JSC 26943

GUIDELINES FOR THE PREPARATION OF PAYLOAD FLIGHT SAFETY DATA PACKAGES AND HAZARD REPORTS

FOR PAYLOADS USING THE SPACE SHUTTLE

FEBRUARY 1995

National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas

JSC 26943

GUIDELINES FOR THE PREPARATION OF PAYLOAD FLIGHT SAFETY DATA PACKAGES AND HAZARD REPORTS FOR PAYLOADS USING THE SPACE SHUTTLE

February 17, 1995

PREPARED BY:

LELAND D. HILL, P.E.
LSIS PAYLOAD SYSTEM SAFETY
ENGINEER

APPROVED BY:

RICHARD S. SERPAS
EXECUTIVE SECRETARY,
SPACE SHUTTLE PAYLOAD
SAFETY REVIEW PANEL

DESCRIPTION OF CHANGES TO

GUIDELINES FOR THE PREPARATION OF PAYLOAD

FLIGHT SAFETY DATA PACKAGES AND HAZARD REPORTS

FOR PAYLOADS USING THE SPACE SHUTTLE

CHANGE NO.	DESCRIPTION/AUTHORITY	DATE	PAGES AFFECTED
--	BASIC DOCUMENT	2/17/95	All

Note: Dates reflect latest signature date of Revision.

FOREWORD

The Payload Safety Review Panel (PSRP) is responsible for conducting safety reviews necessary to assure the implementation of the payload safety requirements defined in NSTS 1700.7, "Safety Policy and Requirements for Payloads Using the Space Transportation System." The scope of this responsibility encompasses an assessment of the design and flight operations of payloads and experiments prior to flight aboard the Space Shuttle and the International Space Station Alpha (ISSA).

NSTS 13830, "Implementation Procedure for NSTS Payloads System Safety Requirements," provides instructions to payload customers for preparation of data and conduct of the payload safety reviews required for the PSRP to assess compliance with NSTS 1700.7 payload safety requirements. While NSTS 13830 provides general instructions for the content of the Safety Assessment Report (SAR), it does not provide specific guidelines for the preparation of an acceptable SAR. Because of the wide variance in the completeness of data being provided to the PSRP in support of the safety review process, the PSRP conducted an internal review of the payload safety process to identify areas where additional guidance to payload customers could simplify preparation of the required data submittal and enhance the efficiency of the review process. This guidelines document is the result of one of the recommendations assessed during that review process. The purpose of this document is to assist payload customers in preparation of an SAR and related payload hazard reports (HRs). This document addresses only the flight safety review process. A separate SAR addressing additional requirements related to ground processing of payload equipment is required for the ground safety review process.

This document is divided into two parts. Part I provides instructions and guidelines for the development of the SAR descriptive text. Part II contains instructions and guidelines for preparation of payload hazard reports and their required support data. Note that while the formal requirements documents identify the data submittal to the PSRP as an SAR, the more common designation of the Payload Safety Data Package (PSDP) has been used throughout this document.

TABLE OF CONTENTS

PART I
GUIDELINE INSTRUCTIONS FOR THE PREPARATION AND MAINTENANCE OF THE PSDP

1.0 INTRODUCTION 1

2.0 PURPOSE 1

3.0 SCOPE 1

4.0 GENERAL INSTRUCTIONS 1
4.1 PSDP Scope 1
4.2 PSDP Data 1
4.3 Reflown Designs 2
4.4 Change Indentification 2
4.5 Page Identification 2

5.0 FORMAT AND CONTENT 2
5.1 Foreword 2
5.2 Table of Contents 2
5.3 List of Tables and Figures 2
5.4 List of Payload Unique Acronyms and Definitions 2
5.5 Introduction 2
5.5.1 Purpose 2
5.5.2 Scope 2
5.5.3 Safety Analysis 3
5.5.4 Safety Status Summary 3
5.5.4.1 Action Items (AI's) 3
5.5.4.2 Noncompliance Reports (NCR's) 3
5.5.4.3 Operational Controls Identification 3
5.6 Applicable Documents 3
5.7 Payload Description 3
5.8 Ground Operations 3
5.9 Flight Operations 3
5.10 Detailed System Descriptions 3
5.11 Summary of Safety Analyses 4
5.12 Summary of Verifications 4
5.13 Orbiter (SL, SH, etc.) Interfaces and Services 4

PART II
GUIDELINE INSTRUCTIONS FOR THE PREPARATION
OF PAYLOAD HR'S

1.0 INTRODUCTION 5
1.1 Purpose 5
1.2 Background 5
1.3 Scope 5

2.0 INSTRUCTIONS FOR USE 5
2.1 General 5
2.2 Hazard Lists and the Hazard Catalog 6
2.3 HR Composition 6
2.3.1 Hazard Potential/Hazard Categorization 6
2.3.2 Hazard Groups 6
2.3.3 Hazards 6
2.3.4 Hazard Description 7
2.3.5 Safety Requirements 7
2.3.6 Hazard Causes 7
2.3.7 Hazard Controls 7
2.3.8 Verification Methods 7
2.3.9 Status of Verification 7
2.3.10 Supporting Data 8
2.3.11 References 8
2.4 General Comments Applicable to All HR's 8
2.4.1 Number and Title 8
2.4.2 System Description 8
2.4.3 Electrical Inhibits 8
2.4.4 Level of Detail 8
2.4.5 Separation of Hazards 8
2.4.6 Combining Subsystems 8
2.4.7 Deleting HR's 9
2.5 HR Interdependence 9
2.6 Interface HR's 9

3.0 GUIDELINE HAZARD REPORTS 10
Toxic Material Offgassing (Crew Cabin Materials) 11
Broken Glass 13
Excessive Ionizing Radiation 15
EVA Contact Hazards 17
IVA Touch Temperature 20
IVA Crew Contact Hazards 21
Electrical Shock 22

Crew Exposure to LASER Emissions 24
Electrical Shock from Physiological Test Equipment 26
Battery Leakage/Rupture 28
Use of Flammable Materials 31
Hazardous Fluids Leakage in the Payload Bay 33
Ignition of Flammable Atmospheres 35
Electrical Power Distribution Circuitry Damage 37
Radio Frequency Radiation Interfering With STS Circuitry and/or Other Payloads 39
Exposure of the Orbiter/Payload to Excessive Levels of EMI Radiation 41
Rupture and/or Explosion of Pressure System 42
Leakage/Rupture of Sealed Containers 47
Structural Failure 49
Failure of Rotating Equipment 53
Safety Critical Mechanical System Functional Failure or
Partial/Incomplete Deployment/Jettison 55
Collision/Impact During Planned Deployment 58
Premature/Inadvertent Pyrotechnic Device Operation 60
Must Work Pyrotechnics/Debris Generation 62
Collision Following Premature/Inadvertent Appendage Deployment or
Payload Release/Deployment 65
Premature/Inadvertent Liquid Engine or Attitude Control System Operation 67
Premature/Inadvertent Solid Rocket Motor Firing 70

4.0 KEY DOCUMENT REFERENCES 73

APPENDIX A: ACRONYMS AND ABBREVIATIONS 74

PART I
GUIDELINE INSTRUCTIONS FOR THE PREPARATION AND MAINTENANCE OF THE PSDP

1.0 INTRODUCTION

The data requirements for all flight safety reviews (phases 0/I/II/III) are specified in NSTS 13830. Among these data requirements are standard items such as payload description, mission scenario, identification, description and operation of safety critical subsystems, and HR's. This document is divided into two parts, the first covering the information to be contained within the body of the PSDP, and the second containing guidelines for preparing HR's in general with detailed guidelines for the more common HR's.

2.0 PURPOSE

The purpose of this instruction is to outline a format and to provide guidelines for preparing and submitting data for evaluation by the PSRP, and to enhance the efficiency of the payload safety review process. This instruction will also identify non-mandatory data which can augment a thorough technical review.

3.0 SCOPE

This instruction is applicable to all Space Shuttle payloads including deployable and non-deployable payloads manifested in the PLB, payloads in the crew cabin and/or middeck and experiments stowed or conducted in other habitable environments (e.g., Spacelab, Spacehab modules). The data format and content specified in this instruction applies to data submitted for the flight safety reviews (phases 0, I, II, and III).

4.0 GENERAL INSTRUCTIONS

4.1 PSDP Scope

The PSDP must comply with the instructions, definitions, and requirements specified in NSTS 13830. The PSDP will be reviewed in detail by the PSRP during the payload safety review process and will provide the basis for PSRP acceptance and the flight safety certification of the payload. Additionally, the PSDP will be used by the SSP Mission Operations Directorate during pre-mission planning and to make payload-related safety decisions during the actual shuttle mission.

4.2 PSDP Data

The PSDP should contain or summarize all data necessary to substantiate the safety of the payload and its design compliance with the requirements specified in NSTS 1700.7. Certain detailed information need not be delineated if adequately summarized and referred to. The PSDP should be logically organized and cross-referenced where possible to enhance accuracy and reduce duplication. However, some caution must be used throughout the PSDP preparation process with regard to determining whether certain data should be included, omitted, cross-referenced, or restated. Specifically, if the omission or referring to (versus restating) of certain safety related data would detract from the ability of the PSRP to accurately assess the safety of the system design under its planned use, then this data should be explicitly stated. For example, if the design fault tolerance or inhibit structure will be compromised during the nominal, planned mission, this must be accurately explained in the PSDP to support the safety assessment, design/usage acceptance, and the development of any operational hazard controls.

4.3 Reflown Designs

Re-submittal of detailed safety data related to previously approved hardware will only be required to the extent specified in NSTS 13830, paragraph 8.0., "Series Payloads and Reflown Hardware."

4.4 Change Indentification

Whenever changes to the PSDP are incorporated either between reviews or subsequent to a formal data submittal to the PSRP, such changes should be identified. The use of change bars is the preferred method to identify changes in a PSDP. Indexed comments to the changes may be included to explain or justify any changes.

4.5 Page Identification

Each page of the PSDP must be discretely numbered. Each page of each HR shall be labeled with the HR number. Each data submittal to the PSRP must have the total number of pages identified. A signature page is also required to document the concurrence by the payload program manager.

5.0 FORMAT AND CONTENT

5.1 Foreword

This is a general section that should be used for administrative data and to enhance cooperation, coordination, and understanding between the payload organization and the PSRP. The type of information requested are the names, phone numbers, and mailing addresses of participants significant in the development of the PSDP data (e.g., the payload developer and Program Manager, safety engineer, subsystem engineers, etc.). Such information will be used by the PSRP to identify points of contact to clarify the data or resolve technical issues, subject to any restrictions specified by the payload organization.

5.2 Table of Contents

5.3 List of Tables and Figures

5.4 List of Payload Unique Acronyms and Definitions

The number and the reuse of acronyms make the preparation of a glossary of acronym definitions necessary. The list should contain all acronyms and abbreviations that are used within the text of the PSDP, the HR's, and any diagrams or figures.

5.5 Introduction

This is a general section that should be used to describe the data being provided.

5.5.1 Purpose.- State the purpose for which the PSDP was prepared. Typically, the purpose of the flight PSDP is to provide the payload organization and the SSP a comprehensive safety assessment of the payload systems and subsystems that pose hazards while associated with the shuttle. The final updated PSDP represents the substantiating data for the payload organization's certification that the payload is safe and complies with the requirements specified in NSTS 1700.7.

5.5.2 Scope.- Describe the major systems and elements of the payload for which the payload has safety certification responsibility. If the payload utilizes hardware provided by the SSP, such as orbiter GFE, for which the payload does not have safety certification responsibility, the payload need only list that GFE and describe how it is being used. The payload organization should clarify which interfaces among the payload, orbiter, GFE, Spacelab/Spacehab, etc., have been assessed in the hazard analyses and are

addressed in the PSDP. If the payload contains series payload hardware or reflown hardware, this fact and a list of the hardware items should also be identified here.

5.5.3 Safety Analysis.- Describe the process used to verify the accuracy, completeness, and validity of the data contained in the PSDP. If any specific analytical safety analysis technique or tool was used to identify hazards, list that technique here (also see NSTS 13830, paragraph 5.1.6., Safety Analyses.)

5.5.4 Safety Status Summary.- Provide an executive summary of the safety status of the payload. This section should correlate the design maturity of the payload (i.e., concept, preliminary design, critical design or as-built hardware) with the maturity of the safety analysis.

5.5.4.1 Action Items (AI's): List all AI's, and their current status, assigned during previous safety reviews and other safety meetings. Where AI response data has been incorporated into the PSDP, refer to the applicable page and paragraph.

5.5.4.2 Noncompliance Reports (NCR's): List any identified safety noncompliance items and provide their current status. By phase III, this section should reflect the final disposition of all noncompliance issues and list all approved waivers and deviations from the applicable safety requirements.

5.5.4.3 Operational Controls Identification: Prepare a list of all controls to hazards which require a crew or ground operation. This list should identify the applicable HR and control number. Separately list any HR controls that require training of the crew.

5.6 Applicable Documents

Identify all applicable safety related requirements documents by number, date, and revision that are used in the PSDP to substantiate safety compliance.

5.7 Payload Description

Briefly describe the payload in terms of its significant characteristics and functions. Include figures or illustrations to show all major payload configurations. Identify all hazardous systems and subsystems.

5.8 Ground Operations

Briefly describe the sequencing and provide a condensed milestone schedule of ground processing tasks. Include transport, receipt, assembly, test, and integration/installation in the orbiter, and final verification and checkout.

5.9 Flight Operations

Briefly describe the planned event sequence for payload operations during the mission denoting those events with hazard potential. This mission description shall address all mission phases (i.e., ascent, on-orbit, payload deployment, proximity operations, retrieval, descent, and landing). Also, address abort cases and rapid-safing contingencies as applicable for the payload.

5.10 Detailed System Descriptions

Provide separate sections in the PSDP to describe the major elements of the payload with each section containing subsections organized by technical disciplines. Describe the design, function, planned operation, and the safety features of each system within technical discipline description of the major element. If the payload complexity does not warrant separate sections for each major payload element, such a division of data is not required. The detailed system descriptions provide the PSRP and its experts the basis for review of the payload and the PSDP. The level of detail should be adequate to support the compliance documented within the HR.

Note: A goal is to divide the payload descriptive data into discrete segments that will facilitate review of the data by the PSRP and its technical experts and minimize duplication. Since the PSRP technical experts and most payload organizations are organized by technical disciplines, it should be advantageous to both to organize the data in this manner.

5.11 Summary of Safety Analyses

Provide a hazard analyses summary which reflects the results of the hazards analyses for the subsystems and the overall payload. The summary should reflect the hazards that were considered in developing the HR's. This may include any hazards that were considered and dispositioned as eliminated with rationale provided for the elimination. When a hazard is mitigated the hazard report should be referred to. Specific analyses that establish criticality, mitigation, elimination or some other aspect of the hazard assessment should also be summarized. This section and the safety analysis section (paragraph 5.5.3 above) can be combine to a single section.

5.12 Summary of Verifications

Provide a summary of the test and analytic efforts required to verify the compliance to intended performance and design specifications of all safety critical hardware. In order to assess proper compliance of a payload the review of verification techniques and criteria are essential. Clarification of verification methods have consumed significant time during safety reviews. In an effort to effectively review this information prior to the formal review, the Summary of Verifications Section of the PSDP has been established. The level of detail of this section should reflect the type of verification, implementation technique, any pass/fail criteria and results summary.

5.13 Orbiter (SL, SH, etc.) Interfaces and Services

Identify all orbiter-payload interfaces and orbiter-provided services; all orbiter services required for ensuring a payload's safety must be identified as safety critical services. Orbiter/SL/SH safety critical interfaces subsystems include:

a. Structural/Mechanical- Provide a brief description of the major structural and mechanical interfaces (e.g., payload retention latch assembly interfaces, SL pallet hard points, sidewall-mount provisions, RMS grapple interfaces, SL/SH/orbiter middeck mounting provisions, etc.

b. Environmental Control- Provide a brief description of the environmental control interfaces (e.g., orbiter cold plate-to-payload freon lines, SL/SH water-cooling loop interfaces, SL/SH/orbiter middeck rack-mounted payloads requiring air recirculation, etc.).

c. Electrical Power- Provide a brief description of the electrical power distribution subsystem interfaces (e.g., SL remote acquisition unit and experiment power distribution box interfaces, or AC/DC interfaces from orbiter cabin, auxiliary, prime or T-0 GSE power, etc.).

d. Command and Data Management System (CDMS)- Provide a brief description of the interfaces to the orbiter CDMS (e.g., experiment computer interconnect stations and remote acquisition units, etc.).

e. Safety Critical Interfaces- Identify and provide a brief description of orbiter-to-payload interfaces that augment the payload system failure tolerance.

PART II
GUIDELINE INSTRUCTIONS FOR THE PREPARATION OF PAYLOAD HR'S

1.0 INTRODUCTION

1.1 Purpose

The purpose of this part of the document is to provide guidance to payload organizations in the preparation of SSP payload flight HR's to demonstrate compliance to NSTS 1700.7 (current revision). This section of the document provides HR guidelines with candidate causes, typical content, and organization for some of the typical HR's required. HR's are an essential element of a complete safety data package required to support the safety review process (Ref: NSTS 13830). This guidance, combined with the minimum data typically generated during the normal system safety analyses, should facilitate the preparation of complete HR's.

1.2 Background

NASA requires reporting of SSP payload hazards and their controls in the form of HR's. These HR's identify hazards integral to the payload system, document control of these hazards, and specifically address and show compliance with SSP safety requirements. They form the basis of safety compliance documentation submitted for payload safety reviews.

1.3 Scope

This listing is intended to help individual payload programs identify the hazards applicable to SSP mission phases. It does not eliminate the need to perform detailed safety analyses of the payload systems and interfaces; nor, does it eliminate the need to address technical requirements not covered on the GHR's identified herein. It does not comprehensively identify hazards, but instead identifies the more common hazards and describes information typically required. It illustrates HR structure, levels, causes, and suggests appropriate control and verification data.

This document is intended to be used as a "how-to" guide for documenting common hazards for payloads using the Space Shuttle. This is not a requirements document. It in no way is to be construed as levying design requirements, hazard analysis technique, or HR organization.

2.0 INSTRUCTIONS FOR USE

2.1 General

Many of the safety critical subsystems of any specific payload are similar to the safety critical subsystems of other payloads that have been through the safety review process. This document provides guidelines for the more common hazards typically present in these subsystems. These common hazards should be compared to the specific payload design so that applicability can be determined as part of a hazard analysis. The suggested HR content can then be used as an aid in HR construction.

The suggested HR contents of this guide complement the normal payload system safety analysis and incremental safety review processes. Once results are obtained from the system safety analyses, the suggestions presented in this guide on formatting, organization, and presentation can be used to prepare for the safety reviews.

It should be noted that although HR content has been "fixed", different formats are acceptable. The data presented in section 3 are not format-dependent. <u>That is, the suggested HR contents apply to any format.</u>

2.2 Hazard Lists and the Hazard Catalog

Section 3.0 contains the guideline HR list reflecting common hazards for a payload. While performing the preliminary hazard analysis, each HR can be reviewed for applicability to your payload. (Note: The HR's provided are not considered a complete listing of possible hazards, the hazard analysis should be the primary source for identifying hazards of the payload.) Once the hazards are established for a payload, the compilation of the hazards list for the payload should be made and developed into a unique hazard catalog. Each HR can then be grouped under the subsystem where the energy source (or hazardous material) exists. This subsystem grouping is arbitrary and is to be used only as a guide. The GHR's that follow contain suggestions for development of HR's. The guidelines presented are based on historically successful HR's presented to the Payload Safety Review Panel.

