GSE. Variations to the procedures of section 6 have been developed for series payloads and reflown hardware to eliminate unnecessary duplication of effort from previously accomplished safety activity.

The PO is responsible for the safety of the total payload/GSE, including the series/reflown elements and associated interfaces. To fulfill this responsibility, the PO shall assess the previously approved safety data of the series/reflown payloads, payload elements, or GSE for applicability to the new payload and make all appropriate changes. Changes that may warrant revisions to baseline hazard reports include such things as hardware redesign, operational changes, or the need for additional controls. When any revisions are made to baseline hazard reports, a new, unsigned version shall be submitted as part of the reflight package.

The safety certification responsibility, as well as the number and depth of the safety reviews, will be discussed and negotiated with the PO at an early payload integration meeting.

The following unique data for series/reflown payloads, payload elements, and associated GSE shall be submitted (per section 4.3) as a Reflight SDP:

a. Identification of all series/reflown payloads, payload elements, and GSE to be used and the baseline safety analyses by document number, title, and release date. If chemicals are used, provide a new list, even though the chemicals are the same as those used previously.

b. Assessment of each series/reflown payload, payload elements, and GSE to indicate that the proposed use is the same as currently approved (analyzed and documented).

c. New or revised hazard reports, additional data, and identification of hazard reports that are no longer applicable based on the reflight application. Identification and assessment of changes in hardware/software and operations that have any safety impact, including on-orbit verification/reverification of hazard controls.

d. A copy of the approved baseline phase III hazard reports (attachments not required).

e. Report on the completion and results of applicable safety verifications. Submission of safety VTL (JSC Form 764) that identifies all safety verifications from the applicable baseline hazard reports that must be reverified for the reflight mission. In addition, open verifications from new hazard reports must be included.

f. Assessment of all safety noncompliances.

g. Assessment of limited life items for reflown hardware, including an updated list of payload hardware items that could create a hazardous condition if they were to remain in service past their certification expiration date. Include a description of the failure mode and potential hazard created, and identify the safe operational life and safe design life for each item along with sufficient supporting verification data.

h. Description of maintenance, structural inspections, and refurbishment of reflown hardware and assessment of safety impact.

i. Assessment of all testing or ground/flight anomalies and failures during the previous usage of the series/reflown payload or payload element along with corrective action taken and rationale for continued use. (flight hardware/software only)

j. For flight reviews: A list of all pyrotechnic initiators installed or to be installed on the payload. The list will identify for each initiator the function to be performed, the part number, the lot number, and the serial number.

   For ground reviews: Verification that each payload flight system pressure vessel has a pressure vessel logbook that shows pressurization history, fluid exposure, and other applicable data. This verification should account for the planned testing at KSC.

k. Ionizing and non-ionizing radiation forms for each source within the flight hardware or GSE. A definitive statement of non-use is required in the event that no radioactive materials or ionizing sources are present on the reflight payload.

l. For payloads that flew and were assessed for safety on either the shuttle or the ISS and are being reflown on the other vehicle: Results of the assessment of the payload with respect to the safety requirements of the new host vehicle (Flight safety only: current versions of NSTS 1700.7 for the shuttle and the NSTS 1700.7 ISS Addendum for the ISS).

m. A final list of procedures for ground processing (ground only).

n. Certificate of Payload Safety Compliance or Flight Safety Certificate. (Note: For GSE design and ground operations, the Flight Safety Certificate is not an acceptable substitute).

o. A copy of the approved baseline phase III FDS form (ISS payloads only)

