



National Aeronautics and  
Space Administration

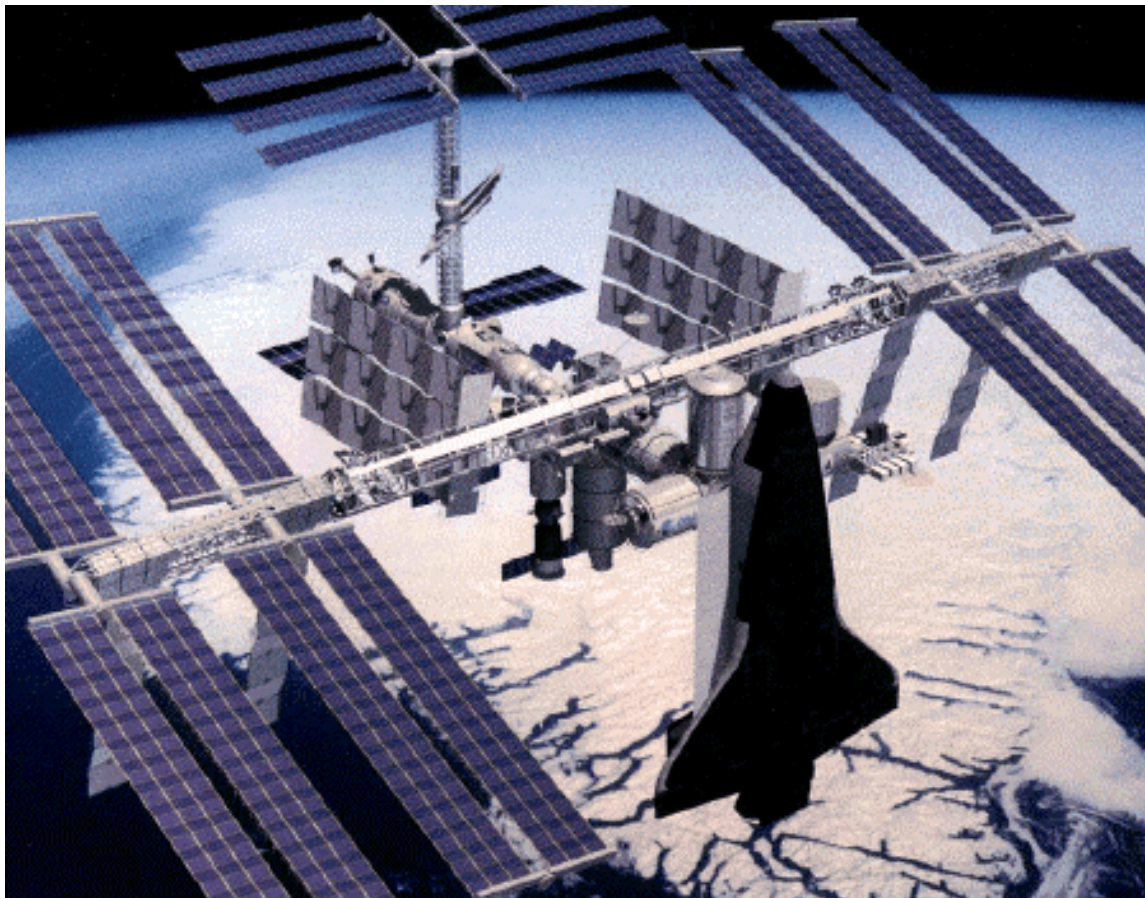
NSTS/ISS 18798  
Revision B

**September 1997**

---

# **Interpretations of NSTS/ISS Payload Safety Requirements**

(Previously Titled NSTS 18798A)



**Lyndon B. Johnson Space Center**  
Houston, Texas 77058

## **NOTE: THE STATEMENT BELOW IS FOR ELECTRONIC USE OF THIS DOCUMENT**

**For ease of finding related documentation letters, the “Bookmark” capability has been implemented. Please use the following process:**

- 1. On the Menu Bar, click on Edit, then click on Bookmark**
- 2. A Pull down menu with Bookmark Name will appear**
- 3. Type in related Topical Division (i.e., Crew IVA, Electrical, Pressure, etc.)**
- 4. Highlight the appropriate topical area in the pull down menu, then click on “Go To”**

## **PREFACE**

In implementing the payload safety review process, the Payload Safety Review Panel (PSRP) has been required to make interpretations of particular safety requirements. NSTS 18798 was issued to compile these letters into one document. The recent release of the International Space Station (ISS) Addendum to NSTS 1700.7B and other documentation changes dictate that this document be reissued and released as a joint SSP/ISS document. These letters will be utilized by the PSRP in assessing all payloads for design compliance.

This release also deletes those letters made obsolete by changes in other documentation and reflects the applicability of each letter to the SSP and ISSP as necessary. Major reductions in the number of interpretation letters were made possible by the inclusion of their contents in other program documentation (see JSC 16979, "Failure Modes and Fault Tolerance for Orbiter," and NASA-STD-5003, "Fracture Control Requirements for Payloads Using the Space Transportation System," which replaces NHB 8071.1).

This document is under joint control of both the SSP and ISSP and will be revised as necessary to reflect current interpretations of payload safety requirements. Future letters will contain an introductory paragraph clearly defining the program applicability.

NSTS/ISS 18798 supersedes NSTS 18798 Revision A and has been organized to facilitate locating information by subject matter as shown in the topical index.

### ***ORIGINAL SIGNED BY :***

Richard N. Richards  
Manager, Space Shuttle Program Integration

### ***ORIGINAL SIGNED BY :***

Jay H. Greene  
Deputy Manager, Space Station Program Office

# Topical Index

<u>Section</u>	<u>Title (JSC Letter Number)</u>	<u>Page #</u>
<b>1. CREW IVA HAZARDS-TOUCH TEMPERATURE</b>		
1.1	Thermal Limits for Intravehicular Activity (MA2-95-048)	1-1
<b>2. ELECTRICAL</b>		
2.1	Separation of Redundant Safety Critical Circuits (ET12-90-115)	2-1
2.2	Protection of Payload Electrical Power Circuits (TA-92-038)	2-3
2.3	On-Orbit Bonding and Grounding (MA2-99-142)	2-12
<b>3. FLAMMABLE ATMOSPHERE</b>		
3.1	Ignition of Flammable Payload Bay Atmosphere (NS2/81-MO82)	3-1
<b>4. PAYLOAD OPERATIONS</b>		
4.1	Monitoring for Safety (TA-88-018)	4-1
4.2	Payload Commanding-POCC (TA-91-062)	4-4
4.3	Crew Mating/Demating of Powered Connectors (MA2-99-170)	4-8
4.4	Contingency Return and Rapid Safing (MA2-96-190)	4-10
4.5	On-Orbit Maintenance (MA2-00-038)	4-13
<b>5. PRESSURE</b>		
5.1	Fault Tolerance of Systems using Specially Certified Burst Disks (TA-88-074)	5-1
5.2	Pressure Stabilized Tanks (TA-89-064)	5-3
<b>6. PYROS</b>		
6.1	Circuit Design for Payloads using Energy Storage Devices for Pyrotechnic Firing Circuits (TA-91-077)	6-1
6.2	Pyrotechnically Operated Isolation Valves for Payloads (TA-92-049)	6-3
<b>7. STRUCTURES/MATERIALS</b>		
7.1	Structural Requirements for Contingency Deorbit (NS2/90-208)	7-1
7.2	Structural Integrity Following Mechanism Failures (TA-93-037)	7-3
7.3	Mechanical Systems Safety (MA2-00-057)	7-4
7.4	Low Risk Fracture Part Clarification (MA2-96-174)	7-7

## **8. VERIFICATIONS**

- |   |     |
|---|-----|
| 8.1 Safety Policy for Detecting Payload Design Errors (TA-94-018)               | 8-1 |
| 8.2 Verification/Reverification Requirements for On-Orbit Payloads (MA2-98-135) | 8-4 |

## **9. OTHER**

- |  |     |
|--|-----|
| 9.1 Computer Control of Payload Hazards (MA2-97-083) | 9-1 |
| 9.2 Small Commonly Used Batteries (MA2-98-069)       | 9-5 |

## **APPENDIX A - Interpretation Letters Summary**

# Index

(Sorted by JSC Letter Number)

<b><u>JSC Letter # (Title)</u></b>	<b><u>Page #</u></b>
ET12-90-115 (Separation of Redundant Safety Critical Circuits)	2-1
MA2-95-048 (Thermal Limits for Intravehicular Activity)	1-1
MA2-96-174 (Low Risk Fracture Part Clarification)	7-7
MA2-96-190 (Contingency Return and Rapid Safing)	4-10
MA2-97-083 (Computer Control of Payload Hazards)	9-1
MA2-98-069 (Small Commonly Used Batteries)	9-5
MA2-98-135 (Verification/Reverification Requirements for On-Orbit Payloads)	8-4
MA2-99-142 (On-Orbit Bonding and Grounding)	2-12
MA2-99-170 (Crew Mating/Demating of Powered Connectors)	4-8
MA2-00-038 (On-Orbit Maintenance)	4-13
MA2-00-057 (Mechanical Systems Safety)	7-4
NS2/81-MO82 (Ignition of Flammable Payload Bay Atmosphere)	3-1
NS2/90-208 (Structural Requirements for Contingency Deorbit)	7-1
TA-88-018 (Monitoring for Safety)	4-1
TA-88-074 (Fault Tolerance of Systems using Specially Certified Burst Disks)	5-1
TA-89-064 (Pressure Stabilized Tanks)	5-3
TA-91-062 (Payload Commanding-POCC)	4-4
TA-91-077 (Circuit Design for Payloads using Energy Storage Devices for Pyrotechnic Firing Circuits)	6-1
TA-92-038 (Protection of Payload Electrical Power Circuits)	2-3
TA-92-049 (Pyrotechnically Operated Isolation Valves for Payloads)	6-3
TA-93-037 (Structural Integrity Following Mechanism Failures)	7-3
TA-94-018 (Safety Policy for Detecting Payload Design Errors)	8-1
TA-94-041 (Mechanical Systems Safety)	7-4

# Index

(Sorted by Title)

<b><u>Title (JSC Letter Number)</u></b>	<b><u>Page #</u></b>
Circuit Design for Payloads using Energy Storage Devices for Pyrotechnic Firing Circuits (TA-91-077)	6-1
Computer Control of Payload Hazards (MA2-97-083)	9-1
Contingency Return and Rapid Safing (MA2-96-190)	4-10
Crew Mating/Demating of Powered Connectors (MA2-99-170)	4-8
Fault Tolerance of Systems using Specially Certified Burst Disks (TA-88-074)	5-1
Ignition of Flammable Payload Bay Atmosphere (NS2/81-MO82)	3-1
Low Risk Fracture Part Clarification (MA2-96-174)	7-7
Mechanical Systems Safety (MA2-00-057)	7-4
Monitoring for Safety (TA-88-018)	4-1
On-Orbit Bonding and Grounding (MA2-99-142)	2-12
On-Orbit Maintenance (MA2-00-038)	4-13
Payload Commanding-POCC (TA-91-062)	4-4
Pressure Stabilized Tanks (TA-89-064)	5-3
Protection of Payload Electrical Power Circuits (TA-92-038)	2-3
Pyrotechnically Operated Isolation Valves for Payloads (TA-92-049)	6-3
Safety Policy for Detecting Payload Design Errors (TA-94-018)	8-1
Separation of Redundant Safety Critical Circuits (ET12-90-115)	2-1
Small Commonly Used Batteries (MA2-98-069)	9-5
Structural Integrity Following Mechanism Failures (TA-93-037)	7-3
Structural Requirements for Contingency Deorbit (NS2/90-208)	7-1
Thermal Limits for Intravehicular Activity (MA2-95-048)	1-1
Verification/Reverification Requirements for On-Orbit Payloads (MA2-98-135)	8-4

# **1. CREW IVA HAZARDS-TOUCH TEMPERATURE**

Title

JSC Letter Number

1.1 Thermal Limits for Intravehicular Activity

MA2-95-048



National Aeronautics and  
Space Administration  
**Headquarters**  
Washington, D. C. 20546-0001



Reply to Attn of :

JSC, MA2-95-048

SEP 26 1995

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration

SUBJECT: Thermal Limits for Intravehicular Activity (IVA) Touch Temperatures

The information contained in this letter is an interpretation and clarification of the payload safety requirements of NHB/NSTS 1700.7, "Safety Policy and Requirements for Payloads Using the Space Transportation System." This letter will be utilized by the Space Shuttle Payload Safety Review Panel (PSRP) in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretations of NSTS Payload Safety Requirements," as applicable against NHB 1700.7A and NSTS 1700.7B. Enclosure 1 is an updated table of contents for NSTS 18798A.

This letter is intended to clarify existing PSRP policy with respect to equipment surface temperature limits for both intentional and incidental crew contact. Intentional contact is defined as contact for normal operational manipulation such as lifting, holding, or grasping. Incidental contact is defined as accidental or unintended contact. For both cases, the temperature range of -18° Celsius to +49° Celsius (0° Fahrenheit to 120° Fahrenheit) is the acceptable range for "bare skin contact" for metallic surfaces. The upper temperature limit for "bare skin contact" is higher than 49° Celsius for surfaces having thermal properties of nonmetallic materials. These acceptable higher temperatures can be determined by using the method described in Enclosure 2.

#### **INTENTIONAL CONTACT**

Payload equipment designs having surfaces requiring intentional contact, where the crew is free to terminate the contact immediately, must satisfy the following constraints.

- (1) Designs with active thermal management (for example, fans, heaters, furnaces, and active cooling devices) must provide a single fault tolerant design to exceeding surface temperatures that are acceptable for "bare skin contact," or be incapable of exceeding the acceptable range for "bare skin contact." In this case, a procedural control using temperature strips (labels) may be utilized as one of the required levels of failure tolerance.
- (2) Designs that do not use active thermal management must provide nominal surface temperatures that are acceptable for "bare skin contact," (i.e., no failure tolerance is required).

Payload equipment having surfaces requiring intentional contact, where the crew is required to maintain contact, shall either:

- (1) Be single fault tolerant against exceeding the acceptable range. In this case, a procedural control using temperature strips (labels) may not be utilized as one of the required levels of failure tolerance, or
- (2) Be incapable of exceeding the acceptable range.

For payload equipment having surfaces that exceed the acceptable range that require crew contact, protective equipment such as gloves or mittens suitable for the worst case temperature extremes resulting from a single failure shall be provided.

#### **INCIDENTAL CONTACT**

Payload equipment having surfaces with the potential for incidental crew contact shall be designed such that nominal surface temperatures are acceptable for intentional bare skin contact (i.e., no failure tolerance is required) or design provisions must be in place that will preclude incidental contact with surfaces outside the acceptable range for "bare skin contact."

Questions concerning this subject should be addressed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, Mail Code NS2, telephone (713) 483-4297.

#### ***ORIGINAL SIGNED BY :***

Ronald D. Dittmore

2 Enclosures

#### **Distribution:**

Payload Safety Distribution

cc:

See List

## MAXIMUM PERMISSIBLE MATERIAL TEMPERATURE

Temperatures higher than those given in Table I are acceptable when they are established in accordance with the following relationship:

$$T_{mPT} = \text{MAXIMUM PERMISSIBLE MATERIAL TEMPERATURE} \\ = YI [ (kpc)^{-1/2} + 31.5 ] + 41$$

where;

$$YI = \text{antilog} [ YII ( a1 ) + \log YIII ]$$

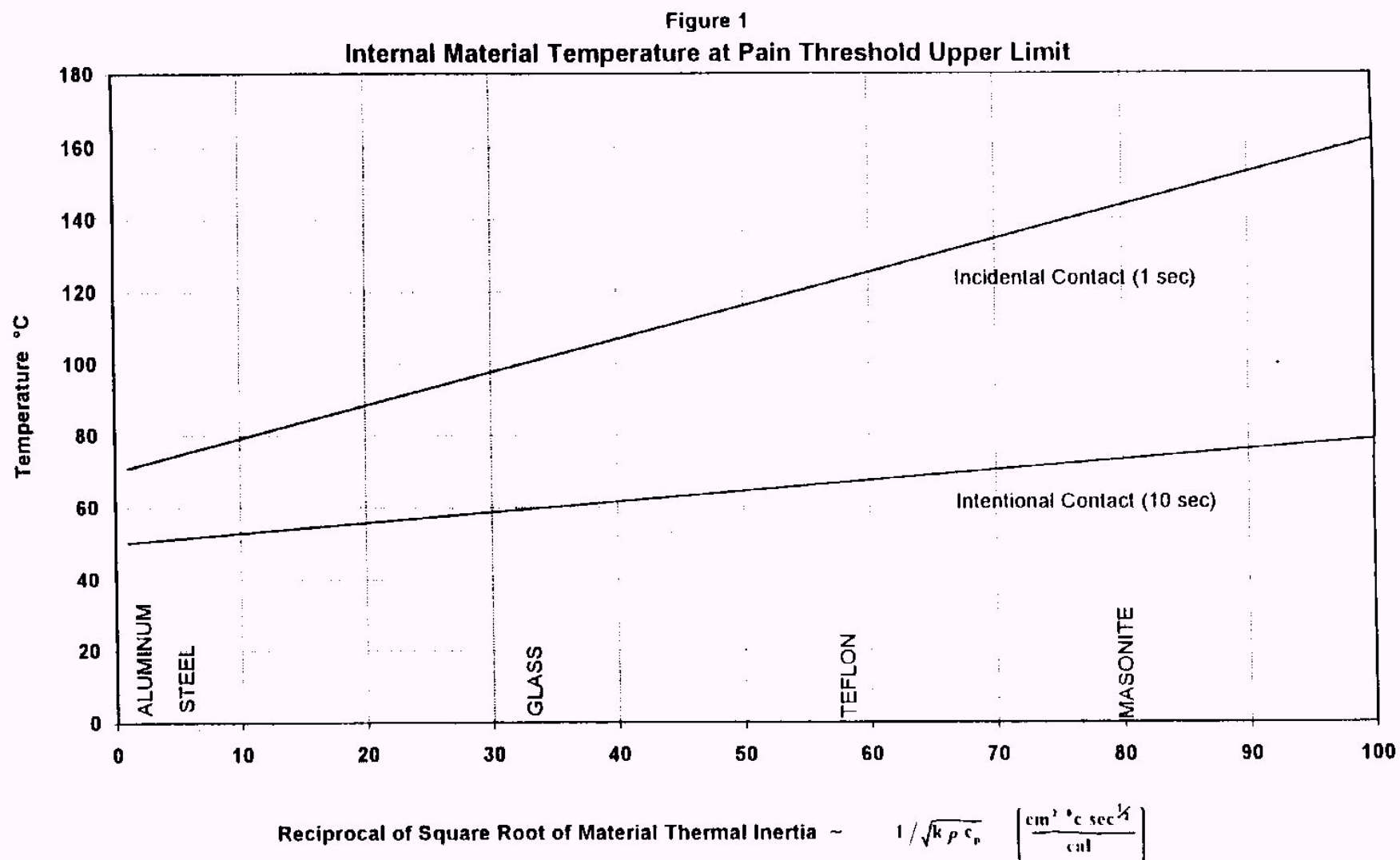
$$YII = 1.094 (t)^{-0.184}$$

$$YIII = 0.490 (t)^{-0.412}$$

and;  $(kpc)^{-1/2}$  = Thermal Inertia Of Contact Material, (k=Coefficient of heat transfer, p=density, and c=specific heat)  
 $a1$  = Epidermal Thickness (mm), (~ Nominal 0.25 mm)  
 $t$  = Time Of Exposure (in seconds) (Time of exposure is limited to values of  $\geq 1$  second for the incidental contact case and  $\geq 10$  seconds for the intentional contact case. See the discussion that follows)