2.3 HR Composition

2.3.1 Hazard Potential/Hazard Categorization.- Hazardous events of concern in the safety review process are either catastrophic or critical. The hazard potential listed on the individual GHR's is the typical worst-case event. Your program's hazard potential classification may be different from the hazard potential listed on the GHR's. Hazard potential classification should be established based on an uncontrolled or unmitigated worst case hazardous event. Guidance is given on the individual GHR's to aid in the selection of hazard potential.

2.3.2 Hazard Groups.- During the analytical process to identify hazards, the payload organization should attempt to define the hazards in terms of the 10 hazard groups listed below. A difficulty common to all such lists is that there is considerable overlap between hazard groups, and assignment of some unsafe act or condition to any one hazard group is arbitrary. What is important is that potentially hazardous items or conditions are identified, described, and tracked through the safety review process.

a. Collision
b. Contamination
c. Corrosion
d. Electrical Shock
e. Explosion
f. Fire
g. Injury or Illness
h. Loss of Orbiter Entry Capability
i. Radiation
j. Temperature Extremes

Review your payload hazards versus this list to determine the applicable hazard groups.

2.3.3 Hazards.- A hazard is defined as a potential risk situation caused by an unsafe act or condition. Hazards can be found in hardware/software systems, the man-machine relationship, or both. For SSP payload safety, the scope of hazards to be reported are those related to the following: personnel injury or death, damage to or loss of the orbiter or SSP equipment, or the use of contingency or emergency operations by the SSP flight crew. The payload organization must perform hazards analyses to identify the potential hazards that exist in a payload design, potential causes for these hazards, the specific hazard controls, and how control of these hazards will be verified. This information is then documented on payload HR's.

Hazards exist (and HR's are needed) whenever an energy source and/or hazardous materials exists. For example, premature firing of a SRM is a hazard applicable to all payloads containing SRM's, regardless of the degree of control. This hazard can be controlled but not eliminated. The only way to eliminate the hazard is to eliminate the SRM in this example.

2.3.4 Hazard Description.- The hazard description should define the risk situation including the unsafe act or condition and its effect on the SSP or personnel. Any limits or restrictions to the applicability of the HR should be reflected in the description.

2.3.5 Safety Requirements.- The detailing of safety requirements on the HR cover page indicates what requirements are to be satisfied within the hazard controls. These requirements should be specified by document, section/paragraph/sub-paragraph. The requirements provided in the following HR guidelines are typical for most subsystems and common HR's. It is the responsibility of the originator of the HR to indicate the requirements that are being applied to their design based upon their hazard analysis. References to the interpretation letters of NSTS 18798 exist in the GHR's but it should not be construed that those are the only applicable letters. NSTS 18798 is updated when additional information must be conveyed to the payload community and the payload organization should review all letters for applicability to their payloads or experiments. Interpretation letters, policy letters, test and verification requirements should be reflected within the controls that are addressing them.

2.3.6 Hazard Causes.- Itemize the identified causes for the risk situation and the unsafe act or condition listed under the hazard description. Hazard causes may be environmental, personnel error, design characteristics, procedural deficiencies, or subsystem malfunctions. The causes listed in the GHR's are typical for the applicable hazard. Causes should be established at a level of detail necessary to explain the event path to the hazard. If a cause from a guideline does not apply, then it should not be carried to the formal HR. Any additional causes applicable to the payload design should be added.

2.3.7 Hazard Controls.- Identify the design features, safety devices, warning devices, and/or special procedures that will eliminate, reduce, safe, or counter the hazards resulting from each hazard cause. If procedures or processes in manufacturing or assembly are critical elements in controlling hazards, the procedures and/or processes must be so identified and addressed individually. All orbiter-provided critical services or interfaces must be identified, described, and analyzed in conjunction with the payload. The order of precedence for reducing hazards is defined in NSTS 1700.7, paragraph 303. This section of the HR shall be initially completed for the phase I submittal and updated as required for each subsequent phase safety review. A direct correlation (indexing) between each hazard cause and the corresponding hazard control(s) must be clearly shown on the HR.

2.3.8 Verification Methods.- Identify the methods used to assure the effectiveness of the hazard controls and the methods used to assure that the payload meets the safety requirements for flight. For phase I, this section should include the types of tests, analyses, inspections or procedures (e.g., vibration testing, fracture analysis) to be used to verify each hazard control, including all orbiter-provided services or interfaces. A direct correlation (indexing) between each verification method and the corresponding hazard control must be clearly shown on the report. Where procedures or processes in manufacturing or assembly are critical elements in controlling hazards, and where the results cannot or will not be verified by subsequent inspection or test, it is mandatory to insure that the procedure or process is adequate for the purpose and that the steps of the procedure or process are verified as they occur. An independent verifier, as delineated by the payload organization, shall attest to proper completion of the procedure or process. For phase II, this section should be updated to refer to specific test (or analysis) procedures and a summary of criteria to be used. For phase III, all safety verifications should be completed, and this section should be updated to reflect any changes in the verification methods made after the phase II review.

2.3.9 Status of Verification.- This section on the formal HR indicates the status of each safety verification. Each status item will be identified by the same number/identifier as the verification method item to which it is related. For phase I, provide a tentative schedule for completion of each verification task (if available). For phase II, specify the schedule for the completion of each specific verification test, analysis, or inspection. For phase III, all safety verifications should be completed; if any verifications are open at phase III, they should be transferred to a safety verification tracking log. (See NSTS 13830) This section should summarize the results of the completed tests, analyses, and/or inspections and refer to particular test reports by document number, title and date. The safety verification tracking log should be attached to the phase III flight safety data package.

2.3.10 Supporting Data.- Sufficient supporting data must be attached to the HR to complete the presentation of hazard control(s) and to demonstrate complete compliance with requirements. The minimum supporting data is defined in NSTS 13830; however, the PSRP may require more than the minimum supporting data depending on the payload complexity, hazard potential, interfaces with the

orbiter, PSRP experience with the payload developer, PSRP experience with similar payloads, etc. The Attached Supporting Data section describes the data that has been typically requested before an HR was approved and signed.

2.3.11 References.- Hazard control and verification references should consist of formal documents such as released drawings, test or analysis reports. If formal documents are not available, then other auditable references, such as numbered engineering notebooks or quality assurance-stamped completed test procedures should be referred to.

2.4 General Comments Applicable to All HR's

The following notes apply to all HR's:

2.4.1 Number and Title.- HR's should be identified by number and title. The number should be a simple index for all HR's. The number should be unique for each HR for each payload; this is to avoid referencing problems. The HR number should never be reassigned. This number serves as index and tracking throughout the safety process and flight. If an HR is eliminated, the number should remain associated with the deleted HR for tracking purposes. One method of HR numbering is using the payload acronym followed by a sequential number. The titles should be descriptive of the hazard reflected within the HR, (e.g., Toxic Material Release, Premature SRM Ignition, EVA Crew Contact Hazards, etc.). Examples are given for each guideline; the customer should choose a title that is appropriate for the HR they develop.

2.4.2 System Description.- Any system details needed for a complete understanding of the system should be in the system description section of the payload safety data package. Drawings and schematics should have relevant components labeled with levels of control and inhibits numbered.

2.4.3 Electrical Inhibits.- When discussing the fault tolerance of inhibits in an electrical system, the entire electrical system from power source through the end function to power return must be considered and documented. Power sources for individual controls should be described and documented. When shown in diagrams, the inhibits and levels of control should be clearly labeled. Circuits passing through any connectors should indicate this on the diagrams.

2.4.4 Level of Detail.- The words "discuss" or "summarize" in the GHR text sections are meant to indicate the need for one or two sentences only. In effect, these words mean "provide the bottom line." Additional detail is needed if "discuss" or "summarize" are used in the HR back-up data suggestions (Attached Supporting Data).

2.4.5 Separation of Hazards.- Subdivide the suggested hazard title (and report) if more appropriate for your payload. For example, one suggested common hazard is "Inadvertent release of hazardous materials." Payloads that contain several hazardous materials that are controlled differently may find that grouping these onto a single HR is cumbersome Therefore, an equivalent approach could be to have two HR's as shown below:

(1) "Inadvertent release of mercury"; and,
(2) "Inadvertent release of methane".

2.4.6 Combining Subsystems.- Subsystem definitions should not cause subdivision of HR's. For example, the following two hazard titles address the same hazard but were incorrectly put on separate HR's because causes and controls were in separate subsystems.

Subsystem	Hazard
Electrical/Electronics	"Inadvertent SRM Firing Caused by Electrical Component Failures"
Pyrotechnics	"Inadvertent SRM Firing Caused by Pyrotechnic Firing"

The required approach is to have one hazard title (and one report) for each hazard regardless of the number of subsystems or procedures involved. In this case, the appropriate HR title is "Premature/Inadvertent SRM Firing".

2.4.7 Deleting HR's.- Any HR that becomes non-applicable due to subsystem alteration or further analysis that indicates a non-hazardous condition should be maintained in the hazard catalog with an indication of its status and the date of that disposition. A HR number should never be re-used for a different hazard.

2.5 HR Interdependence

Each HR should be completely usable as a "stand alone" document. However, cross referencing of common causes and their respective controls between HR's is acceptable (and strongly encouraged) when the alternative is duplication without providing additional insight to requirements compliance. It is strongly encouraged that "shared" supporting data be contained within appendices rather than attaching multiple copies throughout a safety data package.

2.6 Interface HR's

Interfaces between payload elements and/or experiments that are being reviewed separately may not be covered in the individual payload element reports. A supplementary analysis, or interface hazard analysis, is typically performed and interface HR's may be needed.

To determine if interface HR's are needed, the following five general steps should be taken:

(1) The integrator identifies all the interfaces that exist between the elements;

(2) Those interfaces with hazard potential are identified;

(3) Proper control of those interfaces with hazard potential is determined and documented. (A matrix for items (1), (2) and (3) is recommended);

(4) Undocumented interface hazards are documented on a new HR;

(5) Items (1) through (4) are documented for review.

3.0 GUIDELINE HAZARD REPORTS

The more common and standardized HR's have been reflected in the following guidelines. [Note: The HR numbers given within this document are meant for reference only. HR's for a payload should have a unique, sequential designator (e.g. PAYL-01, PAYL-02, etc.)]

No.	Hazard	Page
GHR-1	Toxic Material Offgassing (Crew Cabin Materials)	11
GHR-2	Broken Glass	13
GHR-3	Excessive Ionizing Radiation	15
GHR-4	EVA Contact Hazards	17
GHR-5	IVA Touch Temperature	20
GHR-6	IVA Crew Contact Hazards	21
GHR-7	Electrical Shock	22
GHR-8	Crew Exposure to LASER Emissions	24
GHR-9	Electrical Shock from Physiological Test Equipment	26
GHR-10	Battery Leakage/Rupture	28
GHR-11	Use of Flammable Materials	31
GHR-12	Hazardous Fluids Leakage in the Payload Bay	33
GHR-13	Ignition of Flammable Atmospheres	35
GHR-14	Electrical Power Distribution Circuitry Damage	37
GHR-15	Radio Frequency Radiation Interfering With STS Circuitry and/or Other Payloads	39
GHR-16	Exposure of the Orbiter/Payload to Excessive Levels of EMI Radiation	41
GHR-17	Rupture and/or Explosion of Pressure System	42
GHR-18	Leakage/Rupture of Sealed Containers	47
GHR-19	Structural Failure	49
GHR-20	Failure of Rotating Equipment	53
GHR-21	Safety Critical Mechanical System Functional Failure or Partial/Incomplete Deployment/Jettison	55
GHR-22	Collision/Impact During Planned Deployment	58
GHR-23	Premature/Inadvertent Pyrotechnic Device Operation	60
GHR-24	Must Work Pyrotechnics/Debris Generation	62
GHR-25	Collision Following Premature/Inadvertent Appendage Deployment or Payload Release/Deployment	65
GHR-26	Premature/Inadvertent Liquid Engine or Attitude Control System Operation	67
GHR-27	Premature/Inadvertent Solid Rocket Motor Firing	70

HR GUIDELINE

HR NUMBER: **GHR-1**

TITLE: **Toxic Material Offgassing (Crew Cabin Materials)**

SUBSYSTEM: Materials

HAZARD GROUP: Contamination, Injury, Illness

DESCRIPTION OF HAZARD

Materials of construction release hazardous vapors which retained in a confined area will result in crew injury or illness.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 209.3

HAZARD CATEGORY

CATASTROPHIC
X CRITICAL

Toxic constituents of offgassing materials used in habitable areas from the payload or experiment causes temporary crew injury or illness.

HAZARD CAUSES

1. Use of materials that offgas excessive quantities of toxic trace gas contaminants.

ADDRESSING THE HAZARD

1.0 CAUSE: Use of materials that offgas excessive quantities of toxic trace gas contaminants.
1.1 CONTROL: Describe black-box level testing of assembled articles for toxic offgassing in accordance with NHB 8060.1. (NASA will conduct the testing and interpret the data for the customer as a standard service.) Refer to attached supporting data A, B, and D.
1.1.1 VERIFICATION: For payload components tested as assembled articles, NASA will conduct the testing and interpret the data for the customer.
1.2 CONTROL: Summarize materials control, or a combination of rigorous materials control and black-box testing. (This is a negotiable alternative to black-box level testing.) Refer to attached supporting data C and D.
1.2.1 VERIFICATION: For components evaluated on a materials basis, the payload must provide sufficient information to demonstrate that the methodology is acceptable.

NOTE: Materials are evaluated for offgassing in the worst-case use environment. The offgassing test is normally conducted for 72 hours at ambient pressure and a temperature of 120°F with the hardware unpowered. This time and temperature normally provide an adequate margin above maximum cabin temperatures for thermal effects of powering the hardware; however, testing should be conducted at nominal operating temperature, if it is expected to significantly exceed 120°F (by more than 50°F). Non-electrical hardware may be tested at lower temperatures if it would be damaged by exposure to 120°F. The offgassing rate is not affected by cabin pressure, except that the operating temperature may be higher under a reduced pressure and may required additional assessments and testing (if it exceeds 170°F.)

ATTACHED SUPPORTING DATA

A. Offgassing test report(s) or summaries for assembled article(s).
B. Description of methodology used to evaluate components on materials basis, including rationale for use of untested materials.
C. Memorandum of material acceptance from NASA center with interagency agreement with JSC for materials approval (if applicable.)
D. Memorandum of JSC acceptance of offgassing test reports or methodology used to evaluate components (if applicable).

NOTE: If a materials and processes intercenter agreement is applicable, the only required control and verification in the HR is referring to the responsible NASA center materials certification; no additional supporting data are normally required unless material usage agreements are used.

HR GUIDELINE

HR NUMBER: **GHR-2**

TITLE: **Broken Glass**

SUBSYSTEM: Structural, Materials

HAZARD GROUP: Injury, Illness

DESCRIPTION OF HAZARD

This HR addresses the release of shatterable material such as glass particles in the habitable environment.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 206, 209, 215

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Fragmentation of shatterable material may cause injury to the crew from physical contact or ingestion. Fragments may cause damage to the orbiter and/or Spacelab by lodging in critical equipment.

HAZARD CAUSE

1. Release of fragments from shatterable material in the crew cabin.

NOTE: Shatterable material includes items such as mirrors, lenses, filters, apparatus viewports, experiment apparatus/components and standard commercially available light bulbs.

ADDRESSING THE HAZARD

1.0 CAUSE: Release of fragments from shatterable material in the crew cabin.
1.1 CONTROL: Specify that the release of fragments from items exposed to the crew cabin is controlled by a single positive level of containment which prevents particle release into the crew cabin in the event of fracture.
1.1.1 VERIFICATION: Review of the design.
1.1.2 VERIFICATION: Document an inspection of the flight hardware.
1.2 CONTROL: Specify that the release of fragments from standard camera and optical equipment is controlled by recessing shatterable components for impact protection. Crew procedures should be established to verify no broken glass prior to first use.
1.2.1 VERIFICATION: Review of the design.
1.2.2 VERIFICATION: Document an inspection of the flight hardware.
1.2.3 VERIFICATION: Review of the PIP and/or PIP annex to assure that crew procedures are in place to assure inspection for fragments prior to first use on orbit.
1.3 CONTROL: Specify that the release of fragments from items requiring airflow for cooling is controlled by isolating the cooling air from the crew cabin environment or by filtering the exhaust air with a 50 micron or smaller screen/filter.
1.3.1 VERIFICATION: Review of the design.
1.3.2 VERIFICATION: Document an inspection of the flight hardware.

1.4 CONTROL: Specify that the release of fragments from non-pressurized and not mechanically loaded items not accessible from the crew cabin but not positively contained is controlled by the design of the component to withstand the expected environment.
1.4.1 VERIFICATION: Summarize the results of vibration test(s).
1.4.2 VERIFICATION: Document an inspection of the flight hardware.
1.5 CONTROL: Specify that the release of fragments from pressurized glass components is controlled by positive containment. (A 50 micron or smaller screen/filter is considered a positive method of containment.)
1.5.1 VERIFICATION: Review of the design.
1.5.2 VERIFICATION: Document an inspection of the flight hardware.

NOTE: For ceramic and glass applications that are pressure loaded documentation of compliance to NSTS 14046 should be made in a separate HR.

ATTACHED SUPPORTING DATA

A. List of all shatterable material (include quantity).

HR GUIDELINE

HR NUMBER: **GHR-3**

TITLE: **Excessive Ionizing Radiation**

SUBSYSTEM: Radiation

HAZARD GROUP: Radiation, Illness/Injury

DESCRIPTION OF HAZARD

Injury, illness of crew due to exposure to ionizing radiation sources (materials and generators).

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 212.1

HAZARD CATEGORY

CATASTROPHIC
X CRITICAL

Only applications where the hazard potential are critical can use this generic guideline. Applications with catastrophic hazard potential are a special issue that must be addressed in a case-by-case manner with the Shuttle Program.

HAZARD CAUSES

1. Exposure to excessive levels of radiation.
2. Exposure to excessive levels of ionizing energy.

Causes of this hazard are fundamentally the sources for the ionizing radiation. Loss of containment/barriers are also valid causes and should be developed if the design requires.

ADDRESSING THE HAZARD

1.0 CAUSE: Exposure to excessive levels of radiation.
1.1 CONTROL: Identify all radioactive materials that will be flown. Refer to a JSC Form 44 (to be attached) for each item that contains radioactive materials. Refer to the approval from JSC for the JSC Form 44. Refer to attached supporting data A and B.
1.1.1 VERIFICATION: Review of design to ensure all sources of radioactive materials are properly documented.
1.1.2 VERIFICATION: Completion of JSC Form 44 and approval from JSC.
1.2 CONTROL: Experiment procedures and/or design ensure ionizing radiation levels and exposure of crew and equipment are minimized, in accordance with Federal licensing standards.
1.2.1 VERIFICATION: Review of PIP, PIP annex and/or procedures. Review of design and/or procedures to verify minimum exposure levels have been achieved and to document RCP approval.
1.3 CONTROL: Provide design provisions that prohibit release or displacement of radioactive material and subsequent contamination problems.
1.3.1 VERIFICATION: Review of design, containment analysis, operational hazard analysis.

NOTE: It may prove convenient to refer to other HR's if they relate to radioactive material release.

2.0 CAUSE: Exposure to excessive levels of ionizing energy.

2.1 CONTROL: Document all equipment that emits ionizing levels of electromagnetic radiation. Refer to a JSC Form 44 (to be attached) for each device that emits radioactivity. Refer to the approval from JSC for the JSC Form 44. Document nature and level of ionizing energy. Refer to attached supporting data A and B.