As noted within section 8.2, “Variations for ISS Payloads”, in certain instances in which simple payload hardware is either modified or reconfigured on-orbit and/or is planned for transport on a different vehicle than originally anticipated, a payload may demonstrate compliance to the requirements as noted above via a decreased data submittal (formal memorandum to be provided to the PSRP). This approach must be coordinated and approved by the PSRP Executive Officer (prior to submittal) and will require substantiating technical rationale. Items in the subject formal memorandum shall include (as a minimum) confirmation of the following:

a. The subject payload falls within the classification of a “series/reflight safety assessment” per NSTS/ISS 13830 section 9, and includes a reference to and confirmation of continued applicability of the baselined safety data package, hazard reports, and safety verification methods previously approved by the PSRP;

b. The updated on-orbit operations and/or planned transport introduces no additional hazards or required hazard control re-verifications (Example: The soft-stowed transport configuration falls within the originally-assessed/approved structural analysis with no required additional verification activity);

c. The originally-submitted JF-1114a/JF-906 remains valid for the updated on-orbit operations plan/return flight with no issues related to stated safe operations or safe design life (Note: Baselined safety certificate shall also be included);

d. There have been no safety-relevant anomalies/failures which have occurred with the hardware during on-orbit or ground operations;

During the coordination with the PSRP Executive Officer, additional information and/or requested clarifications may also be requested and shall be included within the formal memorandum as noted above

For series/reflown IP hardware transported to stowed and/or operated aboard the ISS and meeting the constraints of the Category 1 criteria as specified within section 5.4 (flight only), the following unique data for series/reflown payloads and payload elements shall be submitted (per section 4.3) as a reflight SDP:

a. Identification of all series/reflown payloads, payload elements, and GSE to be used and the baseline Flight Safety Certificate by document number, title, and release date.

b. Confirmation that the following statements are true:

(1) There have been no changes to the hardware or its configuration

(2) There have been no changes to the procedures

(3) There have been no anomalies with the use of the hardware

(4) All reverifications of hazard controls (if applicable) will be performed and completed prior to launch

SECTION 10
PAYLOAD SAFETY NONCOMPLIANCE REPORT

The PO shall meet all the requirements of the current versions of NSTS 1700.7, NSTS 1700.7 ISS Addendum, and KHB 1700.7 or process an ISS safety NCR and/or SSP ARHR for each specific case of noncompliance. The PO shall document each noncompliance and submit the completed NCR/ARHR form(s) to the PSRP or GSRP. Each NCR/ARHR shall refer to the applicable payload element, subsystem, or component(s) of the payload.

The PO must develop the acceptance rationale that explains the design features and/or procedures used to conclude that the noncompliant condition is safe. The PO shall attach the supporting data for the acceptance rationale to the NCR/ARHR.

Approval of an NCR/ARHR for the design or operation of one element, subsystem, or component of the payload will not relieve the PO of the responsibility to meet the requirement in any other element, subsystem, or component of the payload. The NCR/ARHR must be approved before the PSRP will approve the associated hazard report(s).

Ground NCRs shall be approved prior to the start of associated KSC ground operations that are impacted by the NCR. The GSRP has been granted the authority to approve NCRs that impact only ground processing and have no impact to the payload flight hardware design, flight operations, or flight safety.

10.1 NCR/ARHR SUBMITTAL AND PROCESSING

All NCRs/ARHRs shall be coordinated with the PSRP or the GSRP, as appropriate, as soon as it is determined that the safety requirement cannot be met.

NCRs/ARHRs for payload design and flight operations shall be submitted to the PSRP Executive Officer in accordance with section 4.3.1. For GSE design and ground operations (KSC), the NCR shall be submitted to the GSRP Chairman in accordance with applicable GSRP processes. If the NCR/ARHR involves payload design that could have an impact on ground operations, the NCR/ARHR shall be concurrently submitted to both the PSRP and the GSRP.

The PO shall ensure that the NCR/ARHR is processed through the appropriate SSP/ISS approval process and is responsible for the development and coordination of the NCR/ARHR presentation to the appropriate panel(s) and/or board(s).

10.1.1 SSP ARHRs

The PO shall document SSP ARHRs in accordance with NSTS 22254. SSP ARHRs are reviewed and approved via the SSP Program Manager in compliance with existing SSP Configuration Management (CM) agreements and processes.