(Reference: Air Standardization Agreement, AIR STD 61/39, 11 September 1984, Maximum Permissible Temperatures Of Materials For Safe Contact With Bare Skin, Air Standardization Coordinating Committee, Washington, DC)

Figure 1 illustrates the above relationship for hot temperatures and maps  $T_{mPT}$  against an appropriate range of values of thermal inertia. The illustration is based upon an average epidermal thickness of 0.25 mm, and displays two operational categories defined as follows; incidental contact and intentional contact for normal operational manipulations such as lifting, holding, or grasping. Specific task times should be based on conservative analysis or tests. When a specific operational scenario requires that contact times vary from those illustrated, the desired values must be applied to the expression above to arrive at a specific surface temperature limit. The times for incidental contact cases must be one second or greater. The times for intentional contact cases must be 10 seconds or greater.



## **2. ELECTRICAL**

<u>Title</u>	<u>JSC Letter Number</u>
2.1 Separation of Redundant Safety Critical Circuits	ET12-90-115
2.2 Protection of Payload Electrical Power Circuits *	TA-92-038
2.3 On-Orbit Bonding and Grounding	MA2-99-142



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

Reply to Attn of :

JSC, ET12-90-115

OCT 16 1990

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Separation of Redundant Safety-Critical Circuits

The information contained in this letter is an interpretation and clarification of the Space Shuttle payload safety requirements for separation of redundant safety-critical circuits. The requirements in this letter are applicable to all payloads designed to NSTS 1700.7B. This letter will be utilized by the Space Shuttle Payload Safety Review Panel in assessing payload design compliance. Please add this letter to your copy of NSTS 18798, "Interpretation of NSTS Payload Safety Requirements."

As a result of increased emphasis on the routing of redundant safety-critical circuits, the following information is provided to aid in the interpretation of NSTS 1700.7B, paragraph 207, Redundancy Separation, which states:

"Safety-critical redundant subsystems shall be separated by the maximum practical distance, or otherwise protected, to ensure that an unexpected event that damages one is not likely to prevent the others from performing the function. All redundant functions that are required to prevent a catastrophic hazard must not be routed through a single connector."

For the purpose of this discussion, wire bundles are considered to be any group of wires that are spot-tied or clamped together. Redundant safety-critical circuits are to be routed in separate cable bundles via different routing paths which are separated to the maximum extent possible. Where separate routing paths are not possible, no less than one-half inch separation between wire bundles shall be assured under any level of vibration or shock to which the vehicle will be exposed.

When practical considerations prevent separated routing of wiring for redundant safety-critical functions to comply with the criteria established in NSTS 1700.7B noted above, then steps must be taken to provide equivalent safety. As an example, equivalent safety could be achieved by the incorporation of a design feature such as a physical barrier that prevents failures in one safety-critical circuit from propagating to adjacent safety-critical circuits.

The payload hazard reports shall identify damage to electrical circuits as a possible cause of the failure of redundant safety-critical circuits. The appropriate hazard controls shall be identified and described in the hazard report and shall be selected from those described earlier in this letter. Questions regarding implementation compliance shall be directed to the Cargo Integration Engineering Office representative, Mr. Stanley E. Snipes, ET12/JSC, at FTS 525-3780.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.

Distribution: Payload Safety Distribution List

cc:

NASA Hqs., MK/S. J. Cristofano  
SM/R. H. Benson

KSC, CM/J. T. Conway  
TM/R. B. Sieck

JSC, AC/D. A. Nebrig  
CA/D. R. Puddy  
CB/D. C. Hilmer  
J. A. Hoffman  
D.C. Leestma

DA2/T. W. Holloway

DA8/C. R. Knarr

B. R. Stone

EA/H. O. Pohl

EP/C. A. Vaughan

EP42/J. W. Griffin

EP54/D. M. Gaston

ES4/N. E. Tengler

USAF SSD-Los Angeles, CLP/Lt. Col. B. A. Lucas  
Lt. Col. J. Chapman

Rockwell-Downey, AD60/R. L. Peercy  
FC16/D. H. Frederick

Vitro Corporation  
Space Operations Center  
Attn: Mr. O. W. Kenton  
400 Virginia Ave. SW, Suite 825  
Washington, DC 20546

ES53/M. D. Pedley

ET/F. J. DeVos

C. A. Graves

ET12/D. E. Tadlock

GA/L. S. Nicholson

GK3/C. M. Vaughn

GR2/I. M. Darnell

NA/C. S. Harlan

PA/R. L. Berry

SD24/N. L. Henry (KRUG)

TA/Staff

TJ2/L. Lo (Rockwell)

VA/D. M. Germany

VK/E. E. Wright

BOE, HS-04/M. Fodroci

W. T. Mays

Aerospace Corporation  
Attn: M5-468/H. De La Puente  
P. O. Box 92957  
Los Angeles, CA 90009



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

Reply to Attn of :

JSC, TA-92-038

FEB 22 1993

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Protection of Payload Electrical Power Circuits

The information contained in this letter is an interpretation and clarification of the Space Shuttle safety requirements in paragraph 213.1 of NSTS 1700.7B for payload wire sizing and circuit protection. The requirements in this letter are applicable to all payloads designed to NSTS 1700.7B and will be utilized by the Space Shuttle Payload Safety Review Panel in assessing payload design compliance. Please add this letter to your copy of NSTS 18798, "Interpretation of Space Shuttle Payload Safety Requirements." This letter supersedes letters ER-87-326, dated January, 8, 1988, subject Protection of Power Distribution Circuitry; EH5-83-88, dated August 2, 1983, subject Payload Wire Size Criteria; and EH13-82-191, dated June 25, 1982, subject Electrical Hazard Control for Payloads. Payloads that have previously been designed to those letters are not affected.

Power distribution circuitry is defined as that wiring from the payload power source through the last payload downsized insulated wire segment.

Properly selected circuit protection devices are defined as devices having operating characteristics such that the wire manufacturer's recommended operating temperature limit for the wire insulation will not be exceeded for any possible loading or fault condition of the circuit under worst case environmental conditions.

Payload electrical power distribution circuitry shall be designed such that payload electrical faults do not damage orbiter wiring nor present a hazard to the orbiter or crew. Circuit protection devices and wire sizes shall be selected in accordance with TM 102179, "Selection of Wires and Circuit Protection Devices for NSTS Orbiter Vehicle Payload Electrical Circuits," and incorporated into the payload design in each of the following cases:

1. When orbiter wiring is to be energized from a payload power bus. This will prevent damage to the orbiter vehicle.



2. When payload power distribution wiring is routed within a crew habitable volume. This will minimize the amount of toxic products generated in the crew environment by limiting the amount of energy delivered to the fault location, thereby reducing the potential for overheating wire insulation. Compliance with TM 102179 is not mandatory when the last wire downsizing is accomplished inside avionics boxes, which are designed and tested to standard aerospace practices.
3. When payload redundant safety critical power has been derived from a single approved orbiter source. Letter TA-91-006, dated February 13, 1991, subject Cargo Bay Primary Power Feeder Fault Tolerance, refers to the implementation policy for this requirement. This is required to prevent a fault in one redundant safety critical circuit from causing the loss of the power source to the other redundant safety critical circuit.
4. When energized payload power distribution circuits are routed through wire bundles containing circuits which, if any were energized, would potentially bypass or remove more than one inhibit to a hazardous function. Protective devices in this application minimize the potential for fault overloads to cause damage to adjacent wiring and consequently to cause reconfigured circuits.

Compliance with circuit protection criteria will not be considered to be an adequate hazard control when reviewing a payload design for compliance with the flammability requirements of NSTS 1700.7B. paragraph 209.2. Circuit protective devices can only limit the energy delivered to a fault or failed component when the current is sufficient to cause the protective devices to open. The energy-limiting action of circuit protection devices may not be adequate to eliminate electrical ignition sources for certain materials configurations; therefore, proper selection of materials in accordance with NHB 8060.1C, "Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures for Materials in Environments that Support Combustion," shall be the primary hazard control method for a flammability hazard.

Enclosed in table form are wire ratings and related circuit protection device information extracted from TM 102179 curves and tables for several common wire insulation ratings for orbiter ambient conditions of 72 °F in the cabin and 200 °F in the cargo bay. The use of wire insulation with ratings other than the three contained in the enclosure will necessitate the use of TM 102179 in order to determine the appropriate requirements.

Questions regarding implementation compliance shall be directed to the Executive Secretary, Payload Safety Review Panel, NS2/JSC, at 713-483-4297.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.

Enclosure

cc:  
See List

**CRITERIA FOR WIRING AND CIRCUIT PROTECTION DEVICES  
FOR 150, 175, AND 200 DEGREES C WIRE INSULATION  
FOR STANDARD ORBITER AMBIENT CONDITIONS**

**ET13/SYSTEMS ENGINEERING AND INTEGRATION OFFICE**

**October 12, 1990**

**ENCLOSURE**

## SCOPE

It is not the intent that this enclosure provide detailed design instructions for the selection of electrical circuit wire size and circuit protection devices for all payload applications. A detailed step-by-step guide that allows a payload to custom design these items for its unique application is contained in JSC engineering document TM 102179, "Selection of Wires and Circuit Protection Devices for NSTS Orbiter Vehicle Payload Electrical Circuits." Information contained in this enclosure has been extracted from figures and tables resident in that document and is intended for use in assessing whether or not a payload has conformed to design criteria for the standard set of ambient conditions defined below.

## NOTES FOR USING TABLES

1. Wire rating information is derived from extensive testing of MB0150-048 Orbiter wiring at JSC and applies to equivalent copper wiring with any type of insulation. For convenience, information pertaining to wire with insulation ratings of 150, 175, and 200 degrees Centigrade are shown. For wire ratings other than these, refer to JSC engineering publication TM 102179, "Selection of Wires and Circuit Protection Devices for NSTS Orbiter Vehicle Payload Electrical Circuits". Wire sizes smaller than 26 gauge are not recommended for use in payloads.
2. The circuit protection devices shown are used on the Orbiter and are recommended for payload use. However, other devices that provide equivalent protection may be utilized in the payload design.
3. An ambient temperature of 72 degrees F is assumed for ground and cabin locations, while 200 degrees F is assumed for the payload bay location during flight. In the tables, the cabin and payload bay location numbers are derived from wire testing performed in a vacuum, one g environment.
4. Glossary of table terms
  - a. Rating - Manufacturer's sea-level ambient rating.
  - b. Min. Blow - Minimum current level at which the device will open.
  - c. Max. Blow - Maximum level of current required to open the device.
  - d. Max. Appl. Load - Maximum Applied Load is the

maximum current level at which the circuit in which the device to be used should be designed to operate. This figure represents the device capability when derated for low gravity or vacuum operation.

e. Current Carrying Capacity of Wire - Represents the maximum sustained current in amperes which the wire can carry in the specified environment and not experience a temperature that exceeds the temperature rating of the insulation material.

f. If an "X" appears in a recommended wire size column, this means that there is no wire gauge large enough for that application.

5. These tables are for the purpose of showing the sizing relationships for circuit protection devices and wiring during ground, cabin, and payload bay use. No inferences should be made regarding how much power might actually be available in any of these locations.

6. Protection of Parallel Power Wires - If two power wires emanate from a source and are joined together again downstream prior to being distributed by the payload, each wire shall have its own circuit protection device. If more than two power wires emanate from a source and are joined together again downstream prior to being distributed by the payload, each wire shall have a circuit protection device both at its source end and at its load end.

7. The tables in this document do not reflect wire bundle derating, nor does NASA/JSC believe bundle derating to normally be necessary. This is due to the multitude of inter-related factors involved in bundling which can either enhance or degrade the current-carrying capacity of a wire. However, in unique applications where a majority of wires in a bundle are heavily loaded simultaneously, the user should consult the previously referenced JSC engineering publication or MIL-W-5088K bundle derating curves.

# **CURRENT CARRYING CAPACITIES OF INSULATED PAYLOAD WIRING** (MAXIMUM AMPERES)

WIRE GAUGE	150 Deg. C WIRE RATING			175 Deg. C WIRE RATING			200 Deg. C WIRE RATING		
	PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION		
	CABIN	P/L BAY	GROUND	CABIN	P/L BAY	GROUND	CABIN	P/L BAY	GROUND
0	310.0	235.0	420.0	335.0	285.0	455.0	361.1	332.0	470.0
2	205.0	160.0	300.0	225.0	196.0	325.0	245.8	225.0	341.0
4	140.0	111.0	230.0	153.0	135.0	249.0	171.6	157.0	267.0
6	107.0	84.0	180.0	118.0	101.0	195.0	128.9	118.0	211.0
8	74.0	58.0	144.0	82.0	70.0	157.0	88.4	81.0	169.0
10	47.5	36.0	78.0	52.0	44.0	85.0	56.2	51.0	91.0
12	34.0	26.0	64.0	37.0	31.8	69.0	40.9	37.0	74.0
14	23.5	18.4	50.0	25.7	22.5	54.0	28.7	26.0	60.0
16	17.4	13.7	37.5	19.1	16.5	41.0	21.4	20.0	43.0
18	15.8	12.0	31.9	17.4	14.6	34.2	19.1	17.0	37.0
20	11.7	9.0	23.5	12.8	10.9	25.1	13.9	13.0	27.0
22	8.7	6.8	19.9	9.5	8.1	21.5	10.4	9.5	23.0
24	6.3	4.8	14.2	6.8	5.8	15.4	7.5	6.8	16.4
26	4.4	3.5	11.5	4.9	4.2	12.4	5.3	4.8	13.2

**FUSE, CARTRIDGE (ME451-0009-XXXX)**

FUSE, CARTRIDGE (ME451-0009-XXXX)					MINIMUM RECOMMENDED WIRE SIZE											
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING					
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION					
DASH #	RATING (amps)	MIN. BLOW (100%)	MAX. APPL. LOAD (50%)	MAX. BLOW	CABIN	P/L	BAY	GROUND	CABIN	P/L	BAY	GROUND	CABIN	P/L	BAY	GROUND
1023	0.5	0.5	0.25	0.75 (150%)	26	26	26		26	26	26		26	26	26	
1001	1.0	1.0	0.50	1.50 (150%)	26	26	26		26	26	26		26	26	26	
1002	2.0	2.0	1.00	3.00 (150%)	26	26	26		26	26	26		26	26	26	
1003	3.0	3.0	1.50	4.50 (150%)	24	24	26		26	24	26		26	26	26	
1021	5.0	5.0	2.50	6.75 (135%)	22	22	26		24	22	26		24	24	26	
1019	7.5	7.5	3.75	10.12 (135%)	20	18	26		20	20	26		22	20	26	
1005	10.0	10.0	5.00	13.5 (135%)	18	16	24		18	18	24		20	18	24	
1006	15.0	15.0	7.50	20.25 (135%)	14	12	20		14	14	22		16	14	22	
1007	20.0	20.0	10.00	27.00 (135%)	12	10	18		12	12	18		14	12	20	
1008	25.0	25.0	12.50	33.75 (135%)	12	10	16		12	10	18		12	12	18	
1009	30.0	30.0	15.00	40.50 (135%)	10	8	14		10	10	16		12	10	16	