2.1.1 VERIFICATION: Review of design to ensure all sources of ionizing energy are properly documented.

2.2 CONTROL: Specify and summarize fault tolerance to inadvertent operation. Identify all inhibits, controls and monitors available. Refer to attached supporting data C.

2.2.1 VERIFICATION: Summarize and refer to analysis to support fault tolerance of design.

2.3 CONTROL: Summarize containment of ionizing radiation. Refer to attached supporting data D.

2.3.1 VERIFICATION: Refer to the containment analysis and as-built hardware for proper configuration. Refer to testing to ensure adequate operation. Refer to any necessary procedures.

ATTACHED SUPPORTING DATA

A. JSC Form(s) 44 describing all uses of radioactive materials or radiation generators.
B. Radioactive Payloads Working Group approval memorandum for JSC Form(s) 44.
C. Schematics of controls and inhibits for operation of ionizing energy generators.
D. Diagrams indicating containment provisions.

HR GUIDELINE

HR NUMBER: **GHR-4**

TITLE: **EVA Contact Hazards**

SUBSYSTEM: Structural, Mechanical

HAZARD GROUP: Injury, Illness

DESCRIPTION OF HAZARD

This HR is to address all hazards that could injure a crew member by puncturing or damaging the EMU while performing EVA in the payload bay or around a spacecraft during on-orbit operations. It applies to any EVA documented in the PIP, including scheduled EVA's, unscheduled EVA's for mission success, and contingency EVA's for hazard control.

NOTE: Any PIP agreed to EVA task used to satisfy the failure tolerance criteria of NSTS 1700.7 can be used only as a third level of protection to safe a payload.

NOTE: The payload organization should address all PIP agreed to EVA's in the phase I data package and HR's.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.1b, 200.3, 217

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Any damage to the EMU is considered catastrophic as it is the only life-support available to the EVA crew member. Any injury to an crew member during an EVA will result in the loss of the EVA crew member's capability to perform a potentially safety critical EVA.

HAZARD CAUSES

1. Sharp edges.
2. Pinch points.
3. Hot/cold spots.
4. Exposure to excessive radiation, magnetic fields, etc.
5. Release of stored energy.
6. Structural failure of payload provided hand holds, restraints, and/or payload hardware interface provisions for restraint systems. (Includes payload provided interface provisions for SSP-provided EVA restraint systems.)
7. Crew member induced loads on payload provided tools and/or interfacing payload hardware exceeds the limit load for which the item was designed. Includes payload interfaces with all tools to be used during the EVA, including SSP provided tools.

The above hazard causes are the typical causes for EVA hazards, but the listing is not all inclusive for every EVA. Some examples of hazard causes that might be applicable to certain payloads are rapid safing of payload hardware, controllability of large masses, excessive rotation, EVA tools, cryogenic systems, and mating/demating of powered connectors.

ADDRESSING THE HAZARD

1.0 CAUSE: Sharp edges.
1.1 CONTROL: Specify payload design criteria for minimizing sharp edges on exposed structure. Include Airborne Support Equipment following deployment that may expose sharp edges. Refer to the applicable documents. (NSTS 07700, Vol. XIV, Appendix 7 or NASA-STD-3000, Vol. IV, Section 14). Refer to attached supporting data A and B.
1.1.1 VERIFICATION: Specify method used to verify sharp edges do not exist or are in-accessible during EVA, or are controlled by covers, blankets, etc. Refer to applicable analysis, test or inspection document.

2.0 CAUSE: Pinch points.
2.1 CONTROL: Identify rotating joints, gimbals or moveable structure that are within the EVA translation paths. Highlight potential pinch locations. Describe protective covers and/or procedural controls or zones of exclusions. Refer to the applicable released drawings and flight procedure requirements. Refer to attached supporting data A and C.
2.1.1 VERIFICATION: Specify method used to verify pinch points are not accessible during EVA or are controlled by covers, blankets, etc. Refer to the applicable analysis, test or inspection document.
2.1.2 VERIFICATION: Review of PIP and/or PIP annex to assure that flight rules are in place for any procedural restrictions or keep-out zones.

3.0 CAUSE: Hot/cold spots.
3.1 CONTROL: Specify how locations containing hot/cold spots or touch temperatures exceeding NSTS 07700, Vol. XIV, Appendix 7 limits are protected from crew accessibility. Describe protective covers and/or procedural controls and zones of exclusion. Refer to the applicable released drawings and/or flight procedure requirements. Refer to attached supporting data A and D.
3.1.1 VERIFICATION: Specify method used to verify hot/cold spots are not accessible during EVA or are controlled by covers, blankets, etc. Refer to the applicable analysis, test or inspection document.
3.1.2 VERIFICATION: Review of PIP and/or PIP annex to assure that flight rules are in place for any procedural restrictions or keep-out zones.
3.2 CONTROL: Identify worst-case thermal environments that are attitude dependent. Submit appropriate inputs to the PIP annex for baseline of appropriate flight rules containing the required attitude restrictions.
3.2.1 VERIFICATION: Review of PIP and/or PIP annex to assure that attitude restrictions are in place.
3.3 CONTROL: Identify methods used to assure that payload heaters cannot cause a hazardous hot spot during an EVA.
3.3.1 VERIFICATION: Refer to the analysis(es) that demonstrate that continuously on heater(s) are not hazardous. (The heaters are not accessible by the crew and/or do not exceed the maximum allowable temperature.)
3.3.2 VERIFICATION: Provide drawings and/or schematics to show heater circuit protection.
3.3.3 VERIFICATION: Review of PIP and/or PIP annex to assure that flight rules are in place for system configuration, EVA procedural restrictions, and/or keep-out zones.

4.0 CAUSE: Exposure to excessive radiation, magnetic fields, etc.
4.1 CONTROL (Preferred): Identify controls and inhibits that control RF radiation during EVA when applicable to meet safety requirements or refer to the applicable portions of the RF radiation HR. Refer to attached supporting data A and E.
4.1.1 VERIFICATION: Refer to applicable drawings.
4.2 CONTROL (Alternative): Refer to designated keep-out zones documented in the PIP annex.
4.2.1 VERIFICATION: Review of PIP annex for designated keep-out zones.

5.0 CAUSE: Release of stored energy.
5.1 CONTROL: For any operation of mechanisms or structures that may store energy, indicate the design provisions that allow for controlled release of the energy during EVA operations.
5.1.1 VERIFICATION: Review of design. Testing. Referencing plans and reports from each as applicable.
5.2 CONTROL: Specify areas that the EVA crew members must avoid because a payload element is not two fault tolerant to inadvertent release of stored energy.
5.2.1 VERIFICATION: Review of PIP and/or PIP annex to assure that flight rules are in place for keep-out zones.

6.0 CAUSE: Structural failure of payload provided hand holds, restraints, and/or payload hardware interface provisions for restraint systems. (Includes payload provided interface provisions for SSP-provided EVA restraint systems.)
6.1 CONTROL: Specify how payload provided restraint provisions are designed with a minimum factor of safety of 1.4 on the design limit load requirements. Identify actual factors of safety used for design. (Includes payload provided interface provisions for SSP-provided EVA restraint systems.) Refer to attached supporting data F.
6.1.1 VERIFICATION: Specify method used to verify ultimate load capability of hardware and specify margins of safety provided. Refer to the applicable analysis, test, or inspection document.

7.0 CAUSE: Crew member induced loads on payload provided tools and/or interfacing payload hardware exceeds the limit load for which the item was designed. Includes payload interfaces with all tools to be used during the EVA, including SSP-provided tools.
7.1 CONTROL: Define the design limit load for each payload provided tool and all interfacing payload hardware and the basis for derivation of the limit load. Identify the actual factors of safety used for the design.
7.1.1 VERIFICATION: Specify method used to verify ultimate load capability of hardware and specify margins of safety provided. Refer to the applicable analysis, test, or inspection document.
7.1.2 VERIFICATION: Specify methods used to calibrate loads from EVA tools such as torque wrenches, powered wrenches, etc.
7.2 CONTROL: Define how sharp edges and debris are controlled during cutting or similar assembly or disassembly tasks.
7.2.1 VERIFICATION: Review of design. Review of PIP and/or PIP annex.

ATTACHED SUPPORTING DATA

A. Drawings and/or pictures of planned and/or controlled EVA envelope.
B. Drawings and/or schematics to show sharp edges (pre- and post-deploy, etc.)
C. Drawings indicating rotating joints or pinch points.
D. Drawings showing hot or cold spots with indications of the worst-case temperatures.
E. Drawings showing the RF fields and worst-case field strengths.
F. Drawings of payload provided hand holds, tethers, and tether/restraint system attach locations with a design limit load requirement for each identified.

HR GUIDELINE

HR NUMBER: **GHR-5**

TITLE: **IVA Touch Temperature**

SUBSYSTEM: Human Factors

HAZARD GROUP: Injury, Illness

DESCRIPTION OR HAZARD

Injury of crew due to exposure to temperatures greater than 45°C or less than 4°C.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.1A
NSTS 21000-IDD-MDK, paragraph 6.2.2

HAZARD CATEGORY

	CATASTROPHIC
X	CRITICAL

HAZARD CAUSES

1. Crew contact with surface greater than 45°C or less than 4°C.

ADDRESSING THE HAZARD

1.0 CAUSE: Crew contact with surface greater than 45°C or less than 4°C.
1.1 CONTROL: Describe how the design is single failure tolerant and/or procedures that ensures the crew does not come into contact with a surface greater than 45°C or less than 4°C.
1.1.1 VERIFICATION: Review of design or test to ensure surfaces do not exceed 45°C or less than 4°C.
1.1.2 VERIFICATION: Review of PIP, PIP annex and/or procedures to ensure no crew contact with surfaces in excess of 45°C or less than 4°C.

ATTACHED SUPPORTING DATA

None generally required.

HR GUIDELINE

HR NUMBER: **GHR-6**

TITLE: **IVA Crew Contact Hazards**

SUBSYSTEM: Structural, Mechanical

HAZARD GROUP: Injury, Illness

DESCRIPTION OF HAZARD

Crew contact with sharp edges, corners, protrusions and pinch points results in crew injury.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 102.1, 200.1a, 200.1b

HAZARD CATEGORY

CATASTROPHIC
X CRITICAL

This HR deals with injury to the IVA crew due to contact with sharp items. The hazard potential must be established by the type of specific injury and how it will affect the crew member.

HAZARD CAUSES

1. Improper hardware design

The causes of this HR are those items that can have a sharp edge, corner or protrusions, pinch and crushing points and entrapment points, and for which a crew member may contact during nominal operations and maintenance procedures.

ADDRESSING THE HAZARD

1.0 CAUSE: Improper hardware design
1.1 CONTROL: Specify the criteria used to round corners and edges, eliminate dangerous protrusions and preclude crew contact with pinch points. NSTS 07700, Vol XIV, Appendix 9, NASA STD 3000 or the SPAH should be used as guides in the design of hardware. If a standard other than the previously listed standards is used a comparison of the standard to NSTS 07700, Vol XIV, Appendix 9, NASA STD 3000 or the SPAH will facilitate acceptance. Crew contact hazards should be considered in any portion of the payload that the crew may enter or work around. Refer to attached supporting data A.
1.1.1 VERIFICATION: Review of design, drawings to insure proper design.
1.1.2 VERIFICATION: Inspection of as-built hardware.

ATTACHED SUPPORTING DATA

A. When a standard is used other than the SPAH, NSTS 07700 Vol XIV, Appendix 9, or NASA STD 3000 summarize the criteria used to preclude IVA contact hazards. Include drawings and a narrative that describes the safety critical design criteria, review process and inspection. (As requested by the PSRP.)

HR GUIDELINE

HR NUMBER: **GHR-7**

TITLE: **Electrical Shock**

SUBSYSTEM: Electrical

HAZARD GROUP: Injury, Illness

DESCRIPTION OF HAZARD

Incidental contact by the crew with high voltages (AC/DC) can lead to severe burns and possibly other physiological effects. The "Description of Hazard" should reflect the voltages within the equipment that lead to the hazard potential.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 102.1, 200.1b

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Hazard categorization should be based on the worst-case effect on the crew (e.g., tissue destruction, electrocution, etc.). These effects are related to current and voltage characteristics. Some contributing factors to electrical shock are voltage, skin resistance and current limiting. In most cases incidental contact with voltages less than 32 volts (AC/DC) have been considered non-hazardous.

HAZARD CAUSES

1. Defective component, wires, insulation, design and/or workmanship.
2. Exposed Terminals, connectors, energized conductive surfaces.

With most payloads and experiments, the source of this hazard is the power that operates the payload. The hazard causes are derived from the locations where the crew may contact electrical voltage during crew activity.

ADDRESSING THE HAZARD

1.0 CAUSE: Defective component, wires, insulation, design and/or workmanship.
1.1 CONTROL: Specify design features, inspections and tests that will assure that damaged components, et. al., are screened out.
1.1.1 VERIFICATION: Reflect the inspections and tests that verify workmanship and assure no (unwanted) conductive surfaces exist.
1.2 CONTROL: Provide an overview summary and refer to any controlling documents for the technique used for grounding and bonding the payload. Clearly define criteria for determining grounding/fault bonding implementation. Refer to attached supporting data C.
1.2.1 VERIFICATION: Verification of controls consist primarily of testing to assure proper grounding has been implemented. Verification should establish the test parameters (resistance criteria) and summarize and refer to the test plan.

2.0 CAUSE: Exposed Terminals, connectors, energized conductive surfaces.
2.1 CONTROL: Identify any terminals, connectors, sockets, etc. that the crew may contact. Summarize the design features that preclude crew contact with electrical power. If a physical

barrier is planned to be removed, indicate any procedures to be implemented to ensure that the crew will not come in contact with powered components, wires or connectors.

2.1.1 VERIFICATION: The presence of the proper connector design or other required design provisions must be verified.

2.1.2 VERIFICATION: Review of procedures, PIP and/or PIP annex.

2.2 CONTROL: Identify all high-voltage sources (transformers, capacitors, etc.). Specify for each the design features that eliminate the voltage (bleed resistors, etc.) or preclude crew contact (enclosure, HV potting, etc.) Refer to attached supporting data A and B.

2.2.1 VERIFICATION: The presence of the design and its certification to perform as required must be verified.

ATTACHED SUPPORTING DATA

A. Summarize in drawing and text any design features that preclude crew contact with high voltages. (Excluding containment behind panels, inaccessible areas, etc.)
B. Provide schematics of all high-voltage sources (transformers, capacitors, etc.) and show the control features that preclude high-voltage exposure. (bleed resistors, etc.) (if applicable.)
C. Document grounding and bonding techniques used. Outline testing procedure and criteria.

HR GUIDELINE

HR NUMBER: **GHR-8**

TITLE: **Crew Exposure to LASER Emissions**

SUBSYSTEM: Electrical, Radiation

HAZARD GROUP: Injury, Illness

DESCRIPTION OF HAZARD

Crew exposure to high-intensity light from LASERs* lead to crew injury and/or blindness. Within the description of the hazard the general description of the LASER source should be made, including such data as the LASER class, output power, light wavelength, pulse (with frequency) or continuous wave, etc., and a description of where and when it operates.

*A similar HR is necessary should a payload's design have a high intensity light source other than a LASER, such as lamps, strobes, etc., that can cause injury to the crew.

NOTE: This Guideline is written to consider LASERs that are to be contained within the crew habitable environment. For LASERs that radiate outside of the orbiter and exceed the ANSI-Z136.1 defined safe levels, the design provisions that will preclude a hazard to the orbiter crew, the orbiter, or the general population must be documented within a unique HR..

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 201.3, 212.3

HAZARD CATEGORY

X CATASTROPHIC
X CRITICAL

Sustained damage to the eye is the common effect of exposure to LASER radiations leading to crew incapacitation/blindness. Depending on LASER emission intensity, dazzling (temporary blindness) and skin tissue destruction can occur. ANSI-Z136.1 can be used as a reference for determining the effect of exposure and thus establishing the hazard potential.

HAZARD CAUSES

1. Electrical fault.
2. Mechanical fault.

The causes of this HR are those faults that can lead to inadvertent activation of the LASER source, mechanical/electrical faults that can lead to loss of beam(s) containment or misdirection of the LASER beam(s).

ADDRESSING THE HAZARD

1.0 CAUSE: Electrical fault.
1.1 CONTROL: Specify the number and list the electrical inhibits that prevent occurrence of the hazard. Describe each control for each inhibit and establish its independence. Indicate how each inhibit is monitored. Describe ground/return leg inhibit and any RF commanding and encryption implemented. Define the fault tolerance of the system electrical inhibits including

orbiter interfaces. Specify any interlocks to prevent operation unless a specific physical configuration is achieved. Refer to attached supporting data B.

1.1.1 VERIFICATION: Refer to the analysis which verifies the fault tolerance. Show how the analysis substantiates inhibit independence. Refer to any tests to verify inhibit and interlock functionality.

2.0 CAUSE: Mechanical fault

2.1 CONTROL: Describe the containment (mechanical, attenuation or dispersion) features of the system design to preclude crew exposure to LASER emissions in excess of the allowable MPE. Refer to attached supporting data C.

2.1.1 VERIFICATION: Review of design. Testing of design to verify containment of LASER emissions.

2.2 CONTROL: Describe any mechanisms that require precision orientation to assure a safe optical path. Describe the design features that assure operation only when the optical path is "safe". Refer to attached supporting data D.

2.2.1 VERIFICATION: Refer to closeout/alignment plan, testing and qualification. Review of design and testing of interlock mechanisms.

2.3 CONTROL: Describe any requirements for the crew to access the areas where the LASER operates. Establish any equipment or crew procedures necessary to safely accomplish the task. Refer to attached supporting data E.

2.3.1 VERIFICATION: Review of PIP, PIP annex and/or procedures.

NOTE: Controls should reflect how requirements to ANSI-Z136.1, American National Standard for Safe Use of LASERs are complied with.

ATTACHED SUPPORTING DATA

A. Specify all sources for LASER emission. Include a table listing all sources, their energy, wavelength, pulse characteristics, dispersion characteristics, hazard classification, etc.
B. Schematics showing all inhibits, controls and monitors. For any interlocks include a diagram indicating the interlock mechanism.
C. Drawing indicating the optical path(s). Indicate the containment feature around the optical path(s).
D. Summarize any precision alignment mechanisms and procedures. Describe the interlocks that preclude operation when a misalignment occurs.
E. Summarize the crew procedures used to control the hazard.

HR GUIDELINE

HR NUMBER: **GHR-9**

TITLE: **Electrical Shock from Physiological Test Equipment**

SUBSYSTEM: Electrical

HAZARD GROUP: Injury, Illness

DESCRIPTION OF HAZARD

Malfunction of physiological test equipment attached to crew members can lead to injury or death of a crew member. This hazard can manifest itself as either direct electrical shock from instrumentation or current paths through the body to an inadvertent ground path.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 213

HAZARD CATEGORIY

X CATASTROPHIC
X CRITICAL

For definitions of critical and catastrophic levels of shock from physiological test equipment refer to JSC 20483, Appendix R.

HAZARD CAUSES

1. Fault with physiologic monitoring/test equipment.

Physiological test equipment (e.g., electrocardiographs, electroencephalograph, catheters, etc.) must be capable of withstanding two failures and not exceed the HRPPC limits for current exposure (refer to JSC-20483, Appendix R.)