10.1.2 ISS NCRs

The PO shall document all ISS NCRs via use of the form “ISS-CM-031, ISS Safety Non-Compliance Report”. ISS NCRs are reviewed/approved via the associated ISS NCR CM process as noted within SSP 50123.

PSRP chair approval of safety non-compliances that fall within the PSRP assessment as “equivalent safety” is a delegated authority from the ISS program and the processing of those NCRs shall fully comply with existing ISS CM agreements and processes.

"Equivalent safety" may be granted for noncompliant conditions that do not meet specific requirements in the exact manner specified; however, the payload design, procedure, or configuration satisfies the intent of the requirement by achieving a comparable or higher degree of safety. Criteria for establishing an "equivalent safety" is based on:

a. Use of alternative methods/controls;

b. Utilization of procedures, protective devices, preflight verification activities, and crew experience base;

c. Reduced time of exposure;

d. Likelihood/probability of additional failures after loss of first control/inhibit;

e. Reduction of hazard category, and/or other factors such as minimum of single fault tolerance (1FT) with a robust design.

Specific requirements and details with respect to this delegated authority and the scope of noncompliant conditions to which it applies will be addressed during the conduct of flight safety review meetings when an applicable noncompliant condition is identified. Under these circumstances, the NCR condition shall be documented on the HR, and the PSRP chair will disposition the NCR.

10.2 EFFECTIVITY

SSP payload ARHRs have an effectivity of one flight only. The PO has the responsibility to correct the noncompliant condition prior to reflight of the same payload or payload element, or prior to the flight of subsequent payloads of the same series.

ISS payload NCRs may have an effectivity of one or more flights or increments. The PO shall state the desired effectivity on the NCR form. The ISS program may concur with or limit the requested effectivity. After expiration of the effectivity and prior to reflight of the same payload or payload element, or prior to the flight of subsequent payloads of the same series, the PO has the responsibility to correct the noncompliant condition.

10.2.1 Waivers

Waivers are granted for noncompliant conditions that do not meet specific requirements.

Shuttle payload waivers have an effectivity of one flight only. The PO has the responsibility to correct the noncompliant condition prior to reflight of the same payload or payload element, or prior to the flight of subsequent payloads of the same series.

Station payload waivers may have an effectivity of one or more flights or increments. The PO shall state the desired effectivity on the NCR form. The ISS program may concur with or limit the requested effectivity. After expiration of the waiver's effectivity and prior to reflight of the same payload or payload element, or prior to the flight of subsequent payloads of the same series, the PO has the responsibility to correct the noncompliant condition.

10.2.2 Deviations

Deviations are granted for noncompliant conditions that do not meet specific requirements in the exact manner specified; however, the payload design, procedure, or configuration satisfies the intent of the requirement by achieving a comparable or higher degree of safety.

Both shuttle and station payload deviations may be approved for unlimited use. The effectivity is the applicable flight number or increment number and subsequent flight or increment numbers.

SECTION 11
LIST OF FORMS

This section contains a list of the forms POs may use in the flight and ground safety review processes.

11.1 JSC FORMS

Current versions of the JSC forms are available in electronic format on the NASA/JSC Payload Safety Home Page. Contact the JSC PSRP Executive Officer for the electronic address.

The PSRP will accept "equivalent" forms (i.e., those that contain all the required information) developed by the payload organization for the following:

JSC Form 542B	Hazard Report and Continuation Sheet
JSC Form 764	Verification Tracking Log
JSC Form 1114A	Certificate of Safety Compliance

The PSRP, however, will not accept substitute "equivalent" forms for the following:

JSC Form 44	Ionizing Radiation
ISS CM 031	International Space Station Non-Compliance Report
JSC Form 1230	Flight Payload Standardized Hazard Control Report
JSC Form 1428	Fire Detection and Suppression Reporting Form
JSC Form 906	Flight Safety Certificate
JSC Form 907	Multilateral Category 1 Constraints

11.2 KSC FORMS

Contact the KSC GSRP Chairman for the KSC forms.