**FUSE, LARGE, REGULAR BLOW (ME451-0016-XXXX)**

FUSE, LARGE, REGULAR BLOW (ME451-0016-XXXX)					MINIMUM RECOMMENDED WIRE SIZE											
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING					
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION					
					CABIN	P/L	BAY	GROUND	CABIN	P/L	BAY	GROUND	CABIN	P/L	BAY	GROUND
DASH #	RATING (amps)	MIN. BLOW (110%)	MAX. APPL. LOAD (100%)	MAX. BLOW												
2035	35.0	38.5	35.0	59.50 (170%)	8	6	12		8	8	12		8	8	14	
2050	50.0	55.0	50.0	85.0 (170%)	6	4	8		6	6	10		8	6	10	
2080	80.0	88.0	80.0	188.0 (235%)	2	0	4		2	2	6		2	2	6	
2100	100.0	110.0	100.0	235.0 (235%)	0	0	2		0	0	4		2	0	4	
2125	125.0	137.5	125.0	250.0 (200%)	0	X	2		0	0	2		0	0	4	
2150	150.0	165.0	150.0	300.0 (200%)	0	X	2		0	X	2		0	0	2	
2200	200.0	220.0	200.0	400.0 (200%)	X	X	0		X	X	0		X	X	0	

**FUSE, SLOW BLOW (ME451-0016-XXXX)**

FUSE, SLOW BLOW (ME451-0016-XXXX)					MINIMUM RECOMMENDED WIRE SIZE											
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING					
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION					
					CABIN	P/L	BAY	GROUND	CABIN	P/L	BAY	GROUND	CABIN	P/L	BAY	GROUND
DASH #	RATING (amps)	MIN. BLOW (110%)	MAX. APPL. LOAD (100%)	MAX. BLOW												
3035	35.0	38.5	35.0	84 (240%)	6	6	8		6	6	10		8	6	10	
3050	50.0	55.0	50.0	120.0 (240%)	4	2	8		4	4	8		6	4	8	
3150	150.0	165.0	150.0	360.0 (240%)	X	X	0		X	X	0		0	X	0	
3200	200.0	220.0	200.0	480.0 (240%)	X	X	X		X	X	X		X	X	X	

**CIRCUIT BREAKER (MC454-0026-XXXX)**

					MINIMUM RECOMMENDED WIRE SIZE								
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING		
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION		
					CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND
DASH #	RATING (amps)	MIN. BLOW (110%)	MAX. APPL. LOAD (95%)	MAX. BLOW									
2010	1.0	1.10	0.95	1.45 (145%)	26	26	26	26	26	26	26	26	26
2020	2.0	2.20	1.90	2.90 (145%)	26	26	26	26	26	26	26	26	26
2030	3.0	3.30	2.85	4.35 (145%)	26	24	26	26	24	26	26	26	26
2050	5.0	5.50	4.75	7.25 (145%)	22	20	26	22	22	26	24	22	26
2075	7.5	8.25	7.125	10.87 (145%)	20	18	26	20	20	26	20	20	26
2100	10.0	11.00	9.50	14.50 (145%)	18	14	22	18	18	24	18	18	24
2150	15.0	16.50	14.25	21.75 (145%)	14	12	20	14	14	20	14	14	22
2200	20.0	22.00	19.00	29.00 (145%)	12	10	18	12	12	18	12	12	18

**CIRCUIT BREAKER, 3 PHASE AC (MC454-0032-XXXX)**

					MINIMUM RECOMMENDED WIRE SIZE								
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING		
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION		
					CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND
DASH #	RATING (amps)	MIN. BLOW (110%)	MAX. APPL. LOAD (95%)	MAX. BLOW									
3030	3.0	3.30	2.85	4.35 (145%)	26	24	26	26	24	26	26	26	26

**REMOTE POWER CONTROLLER (MC450-0017-XXXX)**

					MINIMUM RECOMMENDED WIRE SIZE								
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING		
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION		
					CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND
DASH #	RATING (amps)	MIN. BLOW (125%)	MAX. APPL. LOAD (100%)	MAX. BLOW									
1030	3.0	3.75	3.0	4.50 (150%)	24	24	26	26	24	26	26	26	26
1050	5.0	6.25	5.0	7.50 (150%)	22	20	26	22	22	26	24	22	26
1075	7.5	9.375	7.5	11.25 (150%)	20	18	26	20	18	26	20	20	26
1100	10.0	12.50	10.0	15.00 (150%)	18	14	22	18	16	24	18	18	24
1150	15.0	18.75	15.0	22.50 (150%)	14	12	20	14	14	20	14	14	22
1200	20.0	25.00	20.0	30.00 (150%)	12	10	18	12	12	18	12	12	18

**FUSE, SUBMINIATURE PLUG-IN (ME451-0018-XXXX)**

DASH #   RATING (amps)   MIN. BLOW (100%)   MAX. APPL. LOAD (50%)   MAX. BLOW					MINIMUM RECOMMENDED WIRE SIZE								
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING		
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION		
					CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND
0012	0.125	0.125	0.0625	0.188 (150%)	26	26	26	26	26	26	26	26	26
0025	0.25	0.25	0.125	0.375 (150%)	26	26	26	26	26	26	26	26	26
0050	0.50	0.50	0.25	0.75 (150%)	26	26	26	26	26	26	26	26	26
0075	0.75	0.75	0.375	1.125 (150%)	26	26	26	26	26	26	26	26	26
0100	1.00	1.00	0.50	1.50 (150%)	26	26	26	26	26	26	26	26	26
0150	1.50	1.50	0.75	2.25 (150%)	26	26	26	26	26	26	26	26	26
0200	2.00	2.00	1.00	3.00 (150%)	26	26	26	26	26	26	26	26	26
0300	3.00	3.00	1.50	4.50 (150%)	24	24	26	26	24	26	26	26	26
0400	4.00	4.00	2.00	6.00 (150%)	24	22	26	24	22	26	24	24	26
0500	5.00	5.00	2.50	7.50 (150%)	22	20	26	22	22	26	24	22	26
0750	7.50	7.50	3.75	11.25 (150%)	20	18	26	20	18	26	20	20	26
1000	10.00	10.00	5.00	15.00 (150%)	18	14	22	18	16	24	18	18	24

**FUSE, SMALL WITH AXIAL LEADS (ME451-0010-XXXX)**

DASH #   RATING (amps)   MIN. BLOW (100%)   MAX. APPL. LOAD (50%)   MAX. BLOW					MINIMUM RECOMMENDED WIRE SIZE								
					150 Deg. C RATING			175 Deg. C RATING			200 Deg. C RATING		
					PAYLOAD LOCATION			PAYLOAD LOCATION			PAYLOAD LOCATION		
					CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND	CABIN	P/L	BAY GROUND
1001	0.125	0.125	0.0625	0.188 (150%)	26	26	26	26	26	26	26	26	26
1002	0.25	0.25	0.125	0.375 (150%)	26	26	26	26	26	26	26	26	26
1005	0.50	0.50	0.25	0.75 (150%)	26	26	26	26	26	26	26	26	26
1007	0.75	0.75	0.375	1.125 (150%)	26	26	26	26	26	26	26	26	26
1010	1.00	1.00	0.50	1.50 (150%)	26	26	26	26	26	26	26	26	26
1015	1.50	1.50	0.75	2.25 (150%)	26	26	26	26	26	26	26	26	26
1020	2.00	2.00	1.00	3.00 (150%)	26	26	26	26	26	26	26	26	26
1030	3.00	3.00	1.50	4.50 (150%)	24	24	26	26	24	26	26	26	26
1040	4.00	4.00	2.00	6.00 (150%)	24	22	26	24	22	26	24	24	26
1050	5.00	5.00	2.50	7.50 (150%)	22	20	26	22	22	26	24	22	26
1070	7.00	7.00	3.50	10.50 (150%)	20	18	26	20	20	26	20	20	26
1100	10.00	10.00	5.00	15.00 (150%)	18	14	22	18	16	24	18	18	24



National Aeronautics and  
Space Administration  
**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of :

MA2-99-142

October 12, 1999

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/International Space Station Manager for Technical Development

SUBJECT: On-Orbit Bonding and Grounding

This letter clarifies the payload safety requirements from paragraph 213.1 of the National Space Transportation System (NSTS) 1700.7B, "Safety Policy and Requirements for Payloads using the Space Transportation System (STS)," and NSTS 1700.7B International Space Station (ISS) Addendum, "Safety Policy and Requirements for Payloads using the International Space Station." Please add this letter and the enclosed updated table of contents to your copy of NSTS/ISS 18798, "Interpretation of STS Payload Safety Requirements," as an applicable interpretation against NSTS 1700.7B and NSTS 1700.7B ISS Addendum.

This letter defines criteria for satisfying bonding and grounding requirements when hardware installation occurs on orbit. Two acceptable methods are the preferred Design for Minimum Risk (DFMR) approach and the alternative Failure Tolerance approach. These criteria apply when crew contact with voltages above 32 volts (root mean square or direct current) is possible following normal procedures or after potential electrical or mechanical failures. In both cases, a fault bond path shall be established before power is applied.

This letter does not apply to payloads located in ISS modules that have a floating ground; bonding and grounding designs for such payloads will be evaluated on a case-by-case basis. Electromagnetic Interference (EMI) issues concerning bonding and grounding are not incorporated in this letter. Technical requirements for EMI are contained in section 212.2 of NSTS 1700.7B and NSTS 1700.7B ISS Addendum.

Using the following DFMR criteria provides confidence that the required fault bond will be reliably established and can carry sufficient fault current. This eliminates the need for an additional bond path and for on-orbit verification of the fault bond. The Payload Safety Review Panel (PSRP) will use the following criteria to assess design compliance under the DFMR approach.

1. The minimum surface area of metal (i.e., faying surface) in the bond path for fault bonds with a metal-to-metal wiping feature shall be four times the equivalent cross-sectional area of copper wiring necessary to carry the fault bond current.
2. Hardware used for bonding purposes shall not consist of self-tapping screws; zinc plated bolts, nuts or screws; star, anodized, zinc plated, or unplated washers; or any cadmium-plated hardware.

3. Surface preparation for an electrical bond shall be accomplished during fabrication, assembly, or ground processing by removing all anodic film, grease, paint, lacquer, or other electrical high-resistance properties from the immediate area to ensure negligible radio frequency impedance between adjacent metal parts. Chemical cleaning and surface preparation shall be in accordance with standard practice (Military Standard 464 may be used as a guideline).
4. A certification test shall be performed as part of a ground-based qualification to ensure an acceptable bond resistance will be present using on-orbit assembly methods.
5. Nominal assembly methods shall assure metal-to-metal wiping of the bond area to remove potential oxidation of the bond surface (for metal to metal contact or bond straps).

The alternative, Fault Tolerant approach uses payload experiment connectors to establish the bond path on orbit. The design features described below are required when a conductor is used to establish the bond path via a connector pin. Because a pin failure is considered credible, there shall be two bond paths. The following criteria apply:

1. The redundant bond paths shall be free of credible common cause failure modes.
2. Connector bonds shall include at least one fault bond path in each power connector.
3. Both bond paths shall undergo a certification test as part of the ground-based qualification to ensure an acceptable bond resistance will be present after assembly using nominal on-orbit methods.
4. The connector interface shall be designed such that each pin used as a bond path is separated to the greatest extent possible from redundant bond and powered pins.

NOTE: Grounding of the powered side connector (e.g., using a grounded back-shell) is an acceptable alternative design solution for one of the redundant bond paths identified above.

Questions concerning this subject should be addressed to the Executive Secretary, Space Shuttle PSRP, Mail Code NC4, telephone (281) 483-8848.

***Original Signed By:***

William H. Gerstenmaier

***Original Signed By:***

Jay H. Greene

Enclosure

cc:  
See List

MA2-99-142

3

Distribution:


CB/G. D. Griffith  
DO12/J. M. Childress  
EA4/R. J. Wren  
MS3/K. B. Packard  
NC4/M. L. Ciancone  
OE/S. L. Thomas  
OZ3/D. W. Hartman  
SD2/M. E. Coleman

## cc:

CA/J. D. Wetherbee  
CB/C. J. Precourt  
DA/B. R. Stone  
EA/L. S. Nicholson  
EA4/J. W. Aaron  
LM/T. W. Logan  
MA/R. D. Dittmore  
MG/R. H. Heselmeyer  
MM/J. B. Costello  
MQ/M. D. Erminger  
MS/L. D. Austin, Jr.  
MT/R. M. Swalin  
MV/R. R. Roe, Jr.  
OA/T. W. Holloway  
OE/J. E. Holsomback  
XA/G. J. Harbaugh  
HQ/M-4/W. M. Hawes  
HQ/M-7/N. B. Starkey  
HQ/MO/R. L. Elsbernd  
HQ/MO/S. R. Nichols  
KSC/AA-C/L. J. Shriver  
KSC/MK/D. R. McMonagle  
KSC/MK-SIO/R. L. Segert

### **3. FLAMMABLE ATMOSPHERE**

<u>Title</u>	<u>JSC Letter Number</u>
3.1 Ignition of Flammable Payload Bay Atmosphere	NS2/81-MO82

U.S. Government		Lyndon B. Johnson Space Center		
<b>MEMORANDUM</b>				
REFER TO: NS2/81-M082	DATE APR 09 1981	INITIATOR NS2/EJSchlei:3/18/81:2901 Rewritten: NS2/EJSchlei:4/1/81:2901	ENCL	
TO: MEMORANDUM FOR RECORD		CC: See list below		
FROM: PA/Manager, STS Operations WA/Chairman, STS Payload Safety Review Panel		SIGNATURE Original Signed by: GLYNN S. LUNNEY Glynn S. Lunney Original Signed By: RICHARD A. COLONNA Richard A. Colonna		
SUBJ: Implementation of Paragraph 219 of NHB 1700.7A, "Safety Policy and Requirements For Payloads Using the Space Transportation System (STS)"				
<p>The purpose of this memorandum is to clarify procedures for implementing paragraph 219 of NHB 1700.7A, which states: "FLAMMABLE ATMOSPHERES. During Orbiter entry, landing, or postlanding operations (whether planned or contingency), the normal payload functions shall not cause ignition of a flammable payload bay atmosphere that may result from leakage or ingestion of fluids into the payload bay." This paragraph states that only the normal payload operation is to be considered for implementation; failure modes need not be considered. Contingency landings (i.e., return to launch site and abort once around) must be considered.</p> <p>Hazards from a flammable PLB (payload bay) atmosphere are prevented by controlling all possible ignition sources. These may be divided roughly into two categories: Electrical discharges and hot surfaces. Electrical discharge ignition sources are those caused by arcing, sparking, and operation of switches, relays, motors, etc. Hot surface ignition sources are those caused by the presence of high temperature surfaces such as lamps, heaters, radioisotope thermal generators, etc.</p> <p>The preferred method for preventing electrical ignition of a flammable PLB atmosphere is for all payloads to be unpowered during both launch and descent. If a payload must be powered during launch, it must be designed so that either (1) all ignition sources are controlled or (2) a method is provided for deenergizing all uncontrolled ignition sources. The method for deenergizing must be approved by the STS Payload Safety Review Panel. If a payload must be powered during descent, it must be designed so that all ignition sources are controlled.</p> <p>Electrical ignition sources must be controlled by one of the following procedures, which are listed in the order of preference:</p> <ol style="list-style-type: none"> <li>Seal all relays, switches, motors, and other similar ignition sources to a leak rate of less than or equal to <math>1 \times 10^{-4}</math> standard cubic centimeters of helium per second, at a delta pressure of one atmosphere. Leak rates must be verified by test.</li> <li>Perform the test stated in method 511.1, procedure 1 of MIL-STD-810, "Environmental Test Methods for Aerospace and Ground Equipment," or method 109B of MIL-STD-202, "Test Methods for Electronic and Electric Component Parts."</li> <li>Perform the test stated in method 511.1, procedure 11 of MIL-STD-810.</li> </ol>				
JSC Form 1180 (Rev Jan 76)	INCREASED PRODUCTIVITY - LOWER COST			PAGE 1 OF 2

Also, any exposed surfaces that have temperatures of greater than 352°F must be identified on a hazard report form. These will be assessed for hazardous interaction with the fluids and/or gasses which may be present in the PLB during that STS mission.

Payload developers will review their payloads to assure compliance with NHB 1700.7A. The developers of these payloads to which paragraph 219 applies will submit hazard reports addressing ignition of a flammable PLB atmosphere. These hazard reports will be submitted and reviewed in accordance with the procedures described in JSC 13830, "Implementation Procedure for STS Payloads System Safety Requirements."

Questions or comments on this subject should be directed to Mr. E. J. Schlei, Safety Division, code N52, FTS 525-2901.

cc:

CB/J. P. Kerwin  
CB/J. W. Young  
CH/D. A. Ballard  
CH/J. W. O'Neill  
EA8/L. E. Bell  
LA/R. F. Thompson  
LK/A. E. Morse  
NA/M. L. Raines  
    /C. S. Harlan  
NS/J. B. Hammack  
NS/W. T. Mays (Boeing/HS-04)  
NS2/B. J. Miller  
NS2/B. L. Walker (Boeing/HS-04)  
PA/J. C. Bostick  
PF/L. S. Nicholson  
PH/L. G. Williams  
SD3/J. M. Waligora  
WA3/J. D. Lobb  
NASA Hqs., MR-8/P. D. Davis  
KSC, CP/J. J. Neilon  
    CP-PCO/W. E. Paramore  
    SF-ENG/C. R. Billings  
    SP/R. H. Gray

## **4. PAYLOAD OPERATIONS**

<u>Title</u>	<u>JSC Letter Number</u>
4.1 Monitoring for Safety	TA-88-018
4.2 Payload Commanding-POCC	TA-91-062
4.3 Crew Mating/Demating of Powered Connectors	MA2-99-170
4.4 Contingency Return and Rapid Safing	MA2-96-190
4.5 On-Orbit Maintenance	MA2-00-038



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

APR 06 1989

Reply to Attn of :

NSTS-JSC, TA-88-018

TO: Distribution

FROM: NSTS-TA/Manager, NSTS Integration and Operations

SUBJECT: Monitoring for Safety

The information contained in this letter is considered an interpretation or clarification of the payload safety requirements of NHB 1700.7 and will be utilized by the Safety Review Panel in assessing payload design compliance. Please add this letter to your copy of NSTS 18798 (Interpretations of STS Payload Safety Requirements) as being an applicable interpretation against NHB 1700.7A and NSTS 1700.7B when issued.