ADDRESSING THE HAZARD

1.0 CAUSE: Fault with physiological monitoring/test equipment.
1.1 CONTROL: (PRIMARY) Summarize the design of the physiological monitoring/test equipment that provides two-fault tolerance to catastrophic injury to the crew member (and single fault tolerance to a critical level injury). Indicate the method for assuring the proper operation of the equipment prior to operations on a crew member. Refer to attached supporting data A
1.1.1 VERIFICATION: Refer to fault analysis, functional testing and review of design.
1.1.2 VERIFICATION: Refer to ground path verification test.

NOTE: The acceptability of the use of the alternate option of control 1.2 is at the discretion of the PSRP for any modified equipment.

1.2 CONTROL: (Alternate) Medical equipment that is in common usage among the general populace need not prove fault tolerance given that the HRPPC has reviewed the medical equipment and determined it to be acceptable "Off the Shelf Medical Equipment." Summarize the common use of the equipment and its safety heritage and compare to the intended flight use. Describe in detail any modifications affecting the physical and/or electrical configuration of the equipment. Provide supporting rationale as to why these modifications will not

compromise the safety record of the equipment nor create safety critical failure modes not previously existent. Refer to attached supporting data B and C.

1.2.1 VERIFICATION: Refer to the HRPPC acceptance memorandum for medical equipment design and intended use. Refer to fault analysis of modification's impact on original design. Refer to functional testing of the modified test equipment. Refer to report of the medical equipment pedigree in common usage.

1.2.2 VERIFICATION: Refer to the tests that verifies ground path.

1.2.3 VERIFICATION: Refer to requalification procedures, tests and analyses . Refer to recertification activities and reports.

1.3 CONTROL: Describe any safety critical calibrations or experiment preparation and setup requirements.

1.3.1 VERIFICATION: Refer to procedures for critical calibration and qualification tests.

ATTACHED SUPPORTING DATA

A. Schematics indicating design functional controls to preclude hazardous currents from reaching the crew personnel involved with the test or the operation of the equipment. Indicate all controls, sources of current and paths to the crew.
B. (Alternate) Memorandum of acceptance of medical equipment design as common usage, off the shelf equipment from the HRPPC.
C. (Alternate) Descriptions and schematics of modifications that qualifies as common usage, off the shelf, medical equipment.

NOTE: A medical equipment integration HR should be generated reflecting any concurrent attachment/use of multiple physiological test equipment or other devices.

HR GUIDELINE

HR NUMBER: **GHR-10**

TITLE: **Battery Leakage/Rupture**

SUBSYSTEM: Electrical, Electronics

HAZARD GROUP: Contamination, Fire, Explosion, Corrosion, Illness/Injury

DESCRIPTION OF HAZARD

Rupture of battery and escape of electrolyte or build-up of gases could lead to explosion.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.4a, 201.3, 209.1, 213.2

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

The release of explosive gasses and/or electrolytes can lead to fire, explosion, corrosion, contamination and potential injury to the crew. This hazard is typically categorized as catastrophic.

HAZARD CAUSES

1 Shorting (internal/external)
2. Charging of primary cells; overcharging secondary cells.
3. Cell reversal, or overdischarging.
4. Excessive internal cell/case pressure.
5. Overtemperature.
6. Freeze/thaw.
7. Accumulation and ignition of hazardous gas mixture.
8. Leakage of battery container.

The build-up of pressure due to chemical action, thermal expansion (high temperature and freezing), etc., is the actual cause of the hazard. The actions that lead to the build-up of pressure are those that should be addressed. Controls should reflect implementation of NSTS 20793.

ADDRESSING THE HAZARD

1.0 CAUSE: Shorting
1.1 CONTROL: Identify and describe all manufacturing controls that preclude internal shorting. Ensure all potential internal short causes are addressed. Refer to applicable drawings and note manufacturers' histories. Address compliance with NSTS 20793.
1.1.1 VERIFICATION: Specify what techniques will be used to verify that internal short protection is in place. Summarize and refer to qualification program.
1.2 CONTROL: Describe controls which protect against external shorts or their effects. Refer to the applicable drawings.
1.2.1 VERIFICATION: Summarize analyses to confirm adequate short protection is in place. Identify inspections to assure protection is in place.

2.0 CAUSE: Charging of primary cells; overcharging secondary cells.

2.1 CONTROL: Specify the devices (e.g., automatic reset thermal trips, circuit breakers, etc.) and procedures that will limit the charging current, so as not to initiate or sustain an excessive outgassing or thermal runaway of secondary batteries. Identify monitors available. Specify those controls that prevent charging lithium batteries under any condition (e.g., series, blocking diodes) . For over-discharging, specify devices and procedures that are designed to limit effects of the current discharge or limit the discharge rate. Specify failure tolerance of these systems. Refer to attached supporting data B.

2.1.1 VERIFICATION: Specify how devices, procedures, monitors, etc., which protect against overcharging are to be qualified and verified.

NOTE: If evolution of gasses or electrolyte is credible, describe how the design is verified to preclude resultant venting, fire, or explosion. If venting cannot be prevented in the event of a major battery failure, describe how venting will occur in a manner that is not hazardous to the orbiter.

3.0 CAUSE: Cell reversal or overdischarging.

3.1 CONTROL: Specify procedures, monitoring and/or manufacturing/maintenance controls that ensure the capacity of each cell of a multiple cell battery is within established specifications prior to discharging (e.g., prior to battery conditioning). Refer to attached supporting data C.

3.1.1 VERIFICATION: Discuss how the implementation of controls for cell reversal will be verified.

4.0 CAUSE: Excessive internal cell/case pressure

4.1 CONTROL: State the minimum safety factor above MDP and state how the MDP is established. Specify how the individual cells and case are designed to prevent or control exceeding the MDP (e.g., venting mechanisms, burst discs, pressure relief devices, etc.). State maximum battery qualification temperature. State whether the battery design will be treated as a sealed container, pressurized component or as a pressure vessel and refer to or list the criteria used to make the determination. Refer to attached supporting data D and F.

4.1.1 VERIFICATION: Summarize and refer to verification analysis or test (e.g., burst pressure, proof test) that verifies the safety margin between rupture and operating pressure for worst-case conditions. Summarize and refer to thermal analysis that determined operating conditions.

NOTE: In general batteries are a unique category of pressurized hardware. Some kinds, such as the alkaline batteries, can be classified as sealed containers, whereas some others such as the Nickel-Hydrogen batteries can be categorized as pressurized components. All batteries that have a LBB failure mode, and the release of contents is not a catastrophic hazard, will be classified as non-fracture critical. Battery cells that are not LBB or whose open release of contents would be a catastrophic hazard will also be categorized non-fracture critical if the respective failures would be suitably contained by a battery case or, for chemical releases that would be a catastrophic hazard, by levels of containment as specified in NSTS 1700.7 paragraph 209.1b.

5.0 CAUSE: Over temperature

5.1 CONTROL: Establish an operational condition envelope or similar data format whereby operations within the limits of the envelope will prevent thermal runaway reactions. Describe devices/designs used to keep the system operating within the constraints of the envelope. Refer to applicable documents.

5.1.1 VERIFICATION: Refer to analyses or tests which verify operational condition envelope. Review PIP, PIP annex, and/or procedures to verify any orbiter constraints or procedures are in place.

5.2 CONTROL: Establish fault tolerance to heater operation exceeding operational envelope. Refer to attached supporting data E and G.

5.2.1 VERIFICATION: Summarize verification analysis or demonstration test results that verify the required failure tolerance is maintained (i.e., operating envelope limits are not violated). Describe how procedural precautions, if any, are verified. Refer to applicable documents.

6.0 CAUSE: Freeze/thaw

6.1 CONTROL: Specify designs that prevent or minimize freezing temperatures or prevent physical damage to the cell or case in the event of a freeze. Refer to applicable documents. Specify effects of failed-off heaters and necessary failure tolerance. Identify the minimum battery qualification temperature.

6.1.1 VERIFICATION: Provide results of freeze/thaw analysis or testing. Refer to applicable drawings and documents of temperature controls and cell/case construction.

7.0 CAUSE: Accumulation and ignition of hazardous gas mixture

7.1 CONTROL: For byproducts where controls are necessary for safe operation, specify the control system (e.g., control of free volume, ventilation, temperature control) that effectively maintains the generation and accumulation of hazardous gasses within a safety envelope of operation during worst case-conditions. Refer to attached supporting data H.

7.1.1 VERIFICATION: Summarize and refer to applicable qualification analysis or testing.

8.0 CAUSE: Leakage of battery container.

8.1 CONTROL: Battery container must be compatible with the chemicals that may be released from the batteries. Show the battery container design and how leakage is prevented under battery failure/normal use (e.g., Gortex filters, seals, etc.).

8.1.1 VERIFICATION: Summarize and refer to applicable qualification analysis or testing.

ATTACHED SUPPORTING DATA

A. Detailed description of all batteries. Include manufacturer, model number, number of cells, cell or battery voltage, capacity, series or parallel arrangement and a battery circuit diagram. Provide diagrams of cell/battery construction.
B. Summary of tests and/or analyses performed to establish maximum charge and discharge rates. Specify worst-case assumptions used. Provide complete schematics of battery circuits identifying circuit protection features.
C. Schematics of control and monitoring circuits preventing cell reversal. List precautions included within procedures.
D. Summary of tests and/or analyses showing structural performance under maximum design pressure conditions. Provide details of pressure relieving devices.
E. Detailed schematics of the heater system.
F. Summary of how the operational envelope or limits are defined. Specify all worst-case assumptions used.
G. Summary of test results, schematics of temperature control circuits, details of passive thermal control and operational thermal controls. Schematics should clearly indicate fault tolerance.
H. Summary of evolved gasses and electrolyte analyses to determine composition and quantity of evolved materials. Describe the ignition/explosion concentration and combustion characteristics of the gases generated.

HR GUIDELINE

HR NUMBER: **GHR-11**

TITLE: **Use of Flammable Materials**

SUBSYSTEM: Materials

HAZARD GROUP: Fire, Injury, Illness

DESCRIPTION OF HAZARD

Use of flammable materials leads to injury to the crew, damage to orbiter and other payloads through, fire, smoke and/or heat.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 209.2

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Any fire is considered catastrophic as it could lead to loss of orbiter or loss of crew.

HAZARD CAUSES

1. Use of flammable materials.

A fuel, an oxidizer, and an ignition source must all be present for combustion to occur. An oxidizing atmosphere is always present during ground operations and in manned flight compartments. Although the potential for ignition sources to be present can (and should) be minimized through electrical circuit protection, use of brushless motors, etc., it can never be completely eliminated when electrical power is present in the area. Therefore, elimination of the fuel by elimination of flammable materials or restriction of their use to applications in which they are unable to propagate a flame is the primary means of fire control approved by NASA for payload hardware.

ADDRESSING THE HAZARD

1.0 CAUSE: Use of flammable materials

1.1 CONTROL: Whenever possible, materials should be selected that have already been shown to meet the NHB 8060.1 test criteria in the use environment. Existing flammability test data are compiled in the NASA MSFC MAPTIS and published as the MSFC-HDBK-527/JSC 09604; materials that meet the NHB 8060.1 criteria are A-rated in these documents. Untested materials will be tested and classified in accordance with NHB 8060.1 or controlled as if they were flammable (see control 1.2)

1.1.1 VERIFICATION: Materials will be reviewed to verify an A-rating in MSFC-HDBK-527/JSC 09604.

1.2 CONTROL: The use of flammable materials that do not meet the flammability requirements of NHB 8060.1 is to be minimized. Configuration of any flammable materials is to be controlled as per guidelines specified in NSTS 22648.

1.2.1 VERIFICATION: Materials that do not have an A-rating from MSFC-HDBK-527/JSC 09604 will be tested in accordance to NHB 8060.1. Refer to test reports and include test summary.

1.2.2 VERIFICATION: Design will be reviewed to assure compliance with NSTS 22648 for application and configuration of materials. Refer to analysis and design configurations and final inspections to verify design is in compliance.

ATTACHED SUPPORTING DATA

A. Test report summary of any non-A rated materials (Test reports may be requested). This summary should document the rationales used to accept any materials that have not been tested or do not meet the requirements of NHB 8060.1. When flammability is controlled by the guidelines of NSTS 22648, referring to the specific guideline is all that is required. If flammability is controlled by other means (e.g., stowage of flammable materials when not in use), detailed justification of the application must be provided.
B. Documentation that final inspections were conducted verifying design compliance.

NOTE: If a materials and processes intercenter agreement is applicable, the only required control and verification in the HR is referring to the responsible NASA center materials certification. Attach the materials certification as supporting data. No additional supporting data is required.

HR GUIDELINE

HR NUMBER: **GHR-12**

TITLE: **Hazardous Fluids Leakage in the Payload Bay**

SUBSYSTEM: Materials

HAZARD GROUP: Corrosion, Contamination, Fire

DESCRIPTION OF HAZARD

Release of hazardous fluids in the payload bay through mechanical joints (metallic/nonmetallic seals), fusion joints (welds, brazes, bi-metallic transition joints), or containment walls results in damage to orbiter systems, or other payloads, due to contamination, corrosion, and/or fire.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 200.4a, 202.2d, 209.1a

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

The hazard potential of leaked fluid in the payload bay will be considered catastrophic until proven otherwise.

HAZARD CAUSES

1. Improper design.
2. Improper materials selection and/or processing.
3. Propagation of crack-like defects.
4. Improper workmanship and/or assembly.
5. Material Incompatibility.

ADDRESSING THE HAZARD

1.0 CAUSE: Improper design

1.1 CONTROL: Identify design features which preclude leakage under all environmental conditions. Include details of the following features: number and types of seals, types of joints, back-off prevention, design tolerance to worst-case mated configurations (e.g., misalignment, etc.). Refer to attached supporting data A and B.

1.1.1 VERIFICATION: Refer to and summarize qualification and acceptance testing. Show how the qualification tests conservatively encompass all environments to which the payload will be exposed during installation, flight, landing, etc.

NOTE: Environments which must be considered include appropriate combinations of thermal, vibration, pressure, mechanical, cycle life, etc.

NOTE: Thread friction alone is not considered an acceptable method of positive restraint for back-off prevention. When leakage is a catastrophic hazard, an independent means of positive restraint is necessary to prevent leakage from a mechanical fitting.

NOTE: Bimetallic transition joints. If bimetallic transition joints are used , then the supplier of the hardware must be identified. The process used in forming the joints is critical, and may require supplying the bimetallic joint certification data.

2.0 CAUSE: Improper material selection and processing including usage of stress corrosion sensitive materials
2.1 CONTROL: Use of proper materials selection as per document MSFC-HDBK-527F/JSC 09604 or equivalent and appropriate material processing controls. Refer to attached supporting data C and D.
2.1.1 VERIFICATION: Materials certification by the payload organization or responsible engineering discipline of the NASA center assuring proper selection, processing, and usage of materials.
2.2 CONTROL: Provide appropriate assessment for use of non-A rated or non-table 1 stress corrosion sensitive materials if their failure causes a critical or catastrophic hazard.
2.2.1 VERIFICATION: Summarize documentation and rationale for the usage of non-A rated or non-table 1 stress corrosion sensitive materials if their failure causes a critical or catastrophic hazard. Attach MUA's for stress corrosion sensitive materials whose failure causes a catastrophic hazard.

NOTE: Attachment of MUA's to HR's or documentation and rationale for the usage of SCC susceptible materials is not required for organizations covered by M&P intercenter agreements with JSC, since their review procedures and acceptance criteria have been determined equivalent to those of JSC.

3.0 CAUSE: Propagation of crack-like defects
3.1 CONTROL: Design the hardware to comply with NHB 8071.1
3.1.1 VERIFICATION: Identify fracture control plan. State fracture control categorization (fracture critical or non-fracture critical). Identify flaw screening technique (proof or NDE) and summarize results. Identify NDE inspection of fusion joints in fracture critical applications (lines/ fittings/ components/ container walls) and summarize results. Provide summary of fracture mechanics analysis.

4.0 CAUSE: Improper workmanship and/or assembly.
4.1 CONTROL: Ensure that flight hardware is built in accordance with approved design drawings and assembled as per approved procedures.
4.1.1 VERIFICATION: Refer to the document that shows that flight hardware is built in accordance with approved drawings and assembled per approved procedures. Summarize and refer to the report that identifies successful completion of acceptance testing.

5.0 CAUSE: Materials incompatibility.
5.1 CONTROL: Address fluid compatibility with the system components (consider single barrier failures). Address compatibility of cleaning materials with system seals/components
5.1.1 VERIFICATION: Refer to and summarize material compatibility assessment. Refer to and summarize compatibility data/tests. Refer to and summarize cleaning protocol and procedures.

NOTE: Assure fluids used to fill the system are not contaminated by ground servicing equipment and ground test equipment.

ATTACHED SUPPORTING DATA:

A. System level schematic of material containment including components, lines, fittings, seals, or other mechanical barriers.
B. Provide cut-away diagrams of the flow control devices.
C. Summary table giving rationale for usage of stress corrosion sensitive materials.
D. MUA's on stress corrosion sensitive materials whose failure causes a catastrophic hazard.

HR GUIDELINE

HR NUMBER: **GHR-13**

TITLE: **Ignition of Flammable Atmospheres**

SUBSYSTEM: Electrical

HAZARD GROUP: Fire, Explosion

DESCRIPTION OF HAZARD

Potential ignition of flammable atmospheres by a payload within the orbiter payload bay. Flammable atmospheres may be present during any de-orbit/landing operation.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 209, 219

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Ignition of a flammable atmosphere within the orbiter during the landing phase will result in the loss of the orbiter.

HAZARD CAUSES

1. Arcing/sparking devices.
2. Hot spots.
3. Static electricity discharge.

Typical causes are energy sources energetic enough to initiate combustion. Additional cause may be material incompatibility with hydrazine. All potential ignition sources should be addressed.

ADDRESSING THE HAZARD

1.0 CAUSE: Arcing/sparking devices.
1.1 CONTROL: Indicate the nominal powered state for the payload/experiment during launch and landing. Refer to attached supporting data A.
1.1.1 VERIFICATION: Refer to procedure, PIP or PIP annex that assures payload is to be unpowered. Review of design to assure no power is present.
1.2 CONTROL: Identify any devices that may have arcing or sparking potential. Indicate how these components will be isolated from the flammable atmosphere during ascent, descent and landing mission phases.
1.2.1 VERIFICATION: Refer to procurement specification for hermetically sealed devices. Refer to testing to verify seals on any sealed containers.

2.0 CAUSE: Hot spots.
2.1 CONTROL: Specify potential hot spots and how they are controlled during critical mission phases. Indicate the maximum temperature possible. Indicate if this is sufficient to serve as an ignition source. Refer to attached supporting data B.
2.1.1 VERIFICATION: Summarize and refer to the test or analysis that shows peak temperature and the potential for igniting a flammable atmosphere.

3.0 CAUSE: Static electricity discharge.
3.1 CONTROL: Describe all potential sources for static energy and storage sites. Describe grounding provisions that preclude static energy buildup or discharge. Include hazard controls associated with stray energy paths. Refer to attached supporting data D.
3.1.1 VERIFICATION: Specify tests that demonstrate validity of static discharge techniques. Refer to grounding inspections and tests.
3.2 CONTROL: Describe MLI construction and grounding techniques. Refer to attached supporting data C and D.
3.2.1 VERIFICATION: Refer to inspection of as built design. Refer to grounding tests.

ATTACHED SUPPORTING DATA

A. Schematics indicating inhibits to power use in bay.
B. Drawings and schematics indicating the location of heaters and the control electronics. Indicate thermal control devices or inhibits to operation. Provide thermal analysis summary.
C. Diagrams and drawings indicating the construction and grounding techniques for MLI.
D. Diagrams indicating the grounding locations.