KSC FORM 16-295	Radiation Use Request/Authorization (Radioactive Materials)
KSC FORM 28-34	Radiation Use Request/Authorization (Ionizing Machine/Device)
KSC FORM 16-294	Radiation Training and Experience Summary (Ionizing Radiation)
KSC FORM 16-353	Modification of Radiation Use Authorization
KSC FORM 16-447	Laser Device Use Request/Authorization
KSC FORM 28-626	Optical Device Use Request/Authorization
KSC FORM 16-451	Radiofrequency/Microwave System Use Request/Authorization
KSC FORM 16-450	Training and Experience Summary (Nonionizing Radiation Users)

APPENDIX A

APPLICABLE DOCUMENTS

APPLICABLE DOCUMENTS

The latest revision and changes of the following documents are applicable to the extent stated herein. These documents can be accessed through the Payload Safety website: http://wwwsrqa.jsc.nasa.gov/pce or the KSC GSRP website: http://kscsma.ksc.nasa.gov/GSRP/index.htm. Documents not available on the website may be obtained from the PSRP Executive Officer or GSRP Executive Secretary.

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
NSTS 1700.7, Safety Policy and Requirements for Payloads Using the Space Transportation System.	1, 4.1, 4.2, 5.5, 6.3.1.a(4), 6.3.2, 6.5.2, 7.2.1, 7.2.2, 7.11.2, 7.11.3, 7.12.1, 7.12.2, 8.2.2, 9, 10
NSTS 1700.7 ISS Addendum, Safety Policy and Requirements for Payloads Using the International Space Station.	1, 4.1, 5.5, 6.3.1.a(4), 6.3.2, 7.2.1, 7.2.2, 7.11.2, 7.11.3, 7.12.1, 7.12.2, 8.2.2, 9, 10
KHB 1700.7/45 SW HB S-100, Space Shuttle Payload Ground Safety Handbook.	1, 6.3.1.b(5), 6.4.1.b(5), 6.5.1.b(5), 8.2.2, 10
NSTS 07700 Volume V, Information Management Requirements.	3.2
SSP 50223, International Space Station Export Control Plan.	3.2
NSTS/ISS 18798, Interpretations of NSTS/ISS Safety Requirements.	4.1.3, 6.3.1.a(3), 6.3.1.a(10), 6.4.1.a(3), 6.4.1.a(13), 6.5.1.a(3), 6.5.1.a(15)
JSC 26943, Guidelines for Preparation of Payload Flight Safety Data Packages and Hazard Reports for Payloads Using the Space Shuttle.	4.3, 4.3.2
JSC 27472, Requirements for Submission of Data Needed for Toxicological Assessment of Chemicals and Biologicals to be Flown on Manned Spacecraft.	4.3.1.4, 6.3.1.a(7), 6.4.1.a(7), 6.5.1.a(7), 7.4.1, 7.4.2, 7.4.3
NSTS 14046, Payload Verification Requirements.	7.1.1
SSP 52005, ISS Payload Flight Equipment Requirements and Guidelines for Safety Critical Structures.	7.1.1
NSTS 08060, Space Shuttle System Pyrotechnic Specification.	7.3.2
NSTS 22648, Flammability Configuration Analysis for Spacecraft Applications.	7.4.3
NSTS 22254, Methodology for Conduct of Space Shuttle Program Hazard Analyses.	8.3

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
KHB 1860.1, KSC Ionizing Radiation Protection Program.	7.5.1, 7.5.2, 7.5.3
KHB 1860.2, KSC Non-ionizing Radiation Protection Program.	7.6.1, 7.6.2, 7.6.3
SSP 50038, Computer-Based Control System Safety Requirements.	7.8c
JSC 20793, Crewed Space Vehicle Battery Safety Requirements.	7.11.2, 7.11.3
NASA-STD-5003, Fracture Control Requirements for Payloads Using the Space Shuttle.	7.13.1
NSTS 22254, Methodology for Conduct of Space Shuttle Program Hazard Analyses	10.1.1
SSP 50123, Configuration Management Handbook	10.1.2