The justification for monitoring stems from the NSTS need to maintain the knowledge that the systems being operated are in a state of safety such that a failure can be tolerated at all times. Thus, the knowledge of system status can form the basis for the development of operational flight rules.

We have prepared a comprehensive interpretation of the NHB 1700.7 monitoring requirements (copy enclosed). This interpretation is applicable for all payloads using the STS and is effective for NHB 1700.7 Revision A published in May 1980, and NSTS 1700.7 Revision B which will be released in the near future.

Questions or comments should be addressed to TA/R. L. Blount at (713) 483-1207.

**ORIGINAL SIGNED BY :**

Leonard S. Nicholson

Enclosure

Distribution: Payload Safety Distribution List



## MONITORING PAYLOAD SAFETY PARAMETERS

Monitoring as defined in NHB 1700.7 falls into two categories: real-time and near real-time.

(1) Real-Time Monitoring (RTM) is required to maintain continuous visibility into the status of the remaining safety inhibits when configuring a payload for a potentially hazardous event (i.e., deployment), or the system status when monitoring is necessary for hazard control (i.e., hazard detection and safing in a situation where an immediate hazard to the NSTS could exist).

The RTM monitoring requirements can be met through ground coverage or by direct onboard interfaces in the Orbiter. The following considerations must be made for each case.

(a) RTM of safety parameters met through the use of onboard interfaces exclusive of the ground must use the Orbiter's failure detection annunciation (FDA) system to assure coverage during sleep periods and during operation of other payload systems.

(b) If ground coverage is used, a continuous real-time data link (containing safety parameters) must be assured during the required period. Communication interruption between the flight crew and the ground during these periods may require the safing of the payload. The payload has the obligation to immediately report any changes in configuration of its safety parameters to the NASA Mission Control Center.

(2) Near-Real-Time Monitoring (NRTM) is required to maintain visibility into the status of safety inhibits or systems on a periodic basis (nominally once per orbit). The intent of near-real-time monitoring is to periodically check the status of inhibits or systems which are either not planned for operations or do not pose an immediate hazard to the STS but must ultimately be controlled to prevent the occurrence of a hazard.

The NRTM requirements can be met through ground coverage or by direct onboard interfaces in the Orbiter. The following considerations must be made for each case.

(a) If the NRTM is to be met through ground coverage (without any onboard capability), then:

The payload must assure ground coverage is compatible with the response time for hazard control both in terms of data availability and communications with the Orbiter.

The payload has the obligation to immediately report any changes in configuration of its safety parameters to the NASA Mission Control Center. Crew notification during awake and sleep periods will be at the direction of the Flight Director.

(b) If the NRTM requirement is to be met through onboard interfaces exclusive of the ground, then:

The safety parameters which are required to be monitored per NHB 1700.7 must use the Orbiter's failure detection annunciation (FDA) to

assure coverage during sleep periods and during operation of other payload systems. The system shall be designed such that a change in status of any of these parameters shall activate the FDA (inputs to the FDA may be ganged if necessary). Specific system status may be determined from switch panel talkbacks in response to the FDA.

(3) Crew considerations for monitoring are as follows.

(a) Crew on Station support for RTM is seldom a problem because the crew is involved by the nature of these tasks (i.e., S&A arming, deployment systems, etc.).

(b) Crew on-station support for near real-time monitoring is more difficult to implement. If the user requires crew support to monitor payload systems periodically to meet the NRTM requirement, then he must negotiate crew procedures through the PIP annexes prior to final safety panel approval. During crew awake periods, monitoring functions which involve crew support will normally be approved unless the activity would conflict with other scheduled operations. During crew sleep periods, periodic crew monitoring of safety status onboard during sleep periods will not normally be approved.

(4) Monitoring via the Standard Switch Panel - Standard Switch Panel (SSP) talkback indicators may be used as monitors for the inhibits of a payload only during the operations of that payload unless special services have been negotiated with the STS. The SSP has no standard features for connection to the Orbiter FDA of telemetry systems for monitoring during crew sleep periods or during times when other tasks are being conducted. Payload must provide for a method of monitoring which gives notification of changes in status of monitored items.



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

Reply to Attn of :

JSC, TA-91-062

SEP 11 1991

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Payload Commanding

The information contained in this letter is an interpretation and clarification of the Space Shuttle Program (SSP) safety policy regarding controlling hazardous commanding to a payload during ground processing or flight operations from Payload Operations Control Centers (POCC's) and other ground equipment. This letter applies to all SSP payloads; i.e., payloads required to comply with either NHB 1700.7A or NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System (STS)," and will be utilized by the Space Shuttle flight and ground payload safety review panels in assessing compliance. The safety requirements being clarified are in paragraph 218 of NSTS 1700.7B, and in letter TA-87-050, "Payload Commanding Safety Requirements," which is levied on NHB 1700.7A payloads via paragraph n. of letter TA-87-079, "Resumption of Payload Safety Activity." Please add this letter to your copy of NSTS 18798A, "Interpretations of NSTS Payload Safety Requirements."

The safety policy in the above documents requires payloads to consider hardware failure modes and software errors in determining compliance with SSP failure tolerance requirements. However, failure modes and effects analyses (FMEA's) on the complex active computer systems, such as would be typically used in a POCC, are difficult to perform and are usually inconclusive with respect to determining failure tolerance. Consequently, the SSP has defined an optional alternative safety policy which does not require FMEA type assessments and will provide adequate control of the risks associated with POCC commanding due to hardware failures or software errors. The requirement to demonstrate appropriate failure tolerance to sending multiple hazardous commands due to procedural errors is not affected by this optional alternative safety policy and must still be met. The alternative policy is embodied in the enclosure to this letter entitled "POCC Certification Policy and Requirements."

A payload hazard report must be prepared by the SSP payload addressing the issuance of hazardous commands from a POCC or other ground equipment, regardless of whether or not a payload elects to demonstrate compliance to the alternative policy defined in this letter.

However, the SSP payload may negotiate with the POCC to have the POCC submit a generic hazard report documenting the POCC's compliance with SSP payload safety requirements. This would be a benefit to the POCC if it were a general purpose facility with multiple users. If a generic hazard report has been approved, the SSP payload, as a user of that facility, must reference the generic hazard report in the payload hazard report. The format of this generic hazard report would be as defined in Appendix A of NSTS 13830B, "Implementation Procedure for NSTS Payloads System Safety Requirements." The review and approval of such a generic hazard report may either be coordinated by the SSP payload or by the POCC directly with the SSP.

Questions regarding implementation compliance shall be directed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, mail code NS2, telephone (713) 483-4297.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.

Enclosure

Distribution: Payload Safety Distribution List

cc:

NASA Hqs., M/W. B. Lenoir  
M-7/R. L. Crippen

KSC, CM/J. T. Conway  
MK/B. H. Shaw, Jr.  
TM/J. F. Honeycutt  
TM/G. T. Sasseen  
TM/R.B. Sieck  
TP/J. F. Harrington III  
TV/J. R. Lang

MSFC, EA01/R. J. Schwinghamer  
SA01/J. N. Strickland  
SA21/J. W. Smelser  
SA31/G. C. Ladner  
SA41/C. H. Rutland  
SA51/V. K. Henson  
SA61/R. E. Mitchell  
SA71/J. M. Ellis

JSC, AC/D. A. Nebrig  
CA/D. R. Puddy  
CB/D. C. Brandenstein  
DA/E. F. Kranz  
DA2/T. W. Holloway  
EA/H. O. Pohl  
GA/L. S. Nicholson  
GA/J. H. Greene  
GA2/J. B. Costello  
GM/D. C. Schultz  
MJ/T. R. Loe  
NA/C. S. Harlan  
TA/Staff  
VA/D. M. Germany  
VA/J. C. Boykin  
WA/F. T. Buzzard

USAF SSD-Los Angeles, CLX/Lt. Col. W. LeCompte  
Rockwell-Downey, FC16/D. H. Frederick

Vitro Corporation  
Space Operations Center  
Attn: Mr. O. W. Kenton  
400 Virginia Ave., SW, Suite 825  
Washington, DC 20546

Aerospace Corporation  
Attn: M5-468/H. De La Puente  
M6-209/K. R. Morrison  
P.O. Box 92957  
Los Angeles, CA 90009

## **POCC CERTIFICATION POLICY AND REQUIREMENTS**

THE RISK OF INADVERTENTLY TRANSMITTING MULTIPLE HAZARDOUS COMMANDS AS A RESULT OF HARDWARE FAILURES AND/OR SOFTWARE ERRORS MUST BE REDUCED TO AN ACCEPTABLE LEVEL BY DEMONSTRATING EQUIVALENCE WITH THE FOLLOWING SET OF POCC PROTECTION REQUIREMENTS AND POCC USER REQUIREMENTS:

### **A. POCC PROTECTION REQUIREMENTS**

#### **1. HARDWARE FAILURE/SOFTWARE ERROR DETECTION:**

A software application program must be implemented that monitors the status of the hardware and software components, detects failures, issues error messages to the operator, and terminates command operations. Command operations must be suspended until the error is either resolved or a substitute component is brought on line.

#### **2. COMMAND HARDWARE/SOFTWARE VALIDATION AND CONFIGURATION CONTROL:**

Hardware/software validation shall be performed in order to establish that the hardware/software requirements have been implemented in the command system properly. A software requirements validation shall be performed by personnel not involved in the development of the software.

Following validation, all command system hardware and software elements shall be maintained under formal configuration control. Any change to any hardware/software element of the system configuration shall require additional validation.

#### **3. DATA TRANSFER ERROR DETECTION:**

Software checks must be performed when a command is retrieved from internal or external storage to verify that no data corruption has occurred.

#### **4. SAFING CAPABILITY:**

All hazardous commands must be "safed" (i.e., be identified in the data base such that software will recognize the command as hazardous). The system must ensure that a "safed" command cannot be enabled for uplink until the requirements for processing such a command are satisfied (i.e., the command is unsafed).

## **B. POCC USER REQUIREMENTS**

1. All hazardous commands must be identified in the command data base supplied to the POCC.
2. All commands in the final data base will be checked against the Payload Integration Plan Annex 3 defined hazardous commands list for verification of proper safing. A list of all "safed" commands will be provided to the Annex 3 Book Manager after the data base is certified.
3. Hazardous commands blocks shall be designed to remove no more than one inhibit to a single hazardous function.
4. "Chained" type commands will contain no hazardous commands unless command checking capability is implemented and will terminate chain operations if a "safed" command is detected within the chain. Hazardous "chained" commands shall be designed to remove no more than one inhibit to a single hazardous function.
5. The POCC user must implement a system and procedures for real-time monitoring of all related safety telemetry during command activity. These procedures must allow sufficient time between each command to terminate commanding, if necessary, before transmission of a subsequent command.
6. The POCC user must ensure no command can change to a hazardous command due to a single bit error during transmission (e.g., spacecraft command error detection or command bit structure restrictions).

National Aeronautics and  
Space Administration  
**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of :

MA2-99-170

February 11, 2000

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/Deputy Manager, International Space Station Program

SUBJECT: Crew Mating/Demating of Powered Connectors

The information contained in this letter is an interpretation and clarification of the safety policy. This letter will be utilized by the Payload Safety Review Panel (PSRP) in assessing payload design compliance in accordance with either National Space Transportation System (NSTS) 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System," paragraph 200.1 or NSTS 1700.7B Addendum "Safety Policy and Requirements for Payloads Using the International Space Station (ISS)," paragraph 200.1. This letter replaces MA3-97-093, Subject: Crew Mating/Demating of Powered Connectors, dated March 17, 1998. Please add this letter and updated index to your copy of NSTS/ISS 18798B, "Interpretations of NSTS/ISS Payload Safety Requirements." Rationale associated with this interpretation letter is in italics for reference purposes and is intended to capture the key technical considerations utilized by the PSRP in the development of this policy. This rationale has been documented in order to permit the PSRP and the payload customer to consistently interpret this policy.

This letter is intended to clarify the safety policy regarding the design provisions required when electrical connectors must be mated or demated during extravehicular activity (EVA) or intravehicular activity (IVA). The specific approach is to eliminate potentially hazardous energy levels at the connector interface during mating/demating operations by limiting the energy of the power source or by isolating power sources from the connector. The design must prevent generation of molten metal, electrical shock, and damage to safety critical circuits.

*The PSRP's assessment of the hazards associated with mating/demating defined three concerns.*

1. *Generation of molten metal*
2. *Electric shock (only applies IVA; the extravehicular mobility unit (EMU) provides electrical isolation)*
3. *Damage to safety-critical circuits (protected by the requirement to maintain separation per NSTS 1700.7B, paragraph 207)*

*The hazard level for each of these concerns is catastrophic.*

The mating and demating of low-power connectors (IVA or EVA) is permissible without upstream inhibits or special connector design features. Low-power connections are defined



as those with design features that have power supply capacity or upstream circuit protection that limit maximum continuous current to 3 ampere or less with an open circuit voltage no greater than 32 volts (root-mean-square (RMS) or direct current (DC)). If the connector circuit does not meet this criteria, then the following paragraphs apply:

Note: In the low-power case, computer or operational control of the upstream circuit protection device is not allowed; it must be controlled by hardware design. However, a disconnected cable does satisfy the intent of limiting the upstream power capacity and is an acceptable operational solution.

*Test data (EP5-T51-015) associated with a 22 American Wire Gage (AWG) connector (smallest pin size expected) indicates that the first arcs occur from 1.5 ampere to 3.8 ampere (average is 3) at 33 volts. The smallest pin sizes that were considered were 22 AWG. This criteria should not be used for smaller pins. The low-power connection is based on upstream hardware design features that limit the voltage and current to the values specified for each contact in the connector. Typically, the circuit protection devices that satisfy the maximum continuous current criteria are rated at 2 ampere (e.g., 145 percent of rated current for orbiter circuit breakers). TM 102179 defines the capability (maximum blow) of current limiting devices (such as a circuit breaker). The downstream design is not a factor in this determination. Sustained arcs are the major concern. We accept the risk of momentary exceedences of this limit based on the speed of the circuit protection device. The payload interfaces provided by the orbiter or ISS do not satisfy the low-power criteria.*

1. The design features described below are required for all IVA connectors/circuits with a maximum continuous current of greater than 3 ampere with an open circuit voltage no greater than 32 volts (RMS or DC) (40 volts DC for batteries that are inserted directly into an enclosure) that may require mating/demating. Battery charger connectors will be assessed on a case-by-case basis.

*Medical Operations concurs that 30 volts DC is generally agreed to be the actual threshold for shock hazards (e.g., heart fibrillation). It was further determined that for voltages below 32 volts, no credible shock hazard exists based on the population at risk that NASA has identified applicable to this criteria (documented in TA-94-029). This letter extends the 30-volt criteria to 32 volts DC, with Medical Operations concurrence, based on the accepted risk of considering a subset of the astronaut population which excluded more than the lower 0.5 percentile of the cohort. The concerns with electrical shock are associated with providing a current path across the heart (see Appendix Y of JSC 20483). The primary design feature that keeps a person from "being shocked" is good insulation and a connector design, which minimizes or prevents accidental exposure to voltages greater than 32 volts DC.*

*The PSRP has chosen to extend the 32-volt DC limit criteria set by Medical Operations to 40-volt DC for batteries, because the hazard level is critical for the population at risk and because the hand-to-hand resistance values are sufficiently high enough to reasonably reduce the risk of fibrillation at or below 40 volts. The PRSP considers this a valid assumption for batteries because battery installation results in hand-to-hand contact only. Considering this assumption and data from NASA Standard 3000, Volume 1, Section 6.4.3, the threshold for 40 volts is derived. The calculation is:  $1000\ \Omega$  (based on hand-to-hand contact) \* 40 milliamperes (let-go threshold current based on 99.5 percentile rank of adults) = 40 volts. In other words, in this potential contact configuration and at this voltage and current range, this is a critical rather than catastrophic shock hazard. Therefore, the connector design features are sufficient (without an upstream inhibit) to control this hazard. As a result of the concern for redesigning all batteries, exceeding the 32-volt criteria (documented in TA-94-029) but staying within the extended 40-volt criteria, in this case, was deemed to be acceptable by the PSRP for the reasons outlined above.*



- a. Each powered circuit shall have at least one verifiable upstream inhibit. The design shall provide for verification of the inhibit status at the time the inhibit is inserted. An additional upstream inhibit is required when the short circuit current is greater than 65 amperes.