HR GUIDELINE

HR NUMBER: **GHR-14**

TITLE: **Electrical Power Distribution Circuitry Damage**

SUBSYSTEM: Electrical

HAZARD GROUP: All

DESCRIPTION OF HAZARD

Damage to electrical power distribution circuitry can lead to damage to orbiter wiring, loss of safety critical circuitry, loss of redundant power sources, and/or generation of toxic products.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 201.3, 207, 213.1

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

HAZARD CAUSES

1. Short circuit or load failures which cause over-current in orbiter wiring powered from payload bus/source.
2. Toxic products are generated in the crew environment by overloaded payload wiring with improper circuit protection.
3. Electrical fault in a payload power circuit with improper circuit protection causes damage to co-located safety critical circuits resulting in removal of more then one inhibit.
4. Improper circuit protection and/or load management results in the loss of power distribution redundancy (see NSTS 18798, letter TA-91-006).

NOTE: Select only those causes applicable to your design.

ADDRESSING THE HAZARD

1.0 CAUSE: Short circuit or load failures which cause over-current in orbiter wiring powered from payload bus/source.
1.1 CONTROL: Specify wire sizing and circuit protection based on NSTS 18798, letter TA-92-038.
1.1.1 VERIFICATION: Review of design to assure implementation of proper wire sizing and circuit protection. Inspection of assembled hardware to ensure proper wiring/fusing is in place.

2.0 CAUSE: Toxic products are generated in the crew environment by overloaded payload wiring with improper circuit protection.
2.1 CONTROL: Specify wire sizing and circuit protection based on NSTS 18798, letter TA-92-038. (see exclusion for wiring downsized in avionics boxes).
2.1.1 VERIFICATION: Review of design to assure implementation of proper wire sizing and circuit protection. Inspection of as built hardware to ensure proper wire sizing/fusing is in place.

3.0 CAUSE: Electrical fault in a payload power circuit with improper circuit protection causes damage to co-located safety critical circuits resulting in the removal of more then one inhibit.
3.1 CONTROL: Specify wire sizing and circuit protection based on NSTS 18798, letter TA-92-038.
3.1.1 VERIFICATION: Review of design and inspection of as built hardware to assure implementation of proper wire sizing and circuit protection.

4.0 CAUSE: Improper circuit protection and/or load management results in the loss of power distribution redundancy.
4.1 CONTROL: Protection of wiring by use of appropriate circuit protection devices (refer to NSTS 18798 letters TA-91-006 and TA-92-038).
4.1.1 VERIFICATION: Review of design and inspection of as built hardware to ensure proper wire sizing and circuit protection is in place to protect redundant power sources.
4.2 CONTROL: Proper load constraints in place to protect against improper load conditions.
4.2.1 VERIFICATION: Review of PIP and PIP annex to verify time line constraints are in place to prevent load mismanagement.
4.2.2 VERIFICATION: Systems analysis and loads analysis.

ATTACHED SUPPORTING DATA

A. Schematic diagrams indicating power source, wire sizes, circuit protection devices, wire temperature ratings, etc.
B. Closeout verification summary with close-out photographs. (as requested)

HR GUIDELINE

HR NUMBER: **GHR-15**

TITLE: **Radio Frequency Radiation Interfering With STS Circuitry and/or Other Payloads**

SUBSYSTEM: Radiation

HAZARD GROUP: Radiation

DESCRIPTION OF HAZARD

RF radiation induces hazardous effects on orbiter avionics/circuitry, EMU, RMS, and/or other payloads. This hazard applies to all mission phases.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 201.3, 202.5

HAZARD CATEGORY

X CATASTROPHIC
X CRITICAL

If the value of the RF energy is above the limits specified in the ICD, then the hazard must be categorized as catastrophic. If it is below the ICD curve, then the hazard is categorized as critical when the payload bay doors are closed.

HAZARD CAUSES

1. Electrical/electronic failures.

Errors in the RF control system that can lead to inadvertent transmission should be addressed in detail.

ADDRESSING THE HAZARD

1.0 CAUSE: Electrical/electronic failures.
1.1 CONTROL: Specify the number and list the electrical inhibits that prevent occurrence of the hazard. Describe each control for each inhibit and establish its independence. Indicate how each inhibit is monitored. Describe ground/return leg inhibit and any RF commanding and encryption implemented. Define the fault tolerance of the system electrical inhibits including orbiter interfaces. Refer to attached supporting data A, B, and C.
1.1.1 VERIFICATION: Specify how it was verified that the electrical inhibits and controls can withstand the expected shuttle environment. Refer to qualification procedures and report.
1.2 CONTROL: Specify the fault tolerance to RF radiation exceeding ICD limits for planned operations. List the inhibits, controls and available monitors with flight procedures. Refer to attached supporting data A and C.
1.2.1 VERIFICATION: Summarize the analysis that verifies the fault tolerance of the control system. Describe how the analysis was performed to substantiate inhibit independence. Refer to the analysis.
1.2.2 VERIFICATION: Specify the methods for verifying and/or substantiating the safe state of the inhibits after the last inhibit cycle prior to launch. Methods for verifying inhibit status during other mission events (payload bay door opening/closing, payload retrieval, etc.) must also be specified.

NOTE: Inhibit monitors are required if radiation levels exceed ICD limits by more than 6 dB.

ATTACHED SUPPORTING DATA

A. Schematics showing the electrical inhibits, controls and monitors. Schematic should clearly show the independence of the inhibits.
B. Table listing the electrical inhibits, when last cycled, and how verified.
C. Data showing potential RF levels from the payload transmitters relative to ICD limit levels.

HR GUIDELINE

HR NUMBER: **GHR-16**

TITLE: **Exposure of the Orbiter/Payload to Excessive Levels of EMI Radiation**

SUBSYSTEM: Non-Ionizing Radiation

HAZARD GROUP: Radiation

DESCRIPTION OF HAZARD

Payload circuitry emits excessive EMI (radiated and/or conductive) or the payload itself is susceptible to its surrounding EMI environment.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 212.2

HAZARD CATEGORY

X CATASTROPHIC (If P/L safety critical avionics upset or damaged)
X CRITICAL (If P/L emissions exceed ICD limits)

HAZARD CAUSES

1. Excessive electromagnetic conducted or radiated emissions from payload components operation.
2. Payload susceptible to orbiter or other payload produced EMI.

ADDRESSING THE HAZARD

1.0 CAUSE: Excessive electromagnetic conducted or radiated emissions from the operation of the payload components.
1.1 CONTROL: Design payload circuits such that conducted emissions/transients are within limits specified in NSTS 07700, Vol XIV, Attachment 1 (ICD 2-19001).
1.1.1 VERIFICATION: Provide a systems-level conductive emissions measurement and compare results to allowables specified in ICD 2-19001. Refer to EMI test report acceptance.
1.2 CONTROL: Design payload circuits such that radiated emissions are below allowable limits for other payloads.
1.2.1 VERIFICATION: Provide a systems-level radiative emissions measurement and compare results to allowables specified in ICD 2-19001. Refer to EMI test report acceptance.

2.0 CAUSE: Payload susceptible to orbiter or other payload produced EMI.
2.1 CONTROL: Design payload circuits such that they are not susceptible to the payloads expected EMI environment.
2.1.1 VERIFICATION: Provide a test report which shows payload circuit compatibility with the EMI environment specified in ICD 2-19001. Refer to attached supporting data A.

NOTE: An EMI test report should be prepared, using the data described in the verifications listed above, and submitted to JSC EMI experts for acceptance.

ATTACHED SUPPORTING DATA

A. Letter of EMI test report acceptance from JSC EMI experts.

HR GUIDELINE

HR NUMBER: **GHR-17**

TITLE: **Rupture and/or Explosion of Pressure System**

SUBSYSTEM: Pressure, Structure

HAZARD GROUP: Fire, Explosion

DESCRIPTION OF HAZARD

Rupture/explosion of pressure system and or pressure vessel results in significant damage to/loss of orbiter, crew or other payloads.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 200.4a, 201.3, 202.2c, 208.3, 208.4, 208.4a, 208.4c, 208.4d, 209.1a

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Rupture and/or explosion of a pressurized system can only be considered a catastrophic hazard because of the potential loss of the orbiter or crew.

HAZARD CAUSES

1. Inadequate design strength to withstand MDP and other loading environments.
2. Improper materials selection and processing, including usage of stress corrosion sensitive materials.
3. Materials incompatibility.
4. Improper workmanship and/or assembly.
5. Contamination or catalytic reaction with reactive fluid.
6. Propagation of crack-like defects.
7. Adiabatic compression detonation (particularly applicable to hydrazine systems).
8. Localized overheating causes exothermic reaction.
9. Liquid freezing/thawing results in rupture.
10. Overfilling of pressure vessel/system during ground operations.
11. Inadequate pressure to maintain structural integrity.

ADDRESSING THE HAZARD

1.0 CAUSE: Inadequate design strength to withstand MDP and other loading environments.

1.1 CONTROL: Document the actual FOS for each item of the pressurized system. Show compliance with minimum FOS with respect to MDP for each item in accordance with NSTS 1700.7, paragraph 208.4. Identify the specification (such as MIL-STD 1522 or DOT) with which the pressure vessel complies. Refer to attached supporting data A, B, and D.

1.1.1 VERIFICATION: Summarize and refer to analyses and/or tests used to determine MDP. Summarize and refer to analyses and/or tests used to determine each item FOS. Document any hardware proof testing. Refer to the tests and/or analyses used to establish independence of flow control devices. Summarize tests results that assure functionality of inhibits, monitors, and controls. Summarize pressure integrity check of the system. Review of design to assure proper installation of the flow control devices.

1.1.2 VERIFICATION: Pressure vessels. Refer to the conducted qualification and acceptance program for design burst factor, actual burst pressure if applicable and proof factor.

NOTE: MDP for a pressurized system shall be the highest pressure defined by maximum relief pressure, maximum regulator pressure or temperature. Transient pressures shall be considered. Design factors of safety shall apply to MDP. Where pressure regulators, relief devices, and/or a thermal control system (e.g., heaters) are used to control pressure, collectively they must be two-fault tolerant from causing the pressure to exceed the MDP of the system. Additional failures or conditions that should be considered in determining MDP include:

Internal chemical reactions
Mechanical component failures (valves, burst disks) (refer to NSTS 18798, letter TA-88-074 for fault tolerance of burst disks)
Electrical component/control failures
Pressure system leakage from high pressure side to low pressure side
Hot abort sites - (NSTS 18798, letter TA-90-008)
Heater failures

NOTE: Bimetallic transition joints: If bimetallic joints are used in the pressure system, then the supplier of the hardware must be identified. The process used in forming the joints is critical, and may require supplying the bimetallic joint certification data.

NOTE: Relief devices: The MDP will often exceed the set point pressure of the relief device due to flow restrictions at full flow capability. With this in mind, consider back pressure effects at maximum flow when sizing relief devices.

NOTE: Burst pressure: Some components may have an upstream safety factor which is different than the downstream factor of safety. For example, some pressure regulators have a burst pressure at the inlet that is different than the burst pressure at the outlet. This should be taken into account while defining safety factor of the given component with respect to MDP.

NOTE: Internal and external loads: MDP assessment should include internal loads as well as external loads. For example, an isolation valve in a liquid system may be subject to internal loads such as back pressure and external loads such as orbiter landing. The combination of the worst case loads need to be considered as part of the safety assessment to assure the isolation valve will not latch open if it must remain closed to preclude a hazardous event.

2.0 CAUSE: Improper material selection and processing including usage of stress corrosion sensitive materials.
2.1 CONTROL: Use of proper materials selection as per document MSFC-HDBK-527/JSC 09604 or equivalent and appropriate material processing controls.
2.1.1 VERIFICATION: Materials certification by the payload organization or responsible engineering discipline of the NASA center assuring proper selection, processing, and usage of materials.
2.2 CONTROL: Provide appropriate assessment for use of non-A rated or non-table 1 stress corrosion sensitive materials if their failure causes a critical or catastrophic hazard. Refer to attached supporting data F and G.
2.2.1 VERIFICATION: Documentation and rationale for the usage of non-A rated or non-table 1 stress corrosion sensitive materials if their failure causes a critical or catastrophic hazard. Attach MUA's for stress corrosion sensitive materials whose failure causes a catastrophic hazard.
2.3 CONTROL: Address compatibility of dissimilar metals.
2.3.1 VERIFICATION: Materials certification by the payload organization or responsible engineering discipline of the NASA center assuring proper selection, processing, and usage of materials.

NOTE: Attachment of MUA's to HR's or documentation and rationale for the usage of SCC susceptible materials is not required for organizations covered by M&P intercenter agreements with JSC, since their review procedures and acceptance criteria have been determined equivalent to those of JSC.

3.0 CAUSE: Materials incompatibility.
3.1 CONTROL: Address fluid compatibility with the pressure system components (consider single barrier failures).
3.1.1 VERIFICATION: Summarize material compatibility assessment. Refer to compatibility data and/or tests.
3.2 CONTROL: Address compatibility of cleaning materials with pressure system seals/components.
3.2.1 VERIFICATION: Refer to cleaning protocol and procedures.

4.0 CAUSE: Improper workmanship and/or assembly.
4.1 CONTROL: Ensure that flight hardware is built in accordance with approved design drawings and assembled as per approved procedures.
4.1.1 VERIFICATION: Refer to the document that shows that flight hardware is built in accordance with approved drawings and assembled per approved procedures.
4.2 CONTROL: Flight hardware acceptance testing.
4.2.1 VERIFICATION: Refer to report that identifies successful completion of acceptance testing.

5.0 CAUSE: Contamination or catalytic reactions with reactive fluid.
5.1 CONTROL: Identify fluid loading conditions.
5.1.1 VERIFICATION: Refer to fluid loading procedures.
5.2 CONTROL: Describe the approach that verifies pressure and temperature remain stable (within expected levels) after fluid loading.
5.2.1 VERIFICATION: Refer to procedures used to verify that pressure and temperature remain stable after fluid loading.

6.0 CAUSE: Propagation of crack-like defects.
6.1 CONTROL: Identify/summarize fracture control plan. State fracture control categorization (fracture critical or non-fracture critical).
6.1.1 VERIFICATION: Refer to fracture mechanics analyses.
6.2 CONTROL: Identify whether pressure vessels are leak before burst (non-hazardous fluid) or safe-life.
6.2.1 VERIFICATION: Refer to leak before burst analysis and/or test.
6.3 CONTROL: (For safe-life pressure vessels) Identify weld inspection prior to and after proof testing. Identify flaw screening technique (proof test or NDE). Identify procedures/protection to prevent handling damage of composite overwrapped pressure vessels. Identify NDE inspection of fusion joints in fracture critical applications (lines/fittings/components). For composite overwrapped pressure vessels, identify their stress rupture life
6.3.1 VERIFICATION: Refer to NDE inspections. Refer to proof test summary. Review handling procedures and/or inspections. Review stress rupture life assessment.

7.0 CAUSE: Pressure surge results in ACD (particularly applicable to hydrazine systems).
7.1 CONTROL: Demonstrate flight hardware (or high fidelity flight qualified hardware) system insensitivity to ACD.
7.1.1 VERIFICATION: Refer to ACD insensitivity test. Refer to ground filling procedure.
7.2 CONTROL: (If sensitive to ACD) Identify the system fault tolerance to inadvertent isolation valve operation. Identify inhibits, monitors and controls that preclude isolation valve operation. Identify when the isolation valve will be activated. Refer to attached supporting data C.
7.2.1 VERIFICATION: Summarize and refer to analyses/tests used to identify fault tolerance as well as inhibit and control independence.
7.3 CONTROL: Describe the design features to preclude pressure surges that result in ACD. Refer to attached supporting data D.
7.3.1 VERIFICATION: Refer to as-built hardware inspections.

8.0 CAUSE: Localized overheating causes exothermic reaction.
8.1 CONTROL: Ensure that highest attainable temperature after any two worst case credible failures does not exceed critical temperature limits. Refer to attached supporting data C.

8.1.1 VERIFICATION: Refer to analysis used to determine fault tolerance and independence of controls and inhibits.
8.1.2 VERIFICATION: Refer to thermal analysis report and summary.
8.1.3 VERIFICATION: Refer to tests that assure functionality of the safety inhibits, controls, and monitors.

NOTE: Localized overheating can be created by several different sources including failed-on heaters and valve solenoids. Thermal soak back due to thruster firing should be considered only when this is a hazard to the orbiter.

NOTE: Critical temperature limits should include those set by fluid thermal decomposition and material compatibility.

9.0 CAUSE: Liquid freezing/thawing results in rupture.
9.1 CONTROL: Ensure that lowest attainable temperature after any two worst case credible failures for all shuttle mission phases does not freeze fluid. Consider abort to a worst case cold landing site in this assessment. Refer to attached supporting data E.
9.1.1 VERIFICATION: Review assessment and tests that verifies fault tolerance and control independence.
9.1.2 VERIFICATION: Refer to tests that assure functionality of safety controls and monitors.
9.2 CONTROL: Describe the thermal protection to preclude freezing.
9.2.1 VERIFICATION: Refer to thermal analysis report and summary that precludes freezing.

10.0 CAUSE: Overfilling of pressure vessel/system during ground operations.
10.1 CONTROL: Describe ground procedures used to prevent overfilling of pressure vessels/system.
10.1.1 VERIFICATION: Refer to pressure vessel/system ground filling procedures

11.0 CAUSE: Inadequate pressure to maintain structural integrity
11.1 CONTROL: Identify whether pressure stabilization is required to maintain the structural integrity of the pressure vessel. If this is the case, then: Identify the critical pressure and how it will be maintained and monitored. Applications using pressure stabilized tanks refer to implementation of compliance to NSTS 18798, letter TA-89-064. Refer to attached supporting data C.
11.1.1 VERIFICATION: Refer to the assessment identifying the minimum tank pressure to ensure structural integrity under launch and landing loads.
11.1.2 VERIFICATION: Refer to the design features used to monitor and maintain the minimum pressure required.

ATTACHED SUPPORTING DATA

A. Provide a table identifying the following for all pressure system items:
   MDP
   FOS
   Burst pressure
   Proof test level (if performed)
   Identify method used to determine the above values (tests or analyses)

B. Provide cut-away diagrams of the flow control devices
C. Detailed electrical schematics identifying inhibits, controls, and monitors (where applicable)
D. System level schematic of pressure system including components, lines, fittings, monitoring points, and control paths
E. Detailed electrical schematics identifying heater monitors and controls
F. Summary table giving rationale for usage of stress corrosion sensitive materials
G. MUA's on stress corrosion sensitive materials whose failure causes a catastrophic hazard

HR GUIDELINE

HR NUMBER: **GHR-18**

TITLE: **Leakage/Rupture of Sealed Containers**

SUBSYSTEM: Structural-Sealed Containers

HAZARD GROUP: Collision, Fire, Explosion

DESCRIPTION OF HAZARD

This HR addresses (1) hazardous rupture due to a differential pressure change (positive or negative) and (2) any hazard that may result from loss of the contained non-hazardous environment. This HR is to address components of spacecraft and cargo element structures that fall under the definition of sealed containers given in NSTS 1700.7, Appendix A. State how a container will be evaluated for hazard potential. Provide results of this assessment upon completion. Refer to attached supporting data A and B.

Elements not designed to contain an environment should be addressed in the Structural Failure HR; battery boxes should be addressed in the Battery Leakage/Rupture HR.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 208.5

HAZARD CATEGORY

X CATASTROPHIC
X CRITICAL

This hazard should be assessed for hazard potential based upon the effects to the orbiter, crew, and other payloads due to the rupture/collapse or release of the environment from the sealed container.