APPENDIX B

ACRONYM LIST

ACRONYM LIST

ANSI	Approved American National Standard
ARHR	Acceptance Risk Hazard Report
ASE	Airborne Support Equipment
CDR	Critical Design Review
CITE	Cargo Integration Test Equipment
CM	Configuration Management
COFR	Certificate of Flight Readiness
COPV	Composite Overwrapped Pressure Vessels
CW	Continuous Wave
DFMR	Design for Minimum Risk
DSO	Detailed Supplementary Objective
DTO	Detailed Test Objective
EAR	Export Administration Regulations
FDS	Fire Detection and Suppression
FRR	Flight Readiness Review
GFE	Government Furnished Equipment
GOWG	Ground Operations Working Group
GSE	Ground Support Equipment
GSRP	Ground Safety Review Panel
HTD	HEDS Technology Demonstrations
ICD	Interface Control Document
IP	International Partner
ISS	International Space Station
ISSP	International Space Station Program
ITAR	International Traffic in Arms Regulations
JSC	Lyndon B. Johnson Space Center
KSC	John F. Kennedy Space Center
LASER	Light Amplification by the Stimulated Emission of Radiation
MDP	Maximum Design Pressure
MER	Mission Evaluation Room
MIP	Mandatory Inspection Point
MSMAP	Multilateral Safety and Mission Assurance Panel
MUA	Material Usage Agreement
NCR	Noncompliance Report
NASA	National Aeronautics and Space Administration
NHZ	Nominal Hazard Zone
NOHD	Nominal Ocular Hazard Distance
NSTS	National Space Transportation System

PDIM	Payload Developer and Integration Manager
PDR	Preliminary Design Review
PIM	Payload Integration Manager
PO	Payload Organization
PRCU	Payload Rack Checkout Unit
PSE	Payload Safety Engineer
PSRP	Payload Safety Review Panel
RF	Radio Frequency
RME	Risk Mitigation Experiment
SDP	Safety Data Package
SMP	Space Medicine Program
SORR	Stage Operations Readiness Review
SR&QA	Safety, Reliability, and Quality Assurance
SSP	Space Shuttle Program
SSP	Space Station Program
TIM	Technical Interchange Meeting
VTL	Verification Tracking Log

APPENDIX C

PRESSURE SYSTEM COMPLIANCE

Table 1 (EXAMPLE)

Pressure System Compliance								
Components	**Ultimate Strength (design burst pressure – (psig)[1]**	**Proof pressure (psig)**	**System MDP (psig)[2]**	**Ultimate Safety Factor - (design burst pressure divided by MDP)**	**Minimum Ultimate Safety Factor Required by '1700**	**Proof Factor (Maximum Test Pressure Divided by MDP)[3]**	**Leak Rate Method Used[4]**	**Containment Integrity Pass/Fail Criteria**
Components					2.5			
i.e. GN2 isolation valve (list all the compnents)	1000	150	100	1000/100 = 10	2.5	150/100 = 1.5	Bubble Soap	No Bubbles Detected
Lines and fittings					4			
Lines (list the different size lines)	5000	150	100	50	4	1.5	Bubble Soap	Bubbles Detected
Fittings (list the different fittings)	4000	150	100	40	4	1.5	Bubble Soap	Bubbles Detected
Pressure Vessel					**See note 5**			
Pressure Vessel (show each pressure vessel)	4000	3000	2000	2	2	1.5	Helium Mass Spectrometer	< 10^{-7} sccs

[1] Ultimate strength (design burst pressure) may be determined by analysis, test, or manufacturers rating

[2] Within a pressure system there may be more than one MDP

[3] If Proof factor is not equal to or greater than 1.5 X MDP explain the reason

[4] Describe the leak test method used (submersion in water, no bubbles; pressure decay, etc)

[5] Small pressure vessels may comply with ASME code, SF of 4 or greater, or space flight rated may be as low a SF of 2 (SF of 1.5 is no longer allowed)