*In this case, the molten metal generation concern is controlled by an upstream inhibit. A downstream break in the circuit (downstream inhibit) or reduction of load is also acceptable if the concerns associated with a short at the connector are addressed. A reduction of load upstream is addressed by the low power criteria. Since connector testing has shown that 67 ampere at 33 volts is the threshold for significant damage to sockets, 65 ampere was chosen as the limit for connector shells. Therefore, a more stringent requirement is imposed for circuits in excess of this value.*

- (1) When payloads have a power supply capacity or upstream circuit protection that limits the short-circuit current to be less than the single wire strand melting current, a reduction of current draw to less than 3 amperes on the downstream side can be used instead of an upstream inhibit. If the melting current value is approached, the power supply or upstream circuit protection must remove all power from the connector within 5 seconds (e.g., an orbiter circuit breaker can deliver 300 percent of rated current for 5 seconds before tripping.) The single wire strand melting current value is :

5.1 ampere for 22 AWG wire/pin,

7.2 ampere for 20 AWG wire/pin,

10.2 ampere for 18 AWG wire/pin, or

12.3 ampere for 16 AWG wire/pin and larger wire/pin sizes

*The amperages listed for the different wire/pin sizes are based on the fusing or melting current of one strand of the wire. Due to the possible variations in a heat sink to remove heat from the heating strand and the wire initial temperature, etc., these amperages are "ballpark values." If a strand of the wire became separated from the main wire and shorted, it would have the main wire to use as a heat sink. Also, if the fusing current were reached, some time would pass before the strand heated to the melting temperature. Considering the above data and the possible modes envisioned for the orbiter, the 5 seconds is based on engineering judgment (and Shuttle Operational Data Book, Volume 3, Figure 4.5.6.4-1) that more than 5 seconds would be required to cause molten metal (the concern is getting molten metal in the crew's eye). Any circuits above this threshold must have an upstream inhibit. This criteria is to be applied to all connections including batteries with cables.*

- (2) When battery connectors/circuits have a power supply capacity that limits the short-circuit current to less than 20 ampere within 0.5 seconds, a reduction of current draw to less than 3 ampere on the downstream side can be used instead of an upstream inhibit. This higher threshold only applies to batteries or battery boxes that are inserted directly into an enclosure.

*At 20 ampere, we no longer have confidence that the shroud alone is acceptable. In this case, a higher current threshold is chosen because the upstream circuit protective device (e.g.,*

*polyswitches) are quick enough to satisfy this requirement. Without a circuit protection device, the determination of upstream capacity is based on the battery itself. This requirement encompasses most of the off-the-shelf batteries in general use (we initially considered approximately 600 watts to be the threshold based on the pistol grip tool battery). The 0.5-second number is based on engineering judgment that the energy (heat) would be sufficiently limited if the current dropped within the 20-ampere limit within 0.5 second. Especially when considering batteries, the initial short duration current delivering properties of even small batteries is relatively high, but the current should decrease rapidly.*

Note: Input electromagnetic interference (EMI) filters upstream of the switching device which removed the downstream load above may cause transient exceedances of the 3-ampere limit until the capacitors are charged in the input EMI filter. This type of design is acceptable if the input filter energy storage capability is no greater than that allowed in the enclosed Energy Storage Calculation chart for the corresponding connector pin gauge.

- b. Connectors shall employ design features that completely enclose or shroud the pins and sockets during making/breaking of electrical contact.

*The primary design feature that keeps a person from being injured by molten metal is the connector design. The pin/sockets separate before the shell is opened. The mechanical retention feature or "key-way" provided by most connectors also prevents the crew from easily opening the connector by pulling on it if they reflexively respond to a short.*

- c. The connector design must provide protection of the powered side from debris/inadvertent shorting when unmated or when mating/demating (e.g., terminated in sockets rather than pins).

*This design feature is required so that inadvertent shorting is precluded when the connector is unmated or exposed to the crew. It is also in place so that the risk of a bent pin causing a short during mated/demate operations is minimized.*

2. The design features described below are required for all IVA connectors/circuits with an open circuit voltage greater than 32 volts (RMS or DC) (40 volts DC for batteries) that may require mating/demating. Battery charger connectors will be assessed on a case-by-case basis.

*It was determined that no shock hazard exists for voltages below 32 volts (documented in TA-94-029). The concerns with electrical shock are associated with providing a current path across the heart (see Appendix Y of JSC 20483). Good insulation is the primary design feature that keeps a person from "being shocked."*

- a. Each powered circuit shall have at least one verifiable upstream inhibit. The design shall provide for verification of the inhibit status at the time the inhibit is inserted. An additional upstream inhibit is required when the open circuit voltage is greater than 200 volts (RMS or DC) or when the short-circuit power/current is greater than 65 amperes or 8200 watts.

*Ground fault interrupts (GFI's) are now required in homes and offices when there is a credible hazard of a circuit path through the individual to ground (this is the closest analogy to the IVA space environment). In the kitchen or bathroom or outside outlets, there is a credible situation where an individual could be part of an unplanned return path (e.g., wet or touching a metal, grounded fixture or appliance). In those situations, the new codes require the use of GFI's. As a parallel to this, an upstream inhibit is required in the zero-gravity environment so that a fault is precluded (another level*

of control for molten metal also). The use of ground fault circuit interrupts (GFCI's) (the Space equivalent of GFI's) is not allowed to substitute for an upstream inhibit because of concerns associated with molten metal since the current is not sufficiently limited. However, the use of GFCI's is prudent and encouraged because it provides additional shock hazard protection. Verification of the upstream inhibit is required since the configuration of the system is changed to support mating and demating operations. In this case, one-time verification is used instead of near real-time monitoring since it is expected that the mating and demating operation will take place shortly after the inhibit is inserted. The requirements associated with the design of the monitor (NSTS 1700.7B, paragraph 201.1C) is still applicable (e.g., monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible. Monitor circuits shall be current limited or otherwise designed to prevent operation of the hazardous functions with credible failures.) Since connector testing associated with mating and demating of powered connectors has only been performed up to 173 volts and 100 amperes, a more stringent requirement is imposed for connectors with an open circuit voltage above 200 volts (extrapolation based on existing test data). The maximum contact fail current, based on testing, was not chosen because the required controls associated with the upstream inhibit and the connector shell provide sufficient protection up to this limit and beyond. An 8200-watt limit (65 amperes at 126 volts) was selected based on the capabilities of the Space Station Direct Current-to-Direct Current/Converter Unit.

- b. Connectors shall employ design features that completely enclose or shroud the pins and sockets during making/breaking of electrical contact.

*This also provides an additional control of containment. During ground processing, we require all connectors for energized mates to be of a scoop-proof design so that a partial inadvertent mismatch will not provide a pin-to-pin contact (lesson learned from the Magellan battery fire at KSC several years ago).*

- c. The connector design must provide protection of the powered side from debris/inadvertent shorting when unmated or when mating/demating (e.g., terminated in sockets rather than pins).
  - d. When mating/demating recessed connectors (e.g., connectors attached to equipment remote from the crew such as back-of-the-rack when the connectors are mated/demated), a design feature for grounding of the case shall be maintained while mating/demating the powered pin/sockets.
  - e. Payloads that are reconfigured on orbit, such that their fault bond is disturbed during mate/demate operations, shall comply with interpretation letter MA2-99-142, Subject: On-orbit Bonding and Grounding.
3. The design features described below are required for all EVA connectors/circuits that may require mating/demating. The installation of batteries during EVA is outside the scope of this letter and will be assessed on a case-by-case basis.

*The PSRP's initial review focus was associated with EVA activities (in support of the Hubble Space Telescope payload). It was determined that electrical shock is not a hazard while in the EMU because there is no conductive path to the crewmember. The overriding concern is the molten metal generation as a result of an arc. This molten metal can compromise the integrity of the EMU or potentially ignite the materials in the suit exposed to the 100 percent oxygen environment (Hamilton Standard has stated that any molten metal on the suit is unacceptable). Due to the rarity of EVA battery installations, and the complexity that would be added to this letter, the subject is excluded from this letter and will be considered on a case-by-case basis.*

- a. Each powered circuit shall have at least two inhibits. At least one of these inhibits must be upstream which removes voltage from the connector. The other design feature shall provide either:
  - (1) An additional inhibit upstream of the connector or
  - (2) Reduction of power/current draws to the lesser of 180 watts or 3 amperes (when payloads have design features that limit the voltage across the connector to less than 200 volts).

The design shall provide for verification of at least one of the upstream inhibits at the time that it is inserted.

*A series of tests were managed by the Engineering Directorate. The theory associated with this subject is that the potential to arc is a function of available power and the sharpness of the pins. Since other tests have been performed with inconsistent results and the phenomenon is not fully understood (consistent sharpness is difficult to establish), the latest testing shows that contacts begin pitting at 1.5 amperes and 123 volts for 22-AWG pins or 184.5 watts. Based on this data, the 180-watt limit was chosen as a conservative value for this interpretation. Test data (EP5-T51-015) associated with a 22-AWG connector (smallest pin size expected) also shows that minimal damage occurs from 1.5 ampere to 3.8 ampere (average is 3) at 33 volts. Therefore, for higher voltages, the limit is based on power, and for lower voltages, the limit is based on current. An adequate margin of safety is in place because the limits are set based on initiation of pitting or contact damage rather than the contact fail threshold. Additionally, the limits are also set based on the smallest pin size, which is rarely used in EVA applications. Since connector testing associated with mating and demating of powered connectors has only been performed up to 173 volts, a more stringent requirement is imposed for connectors with an open circuit voltage above 200 volts (extrapolation based on existing test data). Concerns about corona in proximity to the suit were considered and dismissed because the worst case pressure buildup is below the corona pressure threshold.*

Note: Input EMI filters upstream of the switching device which removed the downstream load in (2) above may cause transient exceedances of the limit identified in (2) until the capacitors are charged in the input EMI filter. This type of design is acceptable if the input filter energy storage capability is no greater than that allowed in the enclosed Energy Storage Calculation chart for the corresponding connector pin gauge.

- b. Connectors shall employ design features that prevent pin damage and/or inadvertent pin contact due to misalignment, e.g., keyed scoop-proof connectors.
- c. The connector design must provide protection of the powered side from debris/inadvertent shorting when unmated or when mating/demating (e.g., terminated in sockets rather than pins).

A flight rule may be imposed which is not favorable to the mission success of the payload (e.g., terminated connector operations) if the design features only support the minimal configuration defined in this letter.

*Flight rules will be prepared for each mission that outline preplanned decisions designed to minimize the amount of real-time rationalization required when anomalous situations occur. These flight rules are not additional safety requirements but do define actions for completion of the flight consistent with crew safety. These flight rules are based on the design features that still function in the system to preclude a hazard. If only the minimal configuration defined in this letter is provided, the operations flexibility (e.g., continued operations in the presence of failures) may be limited so that a flight rule is developed that is contrary to a payload's mission success (a required connector may not be mated or demated).*

Questions concerning this subject should be directed to the PSRP Executive Secretary, Michael Ciancone, at (281) 483-8848.

**Original Signed By:**

William H. Gerstenmaier

**Original Signed By:**

Jay H. Greene

2 Enclosures

Distribution:

CB/G. D. Griffith  
DO12/J. M. Childress  
EA4/R. J. Wren  
MS3/K. B. Packard  
NC4/M. L. Ciancone  
OE/S. L. Thomas  
OZ3/D. W. Hartman  
SD2/M. E. Coleman

cc:

See List

cc:

AE/J. F. Whiteley  
CA/J. D. Wetherbee  
CB/C. J. Precourt  
DA/B. R. Stone  
EA/L. S. Nicholson  
EA4/J. W. Aaron  
MA/R. D. Dittimore  
MA2/A. M. Larsen  
MG/R. H. Heselmeyer  
MM/J. B. Costello  
MQ/M. D. Erminger  
MS/L. D. Austin, Jr.  
MT/R. M. Swalin  
MV/R. R. Roe, Jr.  
NC44/P. L. Mitchell  
OA/T. W. Holloway  
XA/G. J. Harbaugh  
HQ/M-4/W. M. Hawes  
HQ/M-7/S. R. Nichols  
HQ/M-7/N. B. Starkey  
HQ/MO/R. L. Elsbernd  
KSC/AA-C/L. J. Shriver  
KSC/MK/D. R. McMonagle  
KSC/MK-SIO/R. L. Segert

## ENERGY STORAGE CALCULATION

Energy storage is calculated using the following equation:

$$E = \frac{1}{2} C V^2$$

Where: E = Energy (Joules)  
 C = Input line to line capacitance  
 V = Line voltage maximum.

Connector Pin Gauge	Allowable EMI Filter Stored Energy E
4	49.0
8	20.5
10	13.0
12	8.0
14	4.9
16	3.0
18	2.0
20	1.3
22	0.8

National Aeronautics and  
Space Administration  
**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of :

MA2-96-190

JAN 09 1997

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration

SUBJECT: Contingency Return and Rapid Safing

The information contained in this letter is an interpretation and clarification of the payload safety requirements of NHB/NSTS 1700.7, "Safety Policy and Requirements for Payloads Using the Space Transportation System." This letter will be utilized by the Space Shuttle Payload Safety Review Panel (PSRP) in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretations of NSTS Payload Safety Requirements," as applicable against NHB 1700.7A and NSTS 1700.7B. Enclosed is an updated table of contents for NSTS 18798A.

Three previous interpretation letters have been issued to define times allocated for rapid safing of payloads as required by NHB/NSTS 1700.7 paragraph 205, "Contingency Return and Rapid Safing." This letter supersedes and replaces letters TA-88-025, "Policy Letter on Rapid Safing," dated May 16, 1988; TA-89-085, "Policy on Spacelab Module Rapid Safing," dated April 2, 1990; and MA3-94-020, "Contingency Return and Rapid Safing," dated January 13, 1995. This letter addresses the time allocated for safing payload hardware in the payload bay, orbiter crew cabin, Spacelab and other crew habitable payload modules, and module interconnecting transfer tunnels.

All payloads must be safe for aborts and contingency return of the orbiter and shall include design provisions for rapid safing to ensure the capability to safe the payload for payload bay door (PLBD) closure and deorbit. If during planned payload operations an element of the payload or its airborne support equipment is deployed, extended, or otherwise unstowed to a condition where it violates the PLBD envelope or cannot withstand subsequent Space Shuttle induced loads, there shall be design provisions to safe the payload in a time-critical manner. Since payloads must always provide two-fault tolerance with respect to preventing PLBD closure and assuring a safe return configuration, and extravehicular activity can only be used as the third method, the issue becomes one of ensuring the first two methods, or redundant systems, are compatible with the time constraints for the contingency scenarios addressed in paragraphs 1 and 2. For the scenarios described in paragraphs 3, 4, and 5, the payload rapid safing design provisions shall ensure one method which has reliable design features/operations verified by test in accordance with design to minimum risk criteria.

1. EMERGENCY DEORBIT. Approximately 20 minutes is allocated for all payload safing functions required to clear the PLBD envelope for this scenario. The payload



shall provide one method which is capable of meeting the emergency deorbit time limit. If the orbiter Remote Manipulator System (RMS) is in use by the payload, only 10 minutes will be available for the payload element on the RMS to perform all safing functions required to clear the PLBD envelope. (Approximately 10 minutes must be allowed for nonpayload RMS operations.) Additionally, all payload elements in the cargo bay shall establish a safe return configuration (i.e., provide a minimum 1.4 ultimate factor of safety as defined in NHB/NSTS 1700.7 paragraph 208 for entry/landing loads) no later than 30 minutes after the emergency is declared.

For payloads that violate the PLBD envelope while docked to the Mir or the International Space Station (ISS) approximately 1:45 hours is allocated for all safing functions required to clear the PLBD envelope for this scenario. The payload shall provide one method which is capable of meeting the emergency deorbit time limit. If the orbiter RMS is in use by the payload, only 1:35 hours will be available for the payload element on the RMS to perform all safing functions required to clear the PLBD envelope. Additionally, all payload elements in the cargo bay, while docked to the Mir or ISS, shall establish a safe return configuration (i.e., provide a minimum 1.4 ultimate factor of safety as defined in NHB/NSTS 1700.7 paragraph 208 for entry/landing loads) no later than 1:45 hours after the emergency is declared.

2. **NEXT PRIMARY LANDING SITE.** Approximately 1:45 hours is allocated for all payload cargo bay safing functions required to clear the PLBD envelope and establish a safe return configuration for this scenario. The payload design shall provide single-fault tolerance for safing the payload within this time constraint. The emergency deorbit system can be used to satisfy this requirement provided it is single-fault tolerant, or an additional method can be used; i.e., two methods available at the start. If the orbiter RMS is in use by the payload, only 1:35 hours will be available to the payload element on the RMS to perform all safing functions required to clear the PLBD envelope. NSTS 16979, "Shuttle Orbiter Failure Modes and Fault Tolerances for Interface Services," specifies the fault tolerance of orbiter-provided payload services when utilized in conjunction with payload systems (e.g., the RMS is zero-fault tolerant).
3. **ORBITER CABIN PAYLOAD EQUIPMENT.** All crew cabin payload hardware, which is not capable of withstanding subsequent Space Shuttle induced entry/landing loads in its on-orbit operation configuration, shall be designed for rapid safing. Approximately 50 minutes is allocated to reconfigure crew cabin hardware to a safe return configuration.
4. **EMERGENCY MODULE DEACTIVATION.** Penetration of the Spacelab or a crew habitable payload module pressure hull or ingress tunnel is a catastrophic hazard. All payload elements, which because of their mass and/or shape are capable of penetrating the module as a result of subsequent Space Shuttle induced entry/landing loads, shall provide a safe return configuration. Additionally, payload elements which are a penetration hazard shall provide for rapid restraint by tether or other rapid safing provisions during periods of on-orbit reconfiguration by the crew.

Up to 3 minutes is allocated for rapid payload safing during an emergency module deactivation. Flight crew safing operations may be implemented only when the crewmember is utilized as an active operator of payload element hardware (i.e., one crewmember is in the module for each reconfiguration required).