HAZARD CAUSES

1. Internal pressure and/or external pressure exceeds strength capability. Sources of pressure differential are ascent/descent pressure profiles and thermal profiles.
2. Excessive leakage (if loss of internal environment creates a hazard).

The causes applicable to this HR are those that can increase the pressure within the sealed container, inability of the sealed container to contain its environment, or inability of the container to withstand external pressures.

ADDRESSING THE HAZARD

1.0 CAUSE: Internal pressure and/or external pressure exceeds strength capability. Sources of pressure differential are ascent/descent pressure profiles and thermal profiles.

1.1 CONTROL: Specify design criteria for containers with hazard potential. Refer to applicable implementing document. Define maximum expected pressure differential and specify design safety factor against ultimate (1.5 or greater.)

1.1.1 VERIFICATION: Summarize and refer to the strength analysis and visual inspection requirements for the flight hardware. (A proof-test is acceptable in lieu of visual inspection.) Refer to attached supporting data C.

2.0 CAUSE: Excessive leakage (if loss of internal environment creates a hazard).

2.1 CONTROL: Specify maximum acceptable leak-rate and how it was established. If controlling a catastrophic hazard, fracture critical assessment, proof test, and NDE are required.

2.1.1 VERIFICATION: Specify method (i.e., analysis or test) that will assure the maximum leak rate will not cause a loss of the internal environment while in the safe proximity of the orbiter. Refer to the applicable document.

2.1.2 VERIFICATION: Specify method that assures the flight hardware meets the leakage criteria. Refer to the leak-test procedures and/or leak analysis report and summarize results of applicable tests.

ATTACHED SUPPORTING DATA

A. Summary of hazard potential evaluation giving components evaluated and safety conclusion.
B. Summary of flight hardware acceptance rationale for components classified as presenting a hazard.
C. Summary of analyses and tests.

NOTE: Sealed containers of any size, fabricated of conventional metals or fiberglass, with maximum pressures $\leq$ 20 psid and a minimum FOS of 1.5 will be accepted as leak before burst without formal assessment.

HR GUIDELINE

HR NUMBER: **GHR-19**

TITLE: **Structural Failure**

SUBSYSTEM: Structures/Mechanisms

HAZARD GROUP: Collision

DESCRIPTION OF HAZARD

Structural failure of load carrying elements causes hardware to deform or break away and collide with the orbiter or crew during launch, landing or on-orbit operations. All load carrying elements including those made of metals/alloys, Beryllium, composites, bonded structure etc. should be considered.

The structural hardware addressed in this HR should also include any mechanisms which comprise a structural load path.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 208.1,
NSTS 18798, letter TA-92-013, NS2/90-208, and TA-93-037

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

HAZARD CAUSES

1. Inadequate structural strength for induced loads and thermal effects during all mission phases.

NOTE: Generally load sources to be considered include those associated with nominal flight events, such as launch, ascent, on-orbit operations, descent and nominal end-of mission landing (if applicable). Loads from a shuttle abort landing and an emergency landing must be considered even for non-returnable payloads. Loads due to on-orbit operations are often payload unique and need to be considered when applicable. On-orbit operations might include orbiter reaction control system jet firings, orbital maneuvering system engine burns, remote manipulator system operations, astronaut intra- and extravehicular activities. Payloads which might see configuration changes on-orbit need to be assessed for return configurations in which they are safe to land. Differential pressure on "vented" structure during ascent and descent must also be accounted for. Environmental loads such as thermal, acoustic, random vibration, and mechanical shock shall be combined with the mechanical and pressure loads as appropriate.

2. Improper material selection and processing, including usage of stress corrosion sensitive materials.
3. Metal fatigue or propagation of inherent cracks/internal flaws.
4. Use of counterfeit or substandard fasteners.
5. Loosening of mechanical (safety critical) fasteners.
6. Improper manufacture and/or assembly.

ADDRESSING THE HAZARD

1.0 CAUSE: Inadequate structural strength for induced loads and thermal effects during all mission phases.

1.1 CONTROL: Summarize how the design of all structures provide positive margins of safety under all loading conditions with respect to the required factors of safety defined in NSTS 07700, Vol. XIV, and NSTS 1700.7. Identify the factors of safety used.

1.1.1 VERIFICATION: Verification of this hazard control involves loads and thermal analyses, stress analyses, strength testing, model verification testing and environmental testing per NSTS 14046. The following documentation should be referred to (as applicable) as Verification items:

a. Structural Verification Plan
b. Design Loads Report
c. Stress Analyses
d. Strength Test Plan and Report
e. Math Model Verification Test Plan and Report
f. Verification Loads and Thermal Analyses Reports
g. Environmental, (e.g., vibroacoustic) Test Plan and Report

1.2 CONTROL: Identify operational controls/constraints to ensure integrity of structural hardware. For example, a unique payload configuration might need to be in free drift or maintain certain attitudes for thermal conditioning of structural composites.

1.2.1 VERIFICATION: Review of PIP, PIP annex, and/or procedures to ensure that operational controls are in place.

2.0 CAUSE: Improper material selection and processing, including usage of stress corrosion sensitive materials.

2.1 CONTROL: Document that materials were selected in accordance with requirements specified in MSFC-HDBK-527/JSC 09604 and MSFC-SPEC-522 or equivalent. Provide appropriate rationale for use of non-A rated or non-table 1 materials if their failure causes a critical or catastrophic hazard.

2.1.1 VERIFICATION: Certification by the payload organization or responsible NASA center assuring proper selection, processing and usage of materials.

2.1.2 VERIFICATION: Documentation and rationale for the usage of non-A rated or non-table-1 stress corrosion sensitive materials if their failure causes a critical or catastrophic hazard. Attach MUA's for stress corrosion sensitive materials whose failure causes a catastrophic hazard. Refer to attached supporting data A.

Note: Attachment of MUA's to HR's or documentation and rationale for usage of SCC susceptible materials is not required for organizations covered by M&P intercenter agreements with JSC, since their M&P review procedures and acceptance criteria have been determined equivalent to those used by JSC.

3.0 CAUSE: Metal fatigue or propagation of inherent cracks/internal flaws.

3.1 CONTROL: Summarize the implementation of the fracture control in accordance with an approved fracture control plan or submit fracture control plan for review/approval. Show compliance with NHB 8071.1 and NSTS 18798 low risk fracture part letter TA-92-013.

3.1.1 VERIFICATION: Review of fracture control plan. Assurance of adherence to plan by submission of fracture control summary report at phase III. Refer to attached supporting data B.

3.2 CONTROL: Specify the proof-test and/ or NDE used for screening flaws. Refer to safe-life analyses on fracture critical parts.

3.2.1 VERIFICATION: Refer to proof-test/NDE test results. Review fracture analyses report.

4.0 CAUSE: Use of counterfeit or substandard fasteners.
4.1 CONTROL: Document methods used to assure that no counterfeit or substandard fasteners are not used where their failure would cause a hazard. Summarize the traceability of the fasteners to the manufacture from which they where procured.
4.1.1 VERIFICATION: Summary of report of lot verification testing and vendor certification program.

5.0 CAUSE: Loosening of mechanical (safety critical) fasteners.
5.1 CONTROL: When loosening of fasteners could cause a hazard, indicate the method of providing positive-locking features to the fasteners. Metal or plastic locking features, lock wire and cotter pins are examples of positive locking features which either prevent or resist the loosening of fasteners. The effectiveness of alternate methods of locking, such as adhesive locking must be justified by test.
5.1.1 VERIFICATION: Review of design to verify selection of appropriate, proven locking features. Acceptance vibration or acoustic testing, as appropriate. Running torque verification during re-installation of fasteners. Visual inspection of lock wire or cotter pins on as-built hardware for proper rigging. Testing of alternate locking methods.

6.0 CAUSE: Improper manufacture and/or assembly.
6.1 CONTROL: Summarize how flight hardware is built in accordance with approved design drawings and assembled as per approved procedures.
6.1.1 VERIFICATION: Review of design. Tests should be conducted to assure functionality. Review of crew procedures, PIP or PIP annex.
6.2 CONTROL: For on-orbit assembly, summarize crew procedures and design features that allow for proper assembly.
6.2.1 VERIFICATION: Review of crew procedures, PIP or PIP annex. Review of design, analyses, tests for proper design and operational capability.

ATTACHED SUPPORTING DATA

A. Screening summary table for stress corrosion sensitive materials. MUA's on stress corrosion sensitive materials whose failure causes a catastrophic hazard.
B. Fracture control summary report:
The minimum information required in a fracture control summary report is indicated below. It should also be noted that for organizations covered by an intercenter agreement on fracture control, a detailed fracture control summary is not required to be submitted to JSC. The details should be on file and available if questions arise. A certification from the responsible NASA center, with the intercenter agreement, that the payload meets the fracture control requirements is adequate and acceptable. For organizations not covered by the intercenter agreement, a fracture control summary should be submitted by the phase III safety review for JSC review and approval.

Fracture control summary report (from JSC 25863)

The FCSR will document the completed fracture control program in summary form. As a minimum, the following information will be provided:

1. Identification of fracture critical and low risk fracture parts showing the material and heat treatment used and the basis for acceptability (safe-life analysis, test, acceptable durability, insignificant fatigue loading, etc.) Fracture critical parts that are limited life will be specifically noted.
2. Identification of the NDE and/or tests applied for fracture control purposes to each fracture critical part and to each low risk part requiring specific inspection.
3. Identification of fail-safe parts that were classified by engineering judgment and a brief statement of the rationale applied.

4. A statement that inspections or tests specified for fracture control were, in fact, applied and in an acceptable manner.

5. A statement that hardware configuration has been verified for fracture critical parts/components.
6. A statement that proper materials usage has been verified for fracture critical parts/components.
7. If applicable, a summary discussion of alternative approaches or specialized assessment methodology applied but not specifically covered in this FCP.
8. If applicable, identification of any special considerations involving fracture mechanics properties or data, inspections, analysis, etc. not covered in this FCP.
9. Copies of MUA's for fracture critical or low risk parts/components and a summary of DR's, or equivalent reviews, of anomalies that could affect the performance of fracture critical parts/components.
10. Identification of handling procedures and/or protective measures used to prevent damage of fracture critical composite/bonded components.
11. If no parts/components or procedures are identified during the program that require the information as listed above, a statement to that effect will be submitted as the FCSR.

Supporting detailed documentation such as calculations, reports, procedures or drawings, etc., will not be submitted as part of the FCSR but will be made available for review if requested.

The FCSR is needed by the phase III safety review.

HR GUIDELINE

HR NUMBER: **GHR-20**

TITLE: **Failure of Rotating Equipment**

SUBSYSTEM: Structures, Mechanical

HAZARD GROUP: Collision

DESCRIPTION OF HAZARD

Break-up of rotating equipment (reaction wheel, fan, gears, etc.) generates debris, resulting in impact with the orbiter, crew or other payloads.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.2, 200.3, 201.3, 208

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

The breaking up of rotating equipment generates debris. This debris can puncture critical components leading to damage to orbiter or loss of crew.

HAZARD CAUSES

1. Mechanical component failure at high rotation rate due to: inadequate strength, usage of materials susceptible to stress corrosion cracking, initiation and/or propagation of flaws or crack-like defects, or overspeed of rotating equipment due to controller failure.

NOTE: Structural strength/crack-like defects. The exceedence of the structural strength or propagation of crack-like defects are the primary causes of this hazard. The exceedence of strength can be driven either by the rotational energy or launch loads not being carried properly by caging mechanisms. Failures that allow for exceeding the "safe" rotational speed must be addressed.

ADDRESSING THE HAZARD

1.0 CAUSE: Mechanical component failure at high speed rotation.
1.1 CONTROL: Summarize the capability of the rotating equipment to withstand shuttle loads. Identify any conditions or constraints that exist for the rotating equipment to withstand launch, on-orbit and/or landing loads. Refer to attached supporting data C.
1.1.1 VERIFICATION: Summarize structural analyses and testing. Refer to the analyses and tests used to establish compatibility with the shuttle environments.
1.2 CONTROL: Specify any constraints to be placed upon the equipment operation. Establish fault tolerance to assure constraints remain in place. Refer to attached supporting data B.
1.2.1 VERIFICATION: Review of PIP, PIP annex and/or procedures for operational constraints of rotating equipment. Refer to the analysis that assures fault tolerance.
1.3 CONTROL: Summarize that materials are selected in accordance with Table 1 of MSFC-SPEC-522 or A-rated materials in accordance with MSFC-HDBK-527. Provide appropriate rationale for use of non-A-rated or non-table 1 materials if their failure causes a critical or catastrophic hazard. Refer to attached supporting data G and H.
1.3.1 VERIFICATION: Materials certification by the payload organization or responsible engineering discipline of the NASA center assuring proper selection, processing, and usage of materials.

1.3.2 VERIFICATION: Documentation and rationale for the usage of non-A rated or non-table 1 stress corrosion sensitive materials if their failure causes a critical or catastrophic hazard. Attach MUA's for stress corrosion sensitive materials whose failure causes a catastrophic hazard.

1.4 CONTROL: Refer to the fracture control plan implementation. Identify the fracture control classification of the rotating equipment. Refer to attached supporting data D.

1.4.1 VERIFICATION: Summarize fracture control analyses, testing and inspections. Summarize rotational energy analysis. Refer to the results of NDI. Refer to the containment analysis.

1.5 CONTROL: Establish that the nominal and maximum rotational speeds are less than the maximum safe speed. Maximum values must be established by the speed that is attainable after two control failures, or the speed attainable if all available power is supplied directly to the drive motors should such controls not exist. Refer to attached supporting data E.

1.5.1 VERIFICATION: Refer to the analyses and/or tests used to establish the nominal and maximum values of rotational speed and the maximum safe rotational speed.

1.6 CONTROL: If the maximum rotational speed can exceed the maximum safe rotational speed then specify the fault tolerance to preventing device overspeed. Include descriptions of each level of control. Describe the monitoring available to the crew and any actions available if an overspeed occurs. Refer to attached supporting data F.

1.6.1 VERIFICATION: Refer to the analyses and/or tests that verify the fault tolerance of the control system.

NOTE: If the system application is a low energy device then NSTS 18798, letter TA-94-057 may apply.

NOTE: If the energy at maximum speed is greater than or equal to 14,240 ft-lbs, the hardware is fracture critical by definition. Typically proof testing/NDE inspections are done to screen for flaws and a fracture mechanics analysis is performed to ensure safe-life on fracture critical hardware per NHB 8071.1. In unique cases where inspection/test requirements per NHB 8071.1 are not possible or cannot be properly applied, the device will be acceptable if containment can be assured and a functional loss of the device does not result in a catastrophic hazard.

NOTE: Devices with rotational energy at maximum speed less than 14,240 ft-lbs are not fracture critical by definition. If break-up should occur, containment can be demonstrated by either analysis or test.

ATTACHED SUPPORTING DATA

A. Drawing of device mechanisms and structure.
B. Schematics indicating electrical inhibits, controls and monitors. Schematic should show independence of inhibits and controls. Control paths should be fully incorporated into diagrams.
C. Structural test data and/or structural analysis margins.
D. Fracture control summary.
E. Tabular data showing rotational equipment nominal speed(s) throughout mission, when they change and the maximum speed(s).
F. Schematics indicating speed controller circuitry and fault tolerance to overspeed condition.
G. Provide a summary table giving rationale for usage of stress corrosion sensitive materials.
H. MUA's on stress corrosion sensitive materials whose failure causes a catastrophic hazard.

HR GUIDELINE

HR NUMBER: **GHR-21**

TITLE: **Safety Critical Mechanical System Functional Failure or Partial/Incomplete Deployment/Jettison**

SUBSYSTEM: Mechanical Systems

HAZARD GROUP: Collision

DESCRIPTION OF HAZARD

Mechanical systems fail resulting in a hazardous condition. This HR addresses the complete functional cycle for mechanical systems that may have a requirement to return to the original stowed (i.e., safe) configuration. Also includes "must-work" functions and debris generation.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.1, 200.2, 200.3, 201.1, 202.4, 203, 208.1, 208.2, 208.3, 210.2

NOTE: Design must incorporate an independent alternate provision for safing single-fault-tolerant mechanical systems used to control a catastrophic hazard. Specify where fault tolerance is used to meet safety requirements and where design for minimum risk is used.

HAZARD CATEGORY

X CATASTROPHIC
X CRITICAL

Worst case hazards include: 1) Preventing payload bay door closure, 2) Incomplete deployment/jettison that impacts crew, orbiter, or payload hardware, 3) Hazards that could lead to the loss of the crew-habitable environment.

HAZARD CAUSES

1. Galling, binding, jamming, friction/cold welding, etc. due to improper design, improper materials selection/processing, or debris.
2. Mechanical system provides insufficient force margin to overcome/withstand mechanical loads.
3. Environment prevents mechanical system from operating or performing a function.
4. Structural failure of mechanism components.
5. Electrical component failure.
6. Pyrotechnic device failure to operate and/or debris generation.
7. Improper assembly/workmanship (on ground or on orbit) and cleanliness (on ground).
8. Improper sequencing due to improper system design (applies to pyrotechnic systems and mechanical systems) or procedural errors.

ADDRESSING THE HAZARD

1.0 CAUSE: Galling, binding, jamming, friction/cold welding, etc. due to improper design, improper materials selection/processing, or debris.

1.1 CONTROL: Identify the design provisions which preclude jamming and/or binding of mechanical device under all environmental conditions. Environments which must be considered include thermal, vibration, and loads. Refer to attached supporting data A, B, C, and G.

1.1.1 VERIFICATION: Summarize inspection procedures to assure that mechanical system is built to drawing specifications and tolerances.
1.1.2 VERIFICATION: Summarize qualification testing.
1.1.3 VERIFICATION: Summarize analyses and/or tests that demonstrate jamming, binding, friction/cold welding are precluded.
1.2 CONTROL: Use proper materials and lubrication selection as per MSFC-HDBK-527/JSC 09604 (or equivalent) and appropriate material processing controls. Refer to attached supporting data D.
1.2.1 VERIFICATION: Materials must be certified by the customer or responsible engineering discipline of the NASA center to assure proper selection, processing and usage of materials.
1.2.2 VERIFICATION: Summarize material compatibility assessment.
1.2.3 VERIFICATION: Summarize compatibility data/tests.
1.3 CONTROL: Identify shielding techniques used to preclude debris from entering the mechanical system.
1.3.1 VERIFICATION: Identify mandatory inspection points to ensure shielding (shrouds/covers) is properly installed . Refer to attached supporting data I.

2.0 CAUSE: Mechanical system provides insufficient force margin to overcome and withstand mechanical loads.
2.1 CONTROL: Describe how the design provides the required operating force margin under worst-case mechanical loads. Summarize compliance to NSTS 18798, letter TA-94-041. Refer to attached supporting data E.
2.1.1 VERIFICATION: Provide summary of analysis and/or test of load conditions at all points in mechanism travel to establish operating force margins.
2.2 CONTROL: Describe how the design provides the required holding force margin of safety to overcome any load-induced failures in the primary mechanical system. Summarize compliance to NSTS 18798, letter TA-94-041.
2.2.1 VERIFICATION: Provide summary of analysis and/or tests of load conditions to prevent inadvertent operation.