When the crewmember is utilized as a test subject, up to 30 seconds is allocated for flight crew egress from experiment apparatus.

5. EQUIPMENT TRANSFER. Flight crew operations may be used to transfer equipment between interconnected habitable modules. An emergency requiring the crewmembers to rapidly return to the orbiter shall not result in transfer equipment which is a penetration hazard remaining unsecured during entry/landing. Penetration of a habitable module pressure hull, airlock, orbiter docking system (ODS) or interconnecting tunnel(s) is a catastrophic hazard. All transfer equipment, which because of its mass and/or shape is capable of penetrating a module, airlock, ODS, or interconnecting tunnel as a result of subsequent Space Shuttle induced entry/ landing loads if left unsecured, shall be capable of establishing a safe return configuration within 3 minutes (unsecured stowage in the airlock or ODS is precluded). Items in transit having penetration potential shall be limited in number such that the cumulative stowage time does not exceed 3 minutes.

Determination of the payload's design compliance with the time limits imposed for the scenarios addressed in paragraphs 3 and 5 must be made by the payload organization and confirmed by Space Shuttle Mission Operations Directorate personnel.

Questions concerning this subject should be directed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, Mail Code NS2, telephone (281) 483-4297.

**ORIGINAL SIGNED BY :**

Richard N. Richards

Enclosure

Distribution:

Payload Safety Distribution

cc:

HQ/M-4/A. M. Allen

MA2

HQ/M-7/S. S. Oswald

HQ/ME/H. L. Smith

KSC/GK3/W. B. Owens

KSC/MK/L. J. Shriver

KSC/MK/W. I. Wiley

KSC/MK-SIO/R. L. Segert

KSC/PH/J. F. Harrington

MSFC/EJ41/J. A. Jones

MSFC/JA01/C. S. Griner

MA2/RLBlount:KM:12/13/96

National Aeronautics and  
Space Administration  
**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of :

MA2-00-038

July 31, 2000

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/Deputy Manager, International Space Station Program

SUBJECT: Interpretation of On-Orbit Maintenance

The information contained in this letter is an interpretation and clarification of the safety policy. This letter will be utilized by the Payload Safety Review Panel (PSRP) in assessing payload design compliance in accordance with either of National Space Transportation System (NSTS) 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System," or NSTS 1700.7B International Space Station (ISS) Addendum, "Safety Policy and Requirements for Payloads Using the ISS," paragraph 215.3. Please add this letter and updated table of contents to your copy of NSTS/ISS 18798B, "Interpretations of NSTS/ISS Payload Safety Requirements."

This letter clarifies the design provisions required for on-orbit payload maintenance. The PSRP has previously required payload hazard analysis to review the nominal sequence of events, demonstrating that the necessary levels of failure tolerance are maintained throughout. However, the lengthening operational duration for payloads increases the likelihood that they will require on-orbit repair. Preserving the option to perform in-flight maintenance necessitates a hazard assessment of potential maintenance activities. Unlike the approach for other payload hazard analysis (which employ nominal procedure or timeline assessments), a maintenance hazard assessment should be generic; it should focus on controlling hazards that result from access to nominally inaccessible components rather than attempting to exhaustively address specific maintenance procedures. The hazard assessment must also address the use of flight spare components.

This letter also includes supporting rationale (in italics) for reference purposes; it is intended to define the technical considerations that prompted development of this policy. This rationale has been documented to facilitate consistent understanding of this policy.

*The PSRP seeks to ensure that the safety assessment is complete and accurate. The PSRP provides real-time assistance addressing safety concerns and provides recommendations to program management as necessary.*

#### **Assessment Topics**

1. Safe Access - This assessment should address all potential access paths for contact hazards (such as sharp edges, accessibility, touch temperature, stored energy, and electrical shock) that may be present during maintenance activities.

*The assessment must address all potential access paths and all potential contact hazards for each of these access paths. It must identify any constraints associated with special handling, cool down times, or separating connectors. The requirements of paragraph 200 still apply; the need for maintenance should not be counted as one failure.*

2. Modification of Existing Safety Features - This assessment should address hazards that maintenance activities can create (for example, contamination). This includes establishing why the maintenance tasks are safe to perform and why it is acceptable to defeat any hazard controls during maintenance activities.

*Depending on the complexity of the payload, the payload organization should use established analytical techniques as described in NSTS/ISS 13830, paragraph 4.1.2 to include fault tree, failure mode and effects analysis, etc. as required.*

*Hazard controls or verifications affected by maintenance in a particular area or access path must be addressed. This should include rationale supporting why modifying an existing safety feature is acceptable, clarifying how the hazard is eliminated, or what provisions are substituted for the safety features during the maintenance timeframe.*

3. Reverification of Safety Critical Features - This assessment should address the approach to verification or reverification of safety critical features that may be modified during maintenance and that will be required during subsequent operations.

*All hazard controls and verifications that could be affected by performing maintenance in a particular area or access path must be reestablished and reverified. Reference interpretation letter, MA2-98-135, Verification/Reverification Requirements for On-Orbit Payloads.*

Note: The crew will perform a general inspection (photo documentation) of all visible hardware (for example, wires, foam) during maintenance.

*Long-duration activities, such as ISS missions, do not permit the routine inspections that are normally performed on the ground. Any opportunity should be taken for photo documentation or inspection of a given area when access is provided.*

If a payload organization chooses not to perform a maintenance hazard assessment, a flight rule will be imposed that precludes on-orbit maintenance for that payload.

*Flight rules will be prepared for each mission that outline preplanned decisions designed to minimize the amount of real-time rationalization required when anomalous situations occur. In this case, logistical constraints limit the ability of the PSRP and mission management to implement real-time assessments, and a considerable amount of time (on the order of weeks) may be needed to schedule support in the control center. These flight rules are not additional safety requirements but define actions the operations community plan to take if a maintenance hazard assessment is not performed.*

## **Data Submittal Requirements**

1. The Phase I Safety Data Package (SDP) shall include a preliminary on-orbit maintenance safety assessment.

MA2-00-38

3

2. The Phase II SDP shall include a detailed on-orbit maintenance safety assessment that identifies maintenance activities, safe access areas, and reverification of safety critical features.

3. The Phase III SDP shall include a final, updated maintenance safety assessment.

Questions concerning this subject should be directed to the Executive Secretary, PSRP, JSC/NC4, at (281) 483-8848.

***Original Signed By:***

William H. Gerstenmaier

***Original Signed By:***

Jay H. Greene

Enclosure

Distribution:

CB/G. D. Griffith  
DO12/J. M. Childress  
EA44/R. J. Wren  
MA2/A. M. Larsen  
MA2/D. E. O'Brien  
MA2/D. W. Whittle  
MA2/J. G. Williams  
NC4/M. L. Ciancone  
NC55/SAIC/E. J. Conner  
NE2/G. L. Priest  
OZ3/D. W. Hartman  
SD2/M. E. Coleman  
USA/USH-700D/H. A. Maltby

cc:

See List

MA2-00-38

4

cc:

AE/J. F. Whiteley  
 CA/J. D. Wetherbee  
 CB/C. J. Precourt  
 DA/B. R. Stone  
 EA/F. J. Benz  
 EA4/D. A. Hamilton  
 KN/NASDA/T. Akutsu  
 LM/I. M. Dornell  
 MA/R. D. Dittmore  
 MG/R. H. Heselmeyer  
 MM/J. B. Costello  
 MQ/M. D. Erminger  
 MS/L. D. Austin, Jr.  
 MS3/D. L. Ladrach  
 MS3/K. B. Packard  
 MT/R. M. Swalin  
 MV/R. R. Roe, Jr.  
 NC44/M. L. Mudd  
 OA/T. W. Holloway  
 OR/CSA/H. L. Williams  
 OT/ESA/U. J. Thomas  
 XA/G. J. Harbaugh  
 HQ/M-4/W. M. Hawes  
 HQ/MO/S. R. Nichols  
 HQ/M-7/N. B. Starkey  
 KSC/EC-G1/J. C. Dollberg  
 KSC/MK/W. H. Gerstenmaier (Acting)  
 KSC/MK-SIO/R. L. Segert  
 USA/USH-700D/L. Lo

T. Sgobba  
 T. Heimann  
 ESTEC-GPQ  
 P. O. Box 299 NL  
 2200 AG, Noordwijk  
 The Netherlands

H. Hasegawa  
 Space Station Safety and Product  
 Assurance Office  
 NASDA  
 Tsukuba Space Center  
 2-1-1 Sengen  
 Tsukuba-shi, Ibaraki  
 Japan 305

P. Vorobiev  
 RSC Energia  
 4a Lenin Street  
 Korolev  
 141070 Moscow Region  
 Russia

P. M. Jean  
 Manager, Safety and Product  
 Assurance  
 Space Station Program  
 Canadian Space Agency  
 6767 route de l'Aéroport  
 Saint-Hebert, Quebec  
 Canada J3Y 8Y9

MA2/AMLarsen:cdm:04/25/00:31207

Retyped: MA2/AMLarsen:cdm:06/22/00:31207

CONCUR	CODE >	MA2/AML	MS/LDA	MT/RMS					
	INITIALS >								
	DATE >								

NASA FORM 1267 FEB 79 PREVIOUS EDITIONS MAY BE USED (WINWORD Mar 93)

OFFICIAL FILE COPY

## **5. PRESSURE**

<u>Title</u>	<u>JSC Letter Number</u>
5.1 Fault Tolerance of Systems using Specially Certified Burst Disks	TA-88-074
5.2 Pressure Stabilized Tanks	TA-89-064



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

OCT 18 1988

Reply to Attn of :

NSTS-JSC, TA-88-074

TO: Distribution

FROM: NSTS-TA/Manager, NSTS Integration and Operations

SUBJECT: Fault Tolerance of Systems Using Specially Certified Burst Disks

The information contained in this letter is considered an interpretation or clarification of the payload safety requirements of NHB 1700.7 and will be utilized by the Safety Review Panel in assessing payload design compliance. Please add this letter to your copy of NSTS 18798 (Interpretations of STS Payload Safety Requirements) as being an applicable interpretation against NHB 1700.7A and NHB 1700.7B when issued.

The NSTS Payload Safety requirements dictate that hardware controlling pressure in pressurized systems be collectively two-fault tolerant from causing the pressure to exceed maximum design pressure (MDP) while the payload is associated with the NSTS Orbiter. This requirement is specifically documented in the NHB 1700.7B. Several payload organizations have requested that a properly designed and certified burst disk assembly be considered equivalent to two relief devices when meeting this requirement.

The preferred burst disk design for payloads is one which employs a reversing membrane against a cutting edge to assure rupture. Historical use and experience indicate that a burst disk of this type can be certified as a highly reliable pressure relief device. When a burst disk of this type is used as the second and final control of pressure, the two-fault tolerant requirement may be assessed as having been met if the burst disk meets the following requirements:

- a. The design does not employ sliding parts or surfaces subject to friction and/or galling. In addition, special attention shall be given to the use of stress corrosion resistant materials, particularly in parts under continuous load such as Bellville springs.
- b. The design used must be qualified for the intended application by test data applicable to the intended use conditions including temperature and flow rate.
- c. Qualification must be for the specific part number used, and it must be verified that no design or material changes exist between flight assemblies and assemblies making up the data base.



d. Each flight assembly shall be verified for membrane actuation pressure by use of special tooling or a procedure to prevent cutting edge contact during the test. If this is not feasible, demonstration of good materials and processes control and a rigorous lot screening program approved by the NSTS Payload Safety Review Panel are required.

Identification of qualification and test information for certification of a burst disk shall be included with the hazard report covering pressurization of the system or component to be protected by the burst disk. Approval of the hazard report will constitute acceptance of the burst disk as meeting the specified requirements. Payloads wishing to employ this option are encouraged to provide supporting information as early as possible so that a timely evaluation can be made and any problems resolved. Use of a specially certified burst disk for pressure relief as described does not relieve the system design of any other safety requirements specified in NHB 1700.7 which relate to burst disk requirements.

ORIGINAL SIGNED BY:

Leonard S. Nicholson

Distribution:

Payload Safety Distribution List

TA:RLBlount:111:8-24-88:34971

Retyped:TA:RLBlount:111:8-24-88:34971



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

OCT 17 1989

Reply to Attn of :

NSTS-JSC, TA-89-064

TO: Distribution

FROM: NSTS-TA/Acting Manager, NSTS Integration and Operations

SUBJECT: Verification of the National Space Transportation System (NSTS)  
Payload Propellant Tank Pressures for Pressure Stabilized Tanks

The information contained in this letter is considered an interpretation or clarification of the NSTS payload safety requirements for pressure vessels defined in Paragraph 214 in both NHB 1700.7A and NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System." This letter will be utilized by the NSTS Payload Safety Review Panel in assessing Payload design compliance, and it is applicable to all payloads including those which are to be retrieved. Payload designs which are noncompliant with the policy of this letter shall be reported immediately to the appropriate NSTS payload integration manager for hazard control resolution. Please add this letter to your copy of NSTS 18798, "Interpretations of STS Payload Safety Requirements."

The purpose of this letter is to document the concern associated with propellant tanks or other pressure vessels which are pressure-stabilized and must contain a minimum pressure to maintain the required ultimate factors of safety to insure structural integrity under launch and landing loads. Undetected leakage after ground servicing and/or pressurant absorption into the propellant/fluid could result in tank pressures falling below minimum acceptable values with the potential catastrophic failure of the tank during launch or landing.

The NSTS policy with respect to the design of pressure systems utilizing pressure-stabilized tanks is that the existence of the minimum required tank pressure must be verified prior to the application of safety critical loads into the system. This verification shall include a single fault tolerant pressure monitoring technique which is implemented such that the system pressure decay characteristics can be certified to insure minimum design safety factors will exist at the time of subsequent structural load application. Pressure monitoring can be implemented by using pressure transducers strain gages, or other suitable techniques. Pressure monitoring as a verification method to preclude failure of a pressure stabilized tank may be terminated after the pressure decay characteristics of the system have been certified as acceptable.

The above safety policy is implicit in the existing safety requirements of both NHB 1700.7A, with the additional mandatory requirements of letter TA-87-079, "Resumption of Payload Safety Activity," and NSTS 1700.7B. Both require verification of design features used to control potential hazards.

The hazard of tank buckling is controlled by the existence of the minimum required tank pressure. Hazard control verification is the monitoring of tank pressure to assure safe conditions for launch and landing.

Payload designs which utilize the unpowered bus option to eliminate monitoring of electrical inhibits to a hazardous function must consider, as a part of the design, the requirement for pressure monitoring when the payload is installed in the Orbiter. The unpowered bus configuration cannot be violated to obtain tank pressure data if payload hazard potential exists. If the system pressure decay characteristics cannot be certified prior to the planned time to put the payload into the unpowered bus configuration, a separate powered bus for tank pressure monitoring must be provided.

Questions concerning this policy letter should be directed to Mr. Harold F. Battaglia, mail code TA, telephone (713) 483-1159 or (FTS) 525-1159.

***ORIGINAL SIGNED BY :***

C. Harold Lambert, Jr.

## **6. PYROS**

<u>Title</u>	<u>JSC Letter Number</u>
6.1 Circuit Design for Payloads using Energy Storage Devices for Pyrotechnic Firing Circuits	TA-91-077
6.2 Pyrotechnically Operated Isolation Valves for Payloads	TA-92-049



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

Reply to Attn of :

JSC, TA-91-077

MAR 23 1992

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Circuit Design for Payloads Using Energy Storage Devices for Pyrotechnic Firing Circuits

The information contained in this letter is considered an interpretation or clarification of the payload safety requirements of NHB/NSTS 1700.7, and it will be utilized by the Safety Review Panel in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretation of NSTS Payload Safety Requirements," as being an applicable interpretation against NHB 1700.7A and NSTS 1700.7B.

The use of energy storage pyrotechnic firing circuits offers some advantages over more conventional relay firing circuits; however, they have the potential to reduce failure tolerance against premature firing if not properly designed.

The design must include an interrupt (inhibit) in both the high side and the return side of the stored energy output firing circuit. If the inhibits in the firing circuit (high and low side) are independent, one additional inhibit is required which prevents storing energy and arming the circuit. When the firing circuit inhibits are not independent (one firing Command closes both the high side and return inhibit), two independent inhibits are required which prevent storing energy and arming the circuit. One of these inhibits must interrupt the arming power source and the other must interrupt the return leg of the arming power source.

Existing designs which do not provide independent inhibits in the input and return leg of the arming circuit must show that there are no credible failures which could short power sources to the arming circuit if the firing circuit inhibits are not independent. Please note that "arming" inputs to some energy storage circuits are relatively low power circuits and even current limited power sources could be of concern.

Additionally, energy storage pyrotechnic firing circuits must incorporate design provisions to allow verification of the final connection of all "must work" firing circuits.

This verification will assure that the NASA Standard Initiator has been properly connected, and that the firing circuit resistance is within an acceptable range.

Questions concerning this subject should be directed to the executive secretary,  
Payload Safety Review Panel, NS2/JSC at FTS 525-4297.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.

Distribution:

Payload Safety Distribution List

cc:

NASA Hqs., MC/R. L. Tucker  
ME/D. L. Winterhalter  
KSC, CM/J. T. Conway  
MK/B. H. Shaw, Jr.  
TM/J. F. Honeycutt  
TM/G. T. Sasseen  
TM/R. B. Sieck  
TP/J. F. Harrington, III  
TV/J. R. Lan  
MSFC, EA01/R. J. Schwinghamer  
SA01/A. A. McCool  
SA21/Staff  
SA31/G. C. Ladner  
SA41/C. H. Rutland  
SA51/V. K. Henson  
SA61/R. E. Mitchell  
SA71/J. M. Ellis

JSC, AC/D. A. Nebrig  
CA/D. R. Puddy  
CB/D. C. Brandenstein  
DA/E. F. Kranz  
DA2/B. R. Stone  
EA/H. O. Pohl  
GA/L. S. Nicholson  
GA/T. W. Holloway  
GA2/J. P. Costello  
GM/D. C. Schultz  
MJ/T. R. Loe  
NA/C. S. Harlan  
TA/Staff  
VA/D. M. Germany  
VA/J. C. Boykin  
WA/F. T. Buzzard



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

Reply to Attn of :

JSC, TA-92-049

FEB 02 1993

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Pyrotechnically Operated Isolation Valves for Payloads

The information contained in this letter is considered an interpretation and clarification of the Space Shuttle payload safety requirements of NASA Handbook (NHB)/NSTS 1700.7, and will be utilized by the Payload Safety Review Panel (PSRP) in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretations of NSTS Payload Safety Requirements," as an applicable interpretation against NHB 1700.7A and NSTS 1700.7B.

Policy letter NS2/87-L051, dated April 27, 1987, same subject, established requirements for use of a single pyrotechnically operated isolation valve as the equivalent of two propellant flow control devices. Those requirements are reflected in the current payload safety requirements for use of pyrotechnic isolation valves (pyrovalves) as defined in NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System," paragraph 202.2a(2)(b). The purpose of this policy letter is to expand the existing pyrovalve requirements.

The likelihood of internal propellant leakage or release downstream through a single, parent-metal barrier is no greater than an external release through an acceptably designed, qualified, and acceptance tested component housing. Therefore, failure of a pyrovalve possessing a minimum of one flow barrier will be considered a noncredible single barrier failure if the following criteria, (in addition to all other applicable requirements of NSTS 1700.7B), are met:

1. The internal flow barrier must be a continuous unit of nonwelded parent-metal.
2. The valve is normally closed and will only be opened pyrotechnically after a safe distance from the orbiter has been achieved.
3. The valve structural design must preclude inadvertent operation as a result of exposure to all potential environmental conditions while in the vicinity of the orbiter.

4. The following component acceptance verifications are performed on the flight hardware:
  - a. Certification that the materials of construction conform to drawing specifications prior to fabrication.
  - b. Independent quality inspection verification that the parent-metal barrier conforms to the minimum thickness required by the design drawing.
  - c. Proof test at a minimum pressure of 1.5 X maximum design pressure (MDP) with no evidence of detrimental deformation (ref. NHB 8071.1, paragraph 302(2b).
  - d. Helium leak test (after proof test) at a minimum of 1.0 X MDP with a resulting leak rate less than  $1 \times 10^{-6}$  standard cubic centimeters per second.

Details of the valve design and test methods used to ensure system integrity must be adequately addressed in the safety data package and appropriate hazard reports for flight approval by the PSRP. Questions regarding implementation compliance shall be directed to the Executive Secretary, Space Shuttle PSRP, mail code NS2. (713) 483-4297.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.



## **7. STRUCTURES/MATERIALS**

<u>Title</u>	<u>JSC Letter Number</u>
7.1 Structural Requirements for Contingency Deorbit	NS2/90-208
7.2 Structural Integrity Following Mechanism Failures	TA-93-037
7.3 Mechanical Systems Safety	MA2-00-057
7.4 Low Risk Fracture Part Clarification	MA2-96-174



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

MAY 14 1991

Reply to Attn of :

JSC, NS2/90-208

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Structural Requirements for Contingency Deorbit

The information contained in this letter is an interpretation and clarification of the Space Shuttle payload safety requirements for contingency return that are defined in paragraph 205 of both NHB 1700.7A and NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System." The requirements in this letter are applicable to all payloads. This letter will be utilized by the Space Shuttle Payload Safety Review Panel in assessing payload design compliance. Please add this letter to your copy of NSTS 18798, "Interpretations of NSTS Payload Safety Requirements."

The clarified policy is that a payload must maintain a positive structural margin of safety with respect to an ultimate factor of safety of 1.4 under contingency deorbit thermal conditions which do not include on-orbit thermal preconditioning prior to descent. In the past, some payloads, in assessing structural compatibility for the contingency deorbit case, have erroneously assumed on-orbit thermal preconditioning would be available. Our experience indicates that composite/bonded structure is particularly sensitive to thermal conditions encountered in contingency deorbit cases. The initial thermal conditions to be used for the structural assessment for compatibility for the contingency deorbit case must consider an anytime deorbit from:

- (a) The nominal mission worst thermal conditions, including the primary and backup deployment opportunities.
- (b) Any attitude exposure resulting from the on-orbit thermal environment operational constraints for attitudes which are defined in section 4 of the payload integration plan (PIP).
- (c) The safety constraint conditions defined in terms of maximum solar and deep space exposure times that are specified in the flight decisions section of the flight operations support annex (Annex 3) of the PIP.

The payload organization should include in the payload's structural failure hazard report a cause that addresses the thermal environment in a contingency deorbit case exceeding the temperature limits used in the structural compatibility analysis.

Questions concerning this policy letter should be directed to Mr. R. Brown, mail code ES, telephone (713) 483-8861, or FTS 525-8861.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.

Distribution: Payload Safety Distribution List

cc:

NASA Hqs., M/W. B. Lenoir  
M-7/R. L. Crippen

KSC, CM/J. T. Conway  
MK/B. H. Shaw, Jr.  
TM/J. F. Honeycutt  
TM/G. T. Sasseen  
TM/R. B. Sieck  
TP/J. F. Harrington III  
TV/J. R. Lang

MSFC, EA01/R. J. Schwinghamer  
MM/J. R. Eady  
SA01/G. P. Bridwell  
SA21/J. W. Smelser  
SA31/G. C. Ladner  
SA41/C. H. Rutland  
SA51/V. K. Henson  
SA61/R. E. Mitchell  
SA71/J. M. Ellis

JSC, AC/D. A. Nebrig  
CA/D. R. Puddy  
CB/D. C. Brandenstein  
DA/E. F. Kranz  
DA2/T. W. Holloway  
EA/H. O. Pohl  
ES3/R. G. Brown  
GA/J., H. Greene  
GA2/J. B. Costello  
GM/D. C. Schultz  
MJ/T. R. Loe  
NA/C. S. Harlan/G. W. Johnson  
MA2/M. E. Merrell  
TA/C. H. Lambert, Jr.  
TA/A. M. Larsen  
VA/D. M. Germany  
VA/J. C. Boykin  
WA/L. G. Williams  
WA/F. T. Buzzard



National Aeronautics and  
Space Administration

Washington, D. C.  
20546

AUG 16 1993

Reply to Attn of :

JSC, TA-93-037

TO: Distribution

FROM: TA/Manager, Space Shuttle Integration and Operations

SUBJECT: Structural Integrity Following Mechanism Failures

The information contained in this letter is an interpretation and clarification of the payload safety requirements of NHB/NSTS 1700.7, "Safety Policy and Requirements For Payloads Using the Space Transportation System." This letter will be utilized by the Space Shuttle Payload Safety Review Panel (PSRP) in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretations of NSTS Payload Safety Requirements," as applicable against NHB 1700.7A and NSTS 1700.7B. Enclosed is an updated table of contents for NSTS 18798A.

This interpretation letter is intended to clarify that the requirements in NHB/NSTS 1700.7, paragraph 208.1 (Structural Design), apply to all loading conditions including those that occur after credible mechanism failure(s). Mechanism failure(s) which result in limit load redistribution will require structural verification of the redistributed loads if the PSRP determines the failed condition is credible.

In order to minimize the number of structural configurations to be analyzed, payloads should provide two-failure tolerance against load redistribution caused by credible mechanism failures which could result in a hazard to the orbiter or crew. When two-failure tolerance cannot be implemented, the number of structural configurations to be certified must be approved by the Space Shuttle Program. Structural verification of the redistributed load path is required and the 1.4 factor-of-safety on limit loads must be maintained.

Questions concerning this subject should be directed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, NS2/JSC, at (713) 483-4297.

**ORIGINAL SIGNED BY :**

C. Harold Lambert, Jr.

Enclosure

National Aeronautics and  
Space Administration

**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of : MA2-00-057

September 28, 2000

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/Deputy Manager, International Space Station Program

SUBJECT: Mechanical Systems Safety

The information contained in this letter is an interpretation and clarification of the payload safety requirements for the Space Shuttle Program (SSP) and for the International Space Station (ISS) Program. This letter applies to all SSP and ISS Program payloads; i.e., payloads required to comply with either NSTS 1700.7B paragraph 200.2, "Safety Policy and Requirements for Payloads Using the Space Transportation System" or NSTS 1700.7B, ISS Addendum paragraph 200.2, "Safety Policy and Requirements for Payloads Using the ISS." This letter will be utilized by the flight Payload Safety Review Panel (PSRP) in assessing safety compliance. This letter replaces the previous letter, TA-94-041, "Mechanical Systems Safety," dated June 9, 1994. Please add this letter to your copy of NSTS/ISS 18798B, "Interpretations of NSTS/ISS Payload Safety Requirements," as applicable against NSTS 1700.7B and the ISS Addendum. Enclosed is an updated table of contents for NSTS/ISS 18798B.

This letter is intended to consolidate and clarify the major PSRP policy decisions on matters related to the safety requirements for the design and verification of mechanisms (movable mechanical systems) used in safety critical applications. This letter addresses assurance of safety critical functionality (the ability to operate or the ability to retain configuration) for mechanical systems rather than their strength as a structural element or the electrical aspects of an electromechanical system. For the purposes of this letter, safety critical refers to a system which has the potential to result in a critical or catastrophic hazard.

The revised safety policy, as documented in this letter, provides clarification on usage of the design for minimum risk (DFMR) approach as it applies to functionality of a movable mechanical system. This revised safety policy specifies that compliance with DFMR criteria when applied to movable mechanical systems normally can be used to establish safety compliance in designs with only one additional control or backup for a catastrophic hazard or without additional controls for a critical level hazard. Additionally, this revised safety policy also permits the use of fully compliant simple mechanical systems without mechanical redundancy, i.e., DFMR simple mechanisms can be considered as having two-failure-tolerance equivalency when specifically approved by the PSRP.

A simple mechanical system is defined as a robust mechanism that has relatively few moving parts and can demonstrate low sensitivity to environmental and operational conditions. If a hardware developer elects to follow the simple mechanical system route,

approval must be obtained from the PSRP prior to completion of the phase I safety review. The Mechanical Systems Working Group (MSWG) will support this process by assessing the level of assurance that all credible hazardous failure modes have been identified and that each of these failures will be reliably and effectively controlled as a result of a thorough design, build, and test process.

The design of a movable mechanical system can be considered to meet DFMR in functionality if it can be demonstrated that credible failure modes have been reliably and effectively controlled as a result of a thorough design, build, and test process. Failure modes that must be considered for credibility include, but are not limited to, binding, jamming, inadvertent operation, failure to function, etc. The DFMR approach must include design implementation and verification provisions outlined in items 1 through 11 of this letter, unless clearly not applicable, to enhance the safety critical reliability of mechanical systems to the maximum extent practical. These items will be topics of the review process for all safety critical mechanical systems. The PSRP may accept alternate approaches to the design, build, and test provisions contained herein on a clearly substantiated equivalent safety basis with the MSWG's recommendation.

1.0 Binding/Jamming/Seizing. Designs shall include provisions to prevent binding/jamming/seizing. Appropriate design provisions include, but are not limited to, dual rotating surfaces or other mechanical redundancies, robust strength margins such that self-generated internal particles are precluded, shrouding and debris shielding, proper selection of materials and lubrication design to prevent friction welding or galling, etc. Designs shall also establish dimensional tolerances on all moving parts to ensure that proper functional performance will be maintained under all natural and induced environmental conditions including, but not limited to, thermally induced in-plane and out-of-plane distortions, differential thermal growth and shrinkage, and load-induced deflections. The design shall also take into account tolerances associated with rigging (mechanical adjustment) and shall demonstrate by test and/or analysis that the sensitivity of mechanism performance as a function of rigging tolerances or installation/integration variables is understood. Additionally, mechanical system designs shall ensure compatibility of any lubricants used with interfacing materials and other lubricants used in the design, and shall ensure the lubrication is compatible with the natural and induced environment. The design shall also address proper quantities of lubricant.

2.0 Quick Release Pins. Quick release pins (pip-pins) used in safety critical applications are considered movable mechanical systems subject to the provisions of this letter. A pip-pin design qualified by inspection and test to the provisions of MIL-P-23460 or equivalent shall be used in any system design incorporating safety critical pip-pins. Flight pip-pins shall be subjected to environmental acceptance testing. Pip-pins shall be vibration tested to qualification levels in place in their respective hardware locations during the qualification test of the total assembly, or they may be tested alone in a component test to the predicted qualification levels at the hardware location. Pip-pins shall also be subjected to thermal testing to the maximum/minimum qualification temperatures. Due to a history of failures with pip-pins, the simple mechanical system approach identified above is not applicable.

3.0 Springs. In designs and applications where spring failure would result in a hazard, the springs shall be redundant or designed, evaluated, and used under an acceptable fracture control program (reference NASA-STD-5003). Failure of springs that are properly

controlled under an acceptable fracture control program, is considered noncredible. The design and use of a fail-safe spring or the use of a spring that maintains functionality with the loss of a single coil is acceptable. Where practical, compression springs should be used in lieu of tension or torsional springs.

4.0 Fastener Retention. A means of positive locking (i.e., self-locking threads, self-locking inserts, etc.) shall be provided on all fasteners (threaded and otherwise) to assure integrity of the mechanical assemblies and prevent loose parts. This is in addition to the standard torque/preload of the fastener. Where other locking devices are practicable, locking compounds shall not be used on fasteners to provide locking.

5.0 Strength and Fracture Control. Structural design of safety critical mechanical system components shall adhere to paragraphs 208.1, 208.2, and 208.3 of NSTS 1700.7. Movable mechanical assemblies used in safety critical applications shall be included in an acceptable fracture control program (reference NASA-STD-5003). Mechanical system components and linkages shall be designed with sufficient strength to tolerate an actuation force/torque stall condition at any point of travel and maintain a positive margin of safety with an ultimate factor of safety applied. Mechanical systems that incorporate end of travel mechanical stops shall be designed to have positive strength margins for worst case dynamic loading conditions, considering variables in inertia properties, actuation force/torque, drive train resistance, and other environmental conditions. Exposed mechanical system components, protective shrouds and covers, and mounting structure shall be designed to accommodate inadvertent impact loads from remote manipulator system/ISS remote manipulator system/payload operations and extravehicular activity/intravehicular activity loads, as appropriate, to ensure adequate margins to preclude deformation that could cause a binding or jamming condition or inadvertent operation of the mechanism. A design that incorporates preload as a means of meeting functional and/or structural requirements shall comply with the preload criteria defined in NSTS 08307.

6.0 Positive Indication of Status. All movable mechanical systems shall provide positive indication that the mechanism has achieved its desired position (i.e., ready-to-latch, latched). End of travel stops shall be provided for all movable mechanical systems.

7.0 Torque/Force Margins. For movable mechanical systems in safety critical applications, the operating torque or force margin shall be acceptance-test verified unless another verification approach is approved by the MSWG. When test verified, a margin of 1.0 or greater is required at applicable points of travel. Verification by analysis only will require prior review and approval of the analytical approach and margin requirement by the MSWG. This margin, as demonstrated conservatively by test or analytical calculations, shall take into account worst case environmental conditions, frictional effects, alignment effects, latching forces, thermally induced distortions, load induced distortions, and variations in lubricity including degradation or depletion of lubrication under vacuum and under worst case thermal conditions, etc. Operating torque margin is defined as:

$$\text{Operating Torque Margin} = (\text{Available Driving Torque} / \text{Resisting Torque}) - 1$$

For linear devices, "Force" replaces "Torque" in the above equation.

Mechanism holding torque or force margin shall be acceptance-test verified unless another verification approach is approved by the MSWG. When test verified, a margin of 1.0 or greater is required in the applicable mechanism holding configuration(s). The holding torque or force margin is the margin provided to prevent inadvertent operation. Verification by analysis only will require prior review and approval of the analytical approach and margin requirement by the MSWG. This margin, as conservatively demonstrated by test or analytical calculations, shall take into account worst case environmental conditions, frictional effects, alignment effects, latching forces, thermally induced distortions, and load induced distortions, etc. The holding torque margin is defined as:

$$\text{Holding Torque Margin} = (\text{Available Holding Torque} / \text{Torque Applied by Limit Load}) - 1$$

For linear devices, "Force" replaces "Torque" in the above equation.

Verification by test, as specified in this paragraph, does not require a mechanical system demonstration at greater than limit load conditions but rather requires a test verification of the amount of driving or holding torque or force available under conservative adverse conditions.

8.0 Contamination. Fabrication and handling of safety critical movable mechanical assemblies shall be accomplished in a clean environment with attention given to avoiding nonparticulate (chemical) as well as particulate air contamination. Specific cleanliness requirements shall be established for each movable mechanical assembly and shall address cleanliness levels needed to prevent binding or jamming.

9.0 Assembly Level Acceptance Tests. Each movable mechanical assembly designated for flight or as a qualification test article shall be subjected to acceptance testing which incorporates run-in, functional, and environmental testing. The acceptance tests shall be structured to detect workmanship defects that could affect operational performance. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion.