3.0 CAUSE: Environment prevents mechanical system from operating or performing a function. (Environments which must be considered include thermal, vibration, and loads.)
3.1 CONTROL: Describe how mechanical system satisfies worst-case environmental requirements.
3.1.1 VERIFICATION: Summarize environmental conditions considered and how the worst-case environment was chosen.
3.1.2 VERIFICATION: Summarize environmental qualification test plan.
3.1.3 VERIFICATION: Provide summary of analysis and/or test of motion at every point in mechanism travel under worst-case environmental conditions.
3.2 CONTROL: Describe mechanical system design provisions (independence, fault tolerance, etc.) which overcome any environmentally-induced failures. Describe alternate method to perform functions, as required.
3.2.1 VERIFICATION: Provide summary of hardware inspection, functional tests, independence tests, and analyses/tests of alternate methods.

4.0 CAUSE: Structural failure of mechanical system components.
4.1 CONTROL: Describe factor of safety used in design of mechanical system components. Refer to compliance to NSTS 18798, letter TA-94-041.
4.1.1 VERIFICATION: Provide summary of applicable analyses and/or tests.
4.2 CONTROL: Provide proper indications to ensure that the critical load carrying position of the mechanical system has been achieved.
4.2.1 VERIFICATION: Provide summary of verification tests of critical load carrying position indications.

5.0 CAUSE: Electrical component failure.
5.1 CONTROL: Specify the number and list the electrical inhibits that prevent occurrence of the hazard. Describe each control for each inhibit and establish its independence. Indicate how each inhibit is monitored. Describe ground/return leg inhibit and any RF commanding and encryption implemented. Define the fault tolerance of the system electrical inhibits including orbiter interfaces. Refer to attached supporting data H.
5.1.1 VERIFICATION: Provide summary of electrical schematics, electrical system test (from input stimuli to end function) results, electrical redundancy tests.

6.0 CAUSE: Pyrotechnic device failure to operate and/or debris generation.
6.1 CONTROL: Use pyrotechnic devices which meet criteria specified in NSTS 08060. (Refer to pyrotechnic HR's.) Refer to attached supporting data F.
6.1.1 VERIFICATION: Verify that pyrotechnic devices meet criteria specified in NSTS 08060, or provide summary of locked shut test results, margin test results, electrical schematics, electrical redundancy tests, pyrotechnic system test (from input stimuli to end function) results, etc.

7.0 CAUSE: Improper assembly/workmanship and cleanliness.
7.1 CONTROL: Describe measures taken to assure proper assembly and workmanship. Refer to attached supporting data I.
7.1.1 VERIFICATION: Provide summary of document that shows hardware was built in accordance with approved drawings and assembled per approved procedures.
7.1.2 VERIFICATION: Provide summary of acceptance test report.
7.2 CONTROL: Ensure proper level of cleanliness to prevent debris or contamination from entering moving parts.
7.2.1 VERIFICATION: Provide summary of cleanliness plan. Specify inspection requirement that ensures compliance with cleanliness plan.

8.0 CAUSE: Improper sequencing or procedural errors.
8.1 CONTROL: Describe provisions which preclude sequencing failures or which make mechanical system insensitive to sequencing failures.
8.1.1 VERIFICATION: Provide summary of sequencing test reports and/or input-stimuli-to-end-function test reports.
8.1.2 VERIFICATION: Refer to appropriate PIP annex containing procedures that ensure proper sequencing.

ATTACHED SUPPORTING DATA

A. Detailed drawings and schematics of mechanical and control system.
B. Summary/conclusions of binding analysis, as appropriate.
C. Summary of development and qualification test conditions and results.
D. Summary of materials compatibility review.
E. Derivations of margins against inadvertent operations.
F. Illustration of critical design features and provide summary of NSTS 08060 test results.
G. Logic chart showing failure paths for a given hazardous event to occur. Specify crew indications available at each step.
H. Electrical schematic identifying inhibits/controls or fault tolerance of control circuit.
I. Tabular listing and accompanying summary of all mandatory inspection points.

HR GUIDELINE

HR NUMBER: **GHR-22**

TITLE: **Collision/Impact During Planned Deployment**

SUBSYSTEM: Structural, Mechanisms

HAZARD GROUP: Collision

DESCRIPTION OF HAZARD

Address the potentially hazardous function of deploying the payload from the orbiter bay where collision damage could occur. Address clearances within the payload, between the payload and other payloads, and between the payload and the orbiter. Coordinate with JSC experts.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 201.3, 202.3, 203

HAZARD CATEGORY

X CATASTROPHIC
X CRITICAL

Impact of a payload with the orbiter can damage the payload bay doors, aerosurfaces, structures, etc., leading to inability of the orbiter to return. Additionally contact can lead to explosive energy release should a pressure vessel or other energy storage device be damaged.

HAZARD CAUSES

1. Variations of parameters affecting deployment dynamics (e.g., mechanism used for guiding path, springs, spinning stages, etc.)
2. Inadvertent momentum change (reaction wheel spin-up, etc.) due to electrical component failures
3. Inadvertent momentum change (reaction wheel spin-up, etc.) due to mechanism failures

The causes deal primarily with the improper energy exchange during payload deployment. A nominal variation of deployment parameters are typically established and any failure or fault that can cause an exceedence of those parameters should be addressed. Discuss/coordinate with JSC experts.

ADDRESSING THE HAZARD

1.0 CAUSE: Variations of parameters affecting deployment dynamics (e.g., mechanism used for guiding path, springs, spinning stages, etc.)

1.1 CONTROL: Specify deployment functional design criteria. Include pertinent variables, parameters and tolerances (including fault tolerance) that may effect the separation functions (see below). Refer to attached supporting data A and C.

Spacecraft and ASE:
Umbilical/connector pull drag
Spring constant and/or stroke variation/performance dispersion
Spring failure.
Spring misalignment
Mass property variations
Inter-axis coupling - products of inertia
SC attitude and attitude rates

Electroexplosive device time delay (does not cover synchronization of pyrotechnic or release deployment angle error)
Separation induced shock or impulse loads
SC-ASE interface residue strain energy transfer
Friction in ejection system and between ejection system and detached body
Free play in retention system
Payload flexible body dynamics
Spacecraft geometric reconfiguration

Orbiter:
Orbiter attitude and attitude rates (PRCS and VRCS rates)
RCS jet firings (plume impingement and induced attitude rates)
VRCS failed off
Thermal bowing
Orbiter flexible body dynamics

1.1.1 VERIFICATION: Provide closest approach (i.e., clearances) for worst case separation conditions. Refer to deployment analyses and tests.

2.0 CAUSE: Inadvertent momentum change (reaction wheel spin-up, etc.) due to electrical component failures
2.1 CONTROL: Establish by analysis the affect of a momentum change and establish the hazard potential. Summarize the analysis and results. Specify failure tolerance of the electrical controls. Describe how this failure tolerance is obtained and the independence of the inhibits. Refer to attached supporting data B.
2.1.1 VERIFICATION: Refer to analyses and tests. Summarize the analysis that verifies fault tolerance of the control system. Specify how the analysis was performed to the level needed to establish the independence of the inhibits (if applicable). Include effects of low voltage on digital logic circuitry.

3.0 CAUSE: Inadvertent momentum change (reaction wheel spin-up, etc.) due to mechanism failures
3.1 CONTROL: Refer to the safety critical mechanism functional failure HR.
3.1.1 VERIFICATION: Refer to the safety critical mechanism functional failure HR.

ATTACHED SUPPORTING DATA

A. Summary of parameter analysis including assumptions, parameters and variation of these parameters considered and results of analysis in terms of clearances, relative velocities, pitch/roll rates, etc. Summary of test results showing, in particular, the correlation with analytical results.
B. Diagram detailing the electronic control paths, monitoring, and required failure tolerance.
C. Summaries of procedures and drawings showing monitoring circuits and re-safing controls.

HR GUIDELINE

HR NUMBER: **GHR-23**

TITLE: **Premature/Inadvertent Pyrotechnic Device Operation**

SUBSYSTEM: Electrical, Pyrotechnic

HAZARD GROUP: Collision, Contamination

DESCRIPTION OF HAZARD

Pyrotechnic devices are used in space systems to control a variety of operations including jettison/deployment, solid rocket motor firing, and valve operation. Each of these operations presents unique hazards to the orbiter and crew. The description of hazard should reflect those inadvertent actions due to pyrotechnic operations.

NOTE: This hazard may be addressed in a unique HR or combined with other HR guidelines to develop a single HR to address all aspects of a given hazard.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 201.3, 210, 210.1, 210.2c, 210.3, 215.2

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

HAZARD CAUSES

1. Electrical firing circuit fault/inadvertent electrical activation
2. Thermal extremes
3. Electrostatic discharge
4. RF radiation
5. Shock (impulsive) load and vibration induced ignition (non-NSI's)
6. Improper design/workmanship error

The causes fall into two fundamental groups, inadvertent fire commanding and environmental influences causing ignition of pyrotechnic material.

ADDRESSING THE HAZARD

1.0 CAUSE: Electrical firing circuit fault/inadvertent electrical activation

1.1 CONTROL: Describe pyrotechnic firing circuit and demonstrate that the circuit possesses the necessary fault tolerance to inadvertent firing (two-fault tolerance for a catastrophic hazard, one fault tolerance for critical). Indicate inhibit(s) located in the ground/return leg of the circuit. Describe monitoring available for inhibits. Address compliance with NSTS 18798, letter EP5-88-L278 in regards to design and testing per MIL-STD-1512 and/or MIL-STD-1576. Refer to attached supporting data C.

1.1.1 VERIFICATION: Refer to analysis which establishes the system fault tolerance. Summarize any testing conducted to establish system fidelity.

1.2 CONTROL: Describe mission configurations/time line when the firing of the pyrotechnic is considered safe.

1.2.1 VERIFICATION: Refer to analyses and tests that substantiate the safe to fire times/configurations for the pyrotechnic device(s).

1.3 CONTROL: Summarize how the monitoring system for inhibits is designed, specifically addressing the possibility for monitoring current activating the pyrotechnic device.
1.3.1 VERIFICATION: Refer to analysis which assesses the monitoring system's capability to monitor, without faults (or nominal operation) inducing pyrotechnic firing. Summarize any testing conducted to establish system fidelity.

2.0 CAUSE: Thermal extremes
2.1 CONTROL: Summarize the thermal environments that the pyrotechnic device may experience and the qualification limits of the pyrotechnic device. Demonstrate adequate margin.
2.1.1 VERIFICATION: Refer to thermal testing of pyrotechnic devices. Refer to thermal analysis

3.0 CAUSE: Electrostatic discharge
3.1 CONTROL: If pyrotechnic devices other than NSI's are used summarized compliance with MIL-STD-1512 and/or MIL-STD-1576 for electrostatic discharge testing.
3.1.1 VERIFICATION: Refer to electrostatic test reports for pyrotechnics utilized. Refer to pyrotechnic tracking logs which ensures that only fully qualified pyrotechnics are used. Refer to inspections of as built hardware to verify installation of qualified pyrotechnics.
3.2 CONTROL: If NSI's are used indicate the part number, lot number and serial number.
3.2.1 VERIFICATION: Refer to inspections to be conducted that will verify that initiators that are installed are qualified and properly tracked.

4.0 CAUSE: RF radiation
4.1 CONTROL: (For non-NSI's) Summarize the design feature of the pyrotechnic firing circuit and device that preclude sensitivity to RF radiation.
4.1.1 VERIFICATION: Refer to the analysis of the system and pyrotechnic design that prove margin against no-fire levels of initiators.
4.2 CONTROL: Summarize the test results and testing criteria of pyrotechnic devices to assess susceptibility to RF radiation.
4.2.1 VERIFICATION: Refer to tests and analyses for RF susceptibility.

5.0 CAUSE: Shock (impulsive) load and vibration induced ignition (non-NSI's)
5.1 CONTROL: Summarize limits to which pyrotechnic device is qualified for shock loads. Compare to anticipated worst case mission loadings. Demonstrate adequate margin.
5.1.1 VERIFICATION: Refer to tests and analyses.

6.0 CAUSE: Improper design/workmanship error
6.1 CONTROL: If the pyrotechnic device is an NSI indicate this and refer to attached supporting data A.
6.1.1 VERIFICATION: Refer to inspection to verify NSI installed.
6.2 CONTROL: Summarize design and testing program for non-NSI's. Refer to device specifications and construction details. Refer to attached supporting data B.
6.2.1 VERIFICATION: Summarize testing and analysis used for qualification (not already listed in previous controls and verifications.)

ATTACHED SUPPORTING DATA

A. Provide a listing of all pyrotechnic devices, their function, part number, lot number, and serial number.
B. For non-NSI pyrotechnic device provide drawings and diagrams that indicate the construction of the device (e.g., cutaway drawings.)
C. Provide schematics indicating inhibits, control and monitors in the pyrotechnic firing chain.

HR GUIDELINE

HR NUMBER: **GHR-24**

TITLE: **Must Work Pyrotechnics/Debris Generation**

SUBSYSTEM: As Applicable

HAZARD GROUP: As Applicable

DESCRIPTION OF HAZARD

Failure of a pyrotechnic device used in a must work function (e.g., Super*zip fails to deploy a payload and prevents the PLBD's from closing) or debris generation during operation of pyrotechnic devices.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 210.2a, 210.2b, 210.3

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

NOTE: The hazard potential of a pyrotechnic device will be considered catastrophic until proven otherwise.

HAZARD CAUSES

1. Pyrotechnic device fails to properly function
2. Debris generation

ADDRESSING THE HAZARD

1.0 CAUSE: Pyrotechnic device fails to properly function.
1.1 CONTROL: Indicate proper design and use of pyrotechnic devices that meet the qualification and acceptance testing requirements of NSTS 08060. Summarize compliance to NSTS 08060. Refer to attached supporting data A.
1.1.1 VERIFICATION: Summary of test and analysis, refer to the applicable documentation. Assembly procedures.

NOTE: Submittal of detailed drawings, qualification test procedures, acceptance test procedures, assembly procedures, and performance of test in accordance with NSTS 08060 are required. Tests required for qualification include exposure to planned SSP environments, verification of all redundant pyrotechnic devices, autoignition, drop test, overload and underload tests, locked shut tests, RF susceptibility test or analysis, and structural margin tests. Acceptance tests include firing 10% of lot, verification of margin where applicable (cartridge loaded with 85% by weight of minimum charge), ESD susceptibility, leakage integrity, insulation resistance, N-ray and X-ray, propellant weight records, and receiving inspection of piece parts.

1.2 CONTROL: If the pyrotechnic device is used in a redundant application where the hazard is being controlled by the use of multiple independent methods besides the primary pyrotechnic device, then either demonstrate compliance with criteria equivalent to NSTS 08060, or sufficient margin/redundance to assure safe operation must be documented.
1.2.1 VERIFICATION: Provide summary of applicable analysis and/or test to ensure redundance or margin exists for the must work function/hazard control.

1.3 CONTROL: Include a summary of the lot acceptance data package as defined in NSTS 08060 which includes the following:

- Certified acceptance reports including the date of manufacture of the devices (and the NSI installed) and the lot number(s) of the explosive material(s) utilized.
- Certified list of all piece parts by drawing revision number and receiving inspection records. Total lot quantities and/or serial numbers to provide lot production/rejection traceability.
- Documented final inspection records including X-ray negatives and N-ray negatives of each part in the lot if required by the procurement specification. Copies of the N-ray and X-ray certifications prepared by the performing vendor listing serial numbers of parts radiographed.
- Lot acceptance firing data or other performance parameters which may include pressure/time traces with tabulated values, detonation velocity, delay time, or dent block testing.
- When the device must fracture in a controlled manner (e.g., Superzip*), the capability to withstand loads generated by the pyrotechnics, material tensile strength test results, and proof pressure test results, with the performing vendor's certification, must show proper material selection/design.
- Certificates of charge formula is the same as that used for manufacture of the qualification lot.
- Lot certification of the NSI lot used and a list of serial numbers of devices in the lot with each mating NSI. Shipping data on the NSI used in device manufacture.
- Weight data for each device in accordance with paragraph 3.11 of NSTS 08060.
- Copies of all nondestructive lot acceptance test data which show leak test information, bridge wire resistance reading, and any other applicable information.
- Copies of all failure and corrective action records including MRB waivers/deviations. Include copies of all descriptive information such as discrepancy reports, squawk sheets, material review records, rejection reports, etc., pertaining to discrepant hardware for the subject lot review. This information shall include all reports covering discrepancies from receiving inspection records for piece parts inclusive to end item testing prior to shipment.
- The explosive classification for the device from the U. S. Department of Transportation. A copy of each such classification shall be furnished to the appropriate element contractor, the NASA project office, or the integrating contractor.
- The Component Authority Approval letter for that device from the U. S. Department of Transportation. A copy of each letter, as it applies, shall be furnished to the appropriate element contractor, the NASA project office, or the integrating contractor.
- The Material Safety Data Sheet on the current OSHA form designated for the device being presented for certification. A copy of each such data sheet shall be furnished to the appropriate element contractor, the NASA project office, or the integrating contractor.
- Lot certificate, receiving inspection records of piece parts, and vendor certification records pertaining to material traceability from raw stock.
- Provide the documentation to show the acceptance by JSC pyrotechnic experts for the lot acceptance data package.

1.3.1 VERIFICATION: Provide documentation of final approval of lot in accordance with NSTS 08060 paragraph 5.4.3.

1.4 CONTROL: Identify any limited life items of the pyrotechnic devices and show that the limited-life restrictions are not violated.

1.4.1 VERIFICATION: Documentation to show that limited life items are not used outside of their qualification or certification.

1.5 CONTROL: Summarize any thermal constraints for the proper operation of the pyrotechnic device. Describe the thermal control or operational restrictions for the operations. Refer to attached supporting data G.

1.5.1 VERIFICATION: Test/analysis that determined the pyrotechnic device thermal limits. Show how these limits will not be exceeded (e.g., flight rules, PIP, heaters, etc.).

2.0 CAUSE: Debris generated due to pyrotechnic operation.

2.1 CONTROL: Identify the use of pyrotechnics that meet the requirements of NSTS 08060. Summarize qualification data demonstrating that the devices have been subjected to a locked shut test and have experienced overload testing (115%). Substantiate that each pressure containing device (flight article) has been proof pressured tested. Refer to attached supporting data B, C, D, and E.

2.1.1 VERIFICATION: Lot acceptance test/procedure, proof pressure and lock shut test results.

ATTACHED SUPPORTING DATA

A. Detailed drawing of device
B. Lot and part number with acceptance test results
C. Margin test results (85% and 115%)
D. Proof pressure test results of flight articles
E. Any non-destructive test results
F. Chemical composition of any booster charge in device
G. Test and/or analysis to show thermal limits of the pyrotechnic devices

HR GUIDELINE

HR NUMBER: **GHR-25**

TITLE: **Collision Following Premature/Inadvertent Appendage Deployment or Payload Release/Deployment**

SUBSYSTEM: Mechanical

HAZARD GROUP: Collision

DESCRIPTION OF HAZARD

Collision of the payload with the orbiter or other payloads from the inadvertent release of a mechanism.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 200.4a, 201.3, 202.3, 203, 208.1, 208.2, 208.3, 213.
NSTS 18798, letter TA-94-041

HAZARD CATEGORY

X CATASTROPHIC
X CRITICAL

The worst-case hazard is impact with the orbiter or payload hardware. This impact could lead to loss of crew-habitable environment or damage to the orbiter preventing payload bay door closure.

HAZARD CAUSES

1. Electrical system design errors or electrical system failures.
2. Environmental effects cause inadvertent mechanism operation.
3. Structural failure of mechanical components.
4. Improper assembly/workmanship (on ground or on orbit).

ADDRESSING THE HAZARD

1.0 CAUSE: Electrical system design errors or electrical system failures.
1.1 CONTROL: Specify the number and list the electrical inhibits that prevent occurrence of the hazard. Describe each control for each inhibit and establish its independence. Indicate how each inhibit is monitored. Describe ground/return leg inhibit and any RF commanding and encryption implemented. Define the fault tolerance of the system electrical inhibits including orbiter interfaces. Refer to attached supporting data A and B.
1.1.1 VERIFICATION: Refer to and summarize the documentation that verifies that the electrical system is built to approved drawing specifications.
1.1.2 VERIFICATION: Refer to and summarize procedures/methods used to verify that the electrical inhibits are in the proper position when operation of the mechanism is a hazard. Refer to PIP annex.
1.1.3 VERIFICATION: Provide summary of analyses and/or tests performed to demonstrate design compliance with appropriate safety requirements. Refer to attached supporting data C.

2.0 CAUSE: Environmental effects cause inadvertent mechanism operation.
2.1 CONTROL: Describe design features and safety margins that preclude inadvertent mechanism operation. Explain any environmental design drivers.
2.1.1 VERIFICATION: Provide summary of analyses and/or tests performed that show that the mechanisms are designed for the expected environment. Refer to attached supporting data D.

2.2 CONTROL: Describe monitors/indications provided that demonstrate that the mechanical system is in its proper load carrying configuration.

2.2.1 VERIFICATION: Summarize the methods used to verify that the mechanical components are in the proper load carrying position. Refer to the ground procedure and PIP annex. (When no indication is available to verify proper position, identify as mandatory inspection point.)

3.0 CAUSE: Structural failure of mechanical components.
Refer to structural HR.

4.0 CAUSE: Improper assembly/workmanship.

4.1 CONTROL: Build per approved design/procedures to assure proper assembly and workmanship.

4.1.1 VERIFICATION: Summarize inspection procedures to assure that the mechanism was built in accordance with the approved drawings and assembled per approved procedures.

4.1.2 VERIFICATION: Refer to and summarize acceptance test report.

ATTACHED SUPPORTING DATA

A. Submit schematics showing all power sources, electrical inhibits, inhibit controls (including orbiter wiring and GSE interfaces), monitors, etc.
B. Develop a flight closeout table listing all inhibits, when they were last cycled, what their final states were, and how that state was confirmed.
C. Summary of electrical system tests/analyses.
D. Summary of mechanical system tests/analyses.

HR GUIDELINE

HR NUMBER: **GHR-26**

TITLE: **Premature/Inadvertent Liquid Engine or Attitude Control System Operation**

SUBSYSTEM: Propulsion, Propellants

HAZARD GROUP: Fire, Collision

DESCRIPTION OF HAZARD

The inadvertent operation of payload liquid (or gaseous) propellant delivery systems could damage the orbiter or injure the flight crew by engine plume effects, thrust (collision) effects, thermal loading or release of hazardous propellants or propellant by-products contaminating the orbiter payload bay. This hazard should be addressed for all orbiter mission phases through achieving a safe separation distance and/or through landing.

NOTE: This HR guideline deals with inadvertent thruster or engine operation, not rupture or explosion of the propulsion system. The safe distance curves relate only to thrust generation, not rupture or explosion. There is not a distance that is considered safe for an explosion in orbit.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 201.1d, 201.3, 202.2

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

The worst case effect of this hazard is the loss of the orbiter and crew. This hazard is categorized catastrophic.

HAZARD CAUSES

1. Mechanical component failures
2. Electrical component failures

The causes to be addressed within this HR are those that will lead to inadvertent firing. The flow of propellant is inhibited by the mechanical flow control devices (i.e., valves). A failure within the valves will allow propellant to flow, thus generating thrust. A failure in the control electronics can command the valves open, generating thrust. The payload design must be assessed to determine the specific failures to which the payload is susceptible.

ADDRESSING THE HAZARD

1.0 CAUSE: Mechanical component failures
1.1 CONTROL: List and describe the mechanical devices that interrupt (inhibit) the propellant flow path(s) to the engine(s). Detail propellant quantity per isolated line segment. Establish compatibility of the flow control devices with SSP and payload induced/design environments and loads. Refer to attached supporting data A.
1.1.1 VERIFICATION: Design must be verified to be built to the specifications described in the control. Tests should be conducted to assure functionality.

1.1.2 VERIFICATION: Tests and analyses will have to be conducted to establish the compatibility with the SSP and payload induced/design environments and loads. Refer to applicable qualification procedures and reports.
1.2 CONTROL: Establish the state of propellant flow control devices at launch and subsequent mission phases. Refer to attached supporting data B.
1.2.1 VERIFICATION: Describe the process used to verify position of the flow control devices prior to launch.
1.3 CONTROL: Clarify the number and type of seals or seats for each propellant flow control device. Refer to attached supporting data C.
1.3.1 VERIFICATION: The design must be verified as to the number and qualification of the seals.
1.4 CONTROL: Specify the state that propellant flow control devices assume upon loss of command signal or power (e.g., open, closed, as-is). Establish what state the propellant flow control devices assume upon application of power or command signal.
1.4.1 VERIFICATION: Testing and analysis must verify/establish the state of devices upon failing and/or re-establishment of power and/or command.

NOTE: It is crucial that removal of inhibits and opening of flow control devices be correlated to an operational time line, and that the controls be in place while a hazard potential exists for the orbiter. Early removal of inhibits leads to insufficient fault tolerance.

2.0 CAUSE: Electrical component failures
2.1 CONTROL: Specify each of the independent electrical inhibits that control each of the mechanical inhibits. Describe the controls for each electrical inhibit and establish its independence. Indicate how each inhibit (electrical/mechanical) can be monitored. Indicate those inhibits that are operated by RF and whether the RF links are encrypted. Indicate any orbiter services or hardware used in establishing fault tolerance. Refer to attached supporting data A and D.
2.1.1 VERIFICATION: Specify how it is verified that the inhibits and controls will withstand SSP environments. Summarize the process for verifying that the inhibits are in place prior to launch. Refer to qualification procedures and reports.
2.1.2 VERIFICATION: Specify the procedures which confirm proper state of inhibits and controls prior to launch. Refer to procedure identifications.
2.2 CONTROL: Summarize the fault tolerance of the system electrical inhibits considering failures in the inhibit control systems (e.g., low voltage effects on circuitry and voltage transients) which may remove more than one inhibit. Compliance with pyrotechnic requirements for any pyrotechnically actuated flow control devices can either be documented in another HR or included here. Refer to attached supporting data A.
2.2.1 VERIFICATION: Specify the analysis that verifies fault tolerance of the control system. Analyses and/or tests should include effects of low voltage and voltage transients on circuitry. Summarize how the analysis and/or test was performed to substantiate inhibit independence.
2.3 CONTROL: Define the safe separation distance for removal of inhibits to engine firing and identify when and how each inhibit will be removed. Refer to the safe distance analysis.
2.3.1 VERIFICATION: Specify the analysis for determining the safe separation distance. Specify procedures for confirming timer settings and operating or locking out commands initiation until safe distance is achieved.

NOTE: Safe distance from the orbiter should be established by using the maximum thrust possible along a single axis (this axis may not necessarily be planned to be directed to the orbiter). All thrusters that can be positively summed to that axis should be used in calculation of the thrust potential. Once the thrust potential is established the safe distance chart of NSTS 18798, letter TA-89-009 is applicable.

ATTACHED SUPPORTING DATA

A. Schematic(s) of propellant flow control system including flow control devices, inhibits, controls and monitors. Inhibits and controls should be marked and numbered to indicate proper number of inhibits in place.
B. Table listing each flow control device detailing when last cycled or tested and how the closure was verified.
C. Schematic/cutaway diagram of each flow control device showing sealing surfaces and operation.
D. Table listing each electrical inhibit and controls, indicating when last cycled and how the final position is verified.
E. Summary of derivation of maximum thrust and safe distance.

HR GUIDELINE

HR NUMBER: **GHR-27**

TITLE: **Premature/Inadvertent Solid Rocket Motor Firing**

SUBSYSTEM: Propulsion, Propellants

HAZARD GROUP: Fire, Collision

DESCRIPTION OF HAZARD

The inadvertent ignition or explosion of a payload SRM could damage the orbiter or injure the crew by engine plume effects, energy release, recontact or thrust (collision) effects. It applies to all phases from integration of the components bearing solid propellant into the orbiter at the launch site through achieving a safe distance from the orbiter (or through de-integration upon contingency return).

NOTE: In regards to explosion of a SRM the safe distance criteria does not apply as there is no distance that is considered safe for an explosion on-orbit.

SAFETY REQUIREMENTS TO SATISFY

NSTS 1700.7, 200.3, 200.4a, 201.1d, 201.3, 202.1, 210

HAZARD CATEGORY

X CATASTROPHIC
CRITICAL

Ignition of a SRM while in the payload bay or in the proximity of the orbiter can result in loss of orbiter due to plume damage, thermal loads, overturning moments and contamination. This hazard would be immediately catastrophic to the orbiter and crew.

HAZARD CAUSES

1. Electrical component failures.
2. EMI/EMC (including EMI/EMC caused by rotating the S&A device).
3. Propellant sensitivity to induced environments (e.g., thermal, impact, vibration, shock...)
4. Electrostatic discharge.

All causes that can lead to unplanned ignition of the solid rocket propellant must be addressed. This includes the nominal ignition path and the environmental effects upon the propellant and the pyrotechnic chain. Electrical failures that can lead to inadvertent commanding/firing of the initiators and/or rotating the safe and arm device must be addressed.

ADDRESSING THE HAZARD

1.0 CAUSE: Electrical component failures

1.1 CONTROL: Specify the number and list the electrical inhibits that prevent occurrence of the hazard. Describe each control for each inhibit and establish its independence. Indicate how each inhibit is monitored. Describe ground/return leg inhibit and any RF commanding and encryption implemented. Define the fault tolerance of the system electrical inhibits including orbiter interfaces. Refer to attached supporting data A and B.

1.1.1 VERIFICATION: Specify how it was verified that the electrical inhibit and control components can withstand the expected shuttle and payload induced environments. Refer to applicable qualification procedures and reports.

1.1.2 VERIFICATION: Specify what method is to be used to verify that the electrical inhibits are in the proper position prior to launch.
1.1.3 VERIFICATION: Summarize the analysis that substantiates fault tolerance. Tests/analyses should include effects of low voltage and transient voltages on control circuitry. Summarize how the test/analysis was performed to substantiate inhibit independence.
1.2 CONTROL: Indicate the type of S&A device used and document compliance with MIL-STD-1576. Indicate when the S&A device is rotated. If the S&A is to be rotated to arm prior to the payload reaching a safe distance from the orbiter, provide specific time lines and describe specifics of monitoring that will be available just prior to rotation through deployment. Refer to attached supporting data F.
1.2.1 VERIFICATION: Review of drawings to assure proper installation. Tests should be conducted to assure functionality.
1.2.2 VERIFICATION: Refer to PIP or PIP annex for procedural requirement for S&A rotation.
1.2.3 VERIFICATION: Tests/analyses verifying S&A compliance.
1.3 CONTROL: Define the separation velocity and identify when each inhibit will be removed. Refer to the applicable released drawings and sequence of events.
1.3.1 VERIFICATION: Summarization of separation analysis verifying separation rates.

NOTE: It is crucial that removal of inhibits be correlated to an operational time line, and that the inhibits be in place while a hazard potential exists for the orbiter. Early removal of inhibits leads to insufficient fault tolerance.

2.0 CAUSE: EMI/EMC/RF (including EMI/EMC caused by rotating the S&A device)
2.1 CONTROL: Specify shielding configurations for RF/EMI attenuation (e.g., twisted/braided, etc.). List potential shielding gaps. Refer to attached supporting data C.
2.1.1 VERIFICATION: Summarize and refer to the analysis and/or test results (include dB margins).

3.0 CAUSE: Propellant sensitivity to induced environments
3.1 CONTROL: Identify environments that can cause propellant ignition and define the margins that exist. (e.g., shock exposure from launch, landing, on-orbit, thermal limits, etc.)
3.1.1 VERIFICATION: Specify verification approach and results of tests/analyses. Refer to applicable documents.

NOTE: A thermal analysis shall be provided with maximum and minimum temperatures and duration of exposure. Cook-off and auto-ignition must be evaluated for the high temperature conditions for the specific motor and mission. In extreme low temperature, propellant and propellant/case bond structural integrity shall be verified by testing and analysis. Grain cracking or case bond separation of any size is not permitted.

4.0 CAUSE: Electrostatic discharge
4.1 CONTROL: Specify initiators used and document compliance with MIL-STD-1512. List lot acceptance criteria. If NSI's are used, state so and refer to. For all other pyrotechnic initiators, refer to the design and test document used. Determine if the special test requirements of NSTS 1700.7, paragraph 210.1 are applicable, and if so, document and refer to compliance efforts. Refer to attached supporting data D and E.
4.1.1 VERIFICATION: Describe how it is verified that firing squibs are free from static effects. Summarize and refer to test results.
4.2 CONTROL: Describe how the circuits, MLI, motor cases etc. are grounded and list any special components used (e.g., static bleed resistors, etc.).
4.2.1 VERIFICATION: Review of design/drawings. Inspection for proper installation. Tests should be conducted to assure functionality.
4.3 CONTROL: All non-metallic motor cases shall have a conductive coating applied if the volume resistivity of the case is 10^8 ohm - meter or greater. All parts of the motor must be at the same voltage. After application of the conductive coating, the case must be electrically connected to the adapter and grounded to the orbiter. The system shall remain grounded until the payload is deployed from the orbiter.

4.3.1 VERIFICATION: Verification matrix providing resistivity measurements of the case and grounding integrity.

NOTE: Provide description of case and insulator materials. Under extreme environmental conditions, ESD events, or fragment attack, the case can be as important as the propellant properties.

ATTACHED SUPPORTING DATA

A. Schematic (including orbiter circuitry) showing electrical inhibits, controls and monitors. Schematic should clearly demonstrate independence of inhibits. Circle and number the inhibits. The schematic should identify:
    a. Power sources.
    b. Inhibits (identifying the component that acts as the inhibit).
    c. Monitors for the inhibits and location of status displays.
    d. Inhibit control command sources.
    e. Static control devices (bleed resistor, etc.)
B. Table listing the inhibits, when they were last cycled (actuated), and the final prelaunch state.
C. Drawings/schematics of EMI/EMC suppression devices. Summary of EMI field strength/compatibility analysis.
D. Cutaway diagram of initiator.
E. Table listing flight initiators tested and results, include the model numbers, lot numbers and serial numbers.
F. Provide a diagram of the safe and arm device. Diagram should clearly indicate the design and operation.
G. Provide at phase II:
    Motor manufacture
    Total mass of propellant
    Type of propellant
    Propellant formulation/ingredients
    Motor/propellant explosive classification
    Case description

4.0 KEY DOCUMENT REFERENCES

1. NSTS 1700.7, "Safety Policy and Requirements for Payloads Using the Space Transportation System"*
2. NSTS 13830, "Implementation Procedure for NSTS Payloads System Safety Requirements"*
3. NSTS 18798, "Interpretations of NSTS Payload Safety Requirements"*
4. NSTS 22648, "Flammability Configuration Analysis for Spacecraft Applications"*
5. NSTS 07700, Volume XIV, "Space Shuttle System Payload Accommodations"*
6. NSTS 08060, "Space Shuttle System Pyrotechnic Specification"*
7. NSTS 16979, "Shuttle Orbiter Failure Modes and Fault Tolerances for Interface Services"*
8. NSTS 20793, "Manned Space Vehicle, Battery Safety Handbook"*
9. NSTS 14046, "Payload Verification Requirements"*
10. MSFC-HDBK-527/JSC 09604, "Materials Selection List for Space Hardware Systems"*
11. 45SPW HB S-100/KHB 1700.7, "Space Shuttle Payload Ground Safety Handbook"*
12. MSFC-SPEC-522, "Design Criteria for Controlling Stress Corrosion Cracking"*
13. NHB 8071.1, "Fracture Control Requirements for Payloads Using the NSTS"*
14. NHB 8060.1, "Flammability, Odor, Offgassing and Compatibility Requirements and Test Procedures for Materials in Environments that Support Combustion"*
15. NASA-STD-3000, Volume 1, "Man-Systems Integration Standards"*
16. JSC-20483, "Human Research Policy and Procedures for Space Flight and Related Investigations"*
17. JSC 25863, "Fracture Control Plan for JSC Flight Hardware"*
18. MIL-STD-1522, "Standard General Requirement for Safe Design and Operation of Pressurized Missile and Space Systems"*
19. MIL-STD-1512, "Electroexplosive Subsystems, Electrically Initiated, Design Requirements and Test Methods"*
20. MIL-STD-1576, "Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems"*
21. ANSI-Z-136.1, "American National Standard for Safe Use of Lasers"*

* Note: All documents referred to are latest revision.

APPENDIX A: ACRONYMS AND ABBREVIATIONS

AC	Alternating Current
ACD	Adiabatic Compression Detonation
AI	Action Item
ANSI	American National Standards Institute
ASE	Airborne Support Equipment
CDMS	Command and Data Management System
dB	Decibel
DC	Direct Current
DOT	Department of Transportation
DR	Discrepancy Report
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMU	Extravehicular Mobility Unit
EPDS	Electrical Power and Distribution System
ESD	Electrostatic Discharge
EVA	Extravehicular Activity
FCP	Fracture Control Plan
FCSR	Fracture Control Summary Report
FOS	Factor of Safety
GFE	Government Furnished Equipment
GHR	Guideline Hazard Report
GN&C	Guidance, Navigation and Control
GSE	Ground Support Equipment
HB	Handbook
HDBK	Handbook
HR	Hazard Report
HRPPC	Human Research Policy and Procedures Committee
HV	High Voltage
ICD	Interface Control Document
IDD	Interface Definition Document
IVA	Intravehicular Activity
JSC	Johnson Space Center
KHB	Kennedy Space Center Handbook
LASER	Light Amplification by Stimulated Emission of Radiation
LBB	Leak Before Burst
M&P	Materials and Processes
MAPTIS	Materials and Processes Technical Information System
MDK	Middeck
MDP	Maximum Design Pressure
MLI	Multi-Layer Insulation
MPE	Maximum Permissible Exposure
MRB	Materials Review Board
MSFC	Marshall Space Flight Center
MUA	Material Usage Agreement
N-ray	Neutron Radiation
NCR	Noncompliance Report
NDE	Non-Destructive Examination
NDI	Non-Destructive Inspection
NHB	NASA Handbook
NSI	NASA Standard Initiator
NSTS	National Space Transportation System
OSHA	Occupational Safety and Health Act
PGSC	Payload General Support Computer
PIP	Payload Integration Plan

P/L	Payload
PLB	Payload Bay
PLBD	Payload Bay Door
POCC	Payload Operations Control Center
PRCS	Primary Reaction Control System
PSDP	Payload (Flight) Safety Data Package
psid	Pounds per Square Inch Differential
PSRP	Payload Safety Review Panel
RCP	Radiation Contraints Panel
RCS	Reaction Control System
RF	Radio Frequency
RMS	Remote Manipulator System
S&A	Safe and Arm
SC	Spacecraft
SCC	Stress Corrosion Cracking
SH	Spacehab
SL	Spacelab
SPAH	Spacelab Payload Accommodation Handbook
SRM	Solid Rocket Motor
SSP	Space Shuttle Program
STD	Standard
STS	Space Transportation System
VRCS	Vernier Reaction Control System