9.1 Run-in Test. After initial functional testing, a run-in test shall be performed on each movable mechanical assembly before it is subjected to further acceptance testing. The purpose of the run-in test is to detect material/workmanship defects and to wear-in parts.

9.2 Functional and Environmental Acceptance Tests. Each movable mechanical assembly shall be subjected to functional and environmental tests. Functional tests shall be structured to demonstrate that the movable mechanical assembly is capable of operating to satisfy all performance requirements. Functional tests are required before and after exposure to environmental test conditions in order to establish whether damage or degradation in performance has occurred. Environmental acceptance tests shall be structured to demonstrate the ability to achieve performance requirements when exposed to the expected environmental extremes and to identify any workmanship defects.

10.0 Qualification Test. A Qualification Test Program shall be established for each safety critical movable mechanical assembly. The qualification test program shall assure that a design performance and safety margin exists with respect to all design requirements when exposed to any mechanical, electrical, environmental, including acceptance testing, and



operational stimuli that the product may reasonably expect to encounter during its service life. The mechanism shall be tested in its launch, on-orbit, and landing configurations with the appropriate corresponding environmental extremes and with the mechanism in its appropriate passive or operating state. Inspection and functional tests are required before and after qualification tests. MIL-STD-1540D may be helpful in establishing an effective Qualification Test Program. Natural and induced environmental conditions shall include but are not limited to, thermally induced in-plane and out-of-plane distortions, differential thermal growth and shrinkage, and load-induced deflections. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion.

**11.0 Design Life Verification Tests.** For applications where design life might be a concern due to endurance or fatigue limits being exceeded, potential deterioration of lubrication, or excessive wear, design life verification testing shall be conducted to verify that design life requirements have been complied with. Design life testing for mechanisms that pose a catastrophic hazard potential shall assure at least four times the number of operational cycles, plus four times the number of component and vehicle functional and environmental test cycles. Design life testing for mechanisms that pose a critical hazard potential shall assure at least two times the number of operational cycles, plus two times the number of component and vehicle functional and environmental test cycles. Inspection and functional tests are required before and after design life verification tests. For programs using proto-flight approaches, the test parameters may be adjusted with MSWG approval to avoid excessive endurance or fatigue limit margin erosion. Refurbishment shall be accomplished after the design life verification tests and prior to reacceptance testing.

A comprehensive Mechanical Systems Verification Plan that describes the verification approach for safety critical movable mechanical systems must be submitted for review and approval by the MSWG. The specific purpose of this plan is to establish an understanding on how applicable systems requirements will be implemented and verified. Before a movable mechanical system can be classified as a DFMR Mechanical System, compliance to the subject letter requirements must be provided to and approved by the MSWG. Although cancelled, mechanical system designers may still refer to MIL-A-83577 as a guideline during the design and verification process. Questions concerning this letter should be directed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, JSC/NC4, at (281) 483-8848.

***Original Signed By:***

William H. Gerstenmaier

***Original Signed By:***

Jay H. Greene

Enclosure

cc:

See List

MA2-00-057

6

Distribution:

CB/G. D. Griffith  
 DO12/J. M. Childress  
 EA44/R. J. Wren  
 MA2/A. M. Larsen  
 MA2/D. E. O'Brien  
 MA2/D. W. Whittle  
 MA2/J. G. Williams  
 NC4/M. L. Ciancone  
 NC55/SAIC/E. J. Conner  
 NE2/G. L. Priest  
 OZ3/D. W. Hartman  
 SD2/M. E. Coleman  
 USA/USH-700D/H. A. Maltby

## cc:

AE/J. F. Whiteley  
 CA/J. D. Wetherbee  
 CB/C. J. Precourt  
 DA/B. R. Stone  
 EA/L. S. Nicholson  
 EA4/D. A. Hamilton  
 KN/NASDA/T. Akutsu  
 LM/I. M. Dornell  
 MA/R. D. Dittemore  
 MG/R. H. Heselmeyer  
 MM/J. B. Costello  
 MM/T. W. Logan  
 MQ/M. D. Erminger  
 MS/L. D. Austin, Jr.  
 MS3/D. L. Ladrach  
 MS3/K. B. Packard  
 MT/R. M. Swalin  
 MV/R. R. Roe, Jr.  
 NC44/M. L. Mudd  
 OA/T. W. Holloway  
 OE/J. B. Holsomback  
 OI/W. J. Bennett  
 OR/CSA/H. L. Williams  
 OT/ESA/U. J. Thomas  
 XA/G. J. Harbaugh  
 HQ/M-4/W. M. Hawes  
 HQ/MO/S. R. Nichols  
 HQ/M-7/N. B. Starkey  
 KSC/EC-G1/J. C. Dollberg  
 KSC/MK/J. D. Halsell, Jr.  
 KSC/MK-SIO/R. L. Segert  
 USA/USH-700D/L. Lo

Canadian Space Agency  
 Space Station Program  
 Attn: P. M. Jean  
 Manager, Safety and Product  
 Assurance  
 6767 route de l'Aéroport  
 Saint-Hebert, Quebec  
 Canada J3Y 8Y9

ESTEC-GPQ  
 Attn: T. Sgobba  
 T. Heimann  
 P. O. Box 299 NL  
 2200 AG, Noordwijk  
 The Netherlands

NASDA  
 Tsukuba Space Center  
 Attn: H. Hasegawa  
 Space Station Safety and  
 Product  
 Assurance Office  
 Reliability Assurance  
 2-1-1 Sengen  
 Tsukuba-shi, Ibaraki  
 Japan 305

RSC Energia  
 Attn: P. Vorobiev  
 4a Lenin Street  
 Korolev  
 141070 Moscow Region  
 Russia

National Aeronautics and  
Space Administration  
**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of : MA2-96-174

NOV 21 1996

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration

SUBJECT: Low Risk Fracture Part Clarification

The information contained in this letter is an interpretation and clarification of the Space Shuttle payload safety requirements for fracture control. The requirements of this letter are applicable to all payloads designed to NHB 1700.7A or NSTS 1700.7B. This letter supersedes TA-92-013, "Low Risk Fracture Part," dated June 29, 1992, and will be utilized by the Space Shuttle Payload Safety Review Panel (PSRP) in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretations of National Space Transportation System (NSTS) Payload Safety Requirements." Enclosed is an updated table of contents for NSTS 18798A.

The primary purpose of this letter is to expand the use of the low risk fracture part classification to parts, including fasteners, with limit tensile stresses exceeding 30 percent of the ultimate tensile strength of the material used. This letter is also issued to resolve other interpretation problems that have been encountered with TA-92-013.

The concept of a "low risk fracture part" was introduced into fracture control to reduce the number of parts that become fracture critical by default; when the necessity for classification as fracture critical is in doubt, but not proven; or when light loading conditions significantly mitigate risk of failure due to flaw growth, but cannot be used to place a part in an alternate category. A part may be nonfracture critical because it is inherently fail-safe or a contained/restrained mass, but analyses or tests to verify the classification are impractical or unavailable. The low risk fracture part categorization can be used for such parts. The method is also acceptable for other structures under specific stress limitation. Low risk fracture part classification is achieved when the possibility for failure due to a crack-like flaw can be shown to be extremely remote. Low risk fracture part classification is a nonfracture critical category. The method has been evaluated for payload applications and although not specifically permitted by NHB 8071.1, "Fracture Control Requirements for Payloads Using the NSTS," the low risk fracture approach can be accepted as an alternate fracture control method for payloads, where applicable, if approved by the Payload Safety Review Panel, in accordance with Chapter 6, "Alternate Approaches," of NHB 8071.1. Candidate low risk fracture parts shall be initially addressed in the Phase 1 Safety Review package, and compliance shall be addressed by the Phase 2 Safety Review.

A low risk fracture part shall comply with the requirements that are defined in paragraphs A and B. Low risk fastener requirements are defined in paragraph C only.

- A. **LIMITATIONS ON APPLICABILITY.** The part shall be all metal and shall not be a habitable module, pressure vessel, pressurized hardware (such as lines, fittings, components, containers, etc.), or high energy rotating equipment.

Structural parts that are apparently fail-safe, contained, or low released mass may be considered for low risk fracture part classification when verification by analysis or testing is impractical or prohibitive. For assessment of these parts there is no limitation on stress level, except as limited by safety factor compliance. Other structural parts may also be considered for low risk fracture part classification if the tensile stress at limit load is no higher than 30 percent of design ultimate tensile strength of the material.

- B. **INHERENT ASSURANCE AGAINST FAILURE FROM A FLAW.** The part shall possess inherent assurance against failure due to a crack-like flaw by compliance with the requirements of paragraphs (1) and (2).

- (1) Remote Possibility of Significant Crack-Like Defect. Assurance against the presence of a significant crack-like defect shall be achieved by compliance with the following criteria:

- (a) The part shall be fabricated from a well characterized metal which is not sensitive to stress corrosion cracking. The metal shall be classified in Table I in accordance with MSFC-SPEC-522B, "Design Criteria For Controlling Stress Corrosion Cracking," or rated A in accordance with MSFC-HDBK-527/JSC 09604, "Materials Selection List for Space Hardware Systems."
- (b) The part shall not be fabricated using a process that has a recognized risk of causing significant crack-like defects, such as welding, forging, casting, or quenching heat treatment (for materials susceptible to cracking during heat treatment quenching). It may be assumed that significant crack-like defects do not occur during machining of sheet, bar, and plate products from materials that are known to have good machinability properties and have a materials property ratio of

$$K_{Ic}/F_{ty} > 0.33 \text{ in.}^{1/2} (1.66 \text{ mm.}^{1/2})$$

and are metals or alloys produced in accordance with applicable Military Specifications and Standards or equivalent grade specifications.

- (c) Although a Nondestructive Evaluation is not specifically required as a measure to screen flaws for low risk fracture assessment, all parts classified as low risk fracture parts shall meet inspection standards consistent with aerospace practices to ensure aerospace quality flight hardware. At a minimum, low risk fracture parts shall receive visual inspection. Inspection

shall be made at the individual part level to assure maximum accessibility. Surface damage that could affect part life shall be cause for rejection.

- (2) Remote Possibility of Significant Crack Growth. Assurance against significant crack growth shall be achieved by compliance with any one of the following criteria:
- (a) The part shall not be subjected to significant fatigue loading during its lifetime. Fatigue loading can be considered insignificant when a part undergoes cyclic loading only during acceptance and/or normal protoflight testing (if any), transportation, and one mission, or an equivalent number of cycles.
  - (b) The part shall be shown to possess a high safety margin on fatigue strength. This may be shown by either 1. or 2. as follows:
    - 1. Limiting the maximum cyclic stress,  $S_{max}$ , for a metal part with  $S_{max} <$  endurance limit, or if data are not available, to:
 
$$S_{max} \leq F_{tu}/(4(1-0.5R))$$

where R is the ratio of minimum stress to maximum stress in a fatigue cycle and  $S_{max}$  is the local concentrated stress.
    - 2. A fatigue analysis for crack initiation which conservatively accounts for the effects of notches and mean stress. The analysis must show a minimum of 10 complete service lifetimes with a safety factor of 1.4 on alternating stress.
  - (c) The part shall be shown to possess acceptable durability. Acceptable durability shall be shown by an analysis which predicts that credible initial defects of maximum size caused by machining, assembly, or handling will not propagate to failure in less than four complete service lifetimes. Initial defects shall be assumed to be surface cracks of 0.025-inch (0.63 mm) depth and 0.05-inch (1.25 mm) total length and corner cracks of 0.025-inch (0.63 mm) radius.

C. **LOW RISK FASTENERS.** A fastener or shear pin may be classified as a low risk fracture part if the following requirements are met:

- (1) Failure of the fastener/shear pin would not result in a catastrophic loss of structural integrity.
- (2) The fastener/shear pin shall comply with an applicable high-quality military standard, national aircraft standard, or equivalent commercial standard. A custom made or reworked fastener shall have equivalent quality assurance and verification.

- (3) The fastener/shear pin shall be fabricated from well-characterized metal, which is not sensitive to stress corrosion cracking, and assured to be fabricated in accordance with aerospace-type specifications by an acceptable fastener verification program.
- (4) The fastener shall have rolled threads meeting aerospace or equivalent standards when loaded primarily in tension-requiring specific tensile preload. A fastener in this kind of application shall not be made of Ti-6Al-4V alloy, a high strength (>180 KSI) steel, or any metal with a KIC/FTY ratio that is less than 0.33 inch 1/2 (1.66 mm.1/2), and shall have positive back-off prevention to assure the validity of fracture control.
- (5) The fastener/shear pin shall meet all applicable structural requirements for stress and fatigue analysis, including torque/preload requirements for tension loaded fasteners. In the absence of a suitable analysis, the appropriate requirements of Section (2), "Remote Possibility of Significant Crack Growth," of this letter shall be applied.

The low risk fracture part is an acceptable method for fracture control screening of payload parts. The low risk fracture part category is intended for those parts which specifically meet the requirements and criteria in this letter and shall not be used on parts that are clearly subject to the more conventional screening and fracture control methods defined in NHB 8071.1. The PSRP reserves the prerogative to disapprove categorization as a low risk fracture part where there are unresolved concerns regarding the classification. Parts determined to be low risk fracture parts shall be identified in the Fracture Control Summary Report for the payload, including the justifying rationale.

**ORIGINAL SIGNED BY :**

Ronald D. Dittmore

Enclosure

Distribution:

Payload Safety Distribution

cc:

HQ/M-4/A. M. Allen  
 HQ/M-7/S. S. Oswald  
 KSC/GK3/W. B. Owens  
 KSC/MK/L. J. Shriver  
 KSC/MK/W. I. Wiley

KSC/MK-SIO/R. L. Segert  
 KSC/PH/J. F. Harrington  
 MSFC/EJ41/J. A. Jones  
 MSFC/JA01/C. S. Griner

MA2/HFBattaglia:km:11/6/96:31159

## **8. VERIFICATIONS**

<u>Title</u>	<u>JSC Letter Number</u>
8.1 Safety Policy for Detecting Payload Design Errors	TA-94-018
8.2 Verification/Reverification Requirements for On-Orbit Payloads	MA2-98-135

National Aeronautics and  
Space Administration  
Washington, D. C.  
20546



Reply to Attn of :

JSC, TA-94-018

MAR 25 1994

TO: Distribution

FROM: MA/Director, Space Shuttle Operations

SUBJECT: Safety Policy for Detecting Payload Design Errors

The information contained in this letter is an interpretation and clarification of the payload safety requirements of NHB/NSTS 1700.7, "Safety Policy and Requirements For Payloads Using the Space Transportation System." This letter will be utilized by the Space Shuttle Payload Safety Review Panel (PSRP) in assessing payload design compliance. Please add this letter to your copy of NSTS 18798A, "Interpretations of NSTS Payload Safety Requirements," as applicable against NHB 1700.7A and NSTS 1700.7B. Enclosed is an updated table of contents for NSTS 18798A.

The STS-51 Advanced Communications Technology Satellite (ACTS)/Transfer Orbit Stage (TOS) was successfully deployed from the Space Shuttle orbiter payload bay on September 12, 1993. During the deployment, commands intended to initiate only the primary SUPER\*ZIP explosive cord actually resulted in the simultaneous firing of both the primary explosive cord and backup explosive cord. This simultaneous explosive cord firing resulted in the rupture of a SUPER\*ZIP containment tube and the release of contaminants and high energy debris into the cargo bay.

This hazardous event was caused by a design error that went undetected for a period of years. This embedded design error remained undetected throughout a series of requirements, safety, design and certification reviews, and systems tests. Verification activities were centered on verifying the erroneous design rather than verifying the end functions.

The purpose of this letter is to apply the lessons learned from this experience to the Space Shuttle Program (SSP) payload safety activity.

All payload systems having catastrophic hazard potential for the orbiter or crew as a result of operations in or near the orbiter must use hardware and procedures that have been subjected to a rigorous verification program. Verification programs normally require testing to verify adequate performance margins under all environmental conditions (qualification testing) as well as demonstrating intended system performance on flight hardware. Comprehensive system level testing on payload flight hardware supported by qualification test on protoflight or flight type hardware are the preferred verification methods. It is essential that payload system performance be verified from the input stimuli to the end function.



Safety critical system performance which cannot be verified by test shall be verified by independent parties using dissimilar analysis techniques whenever possible. Single party analytical efforts can be used to verify performance only when the methodology is widely accepted and conservative margins are applied to the results.

The payload organization must focus its attention to all parts of the payload verification program and orbiter interface verification activities to assure that the subelements of the total verification program are integrated into a comprehensive system verification effort that confirms the intended system performance. When the use of ground test equipment (apparatus) is required to replace flight hardware functions, verification methods shall be developed by engineering personnel independent from those designing the flight system. Test requirements, procedures, and test apparatus shall be derived from intended functional requirements rather than from the design, and all items must be maintained under strict configuration control. The payload organization is responsible for developing and presenting sufficient data to the PSRP to substantiate that the test requirements, procedures, and test apparatus will provide an adequate simulation in substitution for the end function.

The payload safety review activity will increase the emphasis on the identification and verification safety assessment of all payload systems having catastrophic hazard potential for the orbiter or crew as a result of operations in or near the orbiter.

The Phase I safety assessment report must identify these systems and reflect the verification approach proposed to confirm intended system performance (qualification test plus comprehensive system level testing of payload flight hardware from beginning stimuli to the end function is the preferred method). Testing supplemented by analysis can be used to verify a function; however, when this approach is used, separate analytical efforts by independent parties are required or conservative safety margins are to be applied to single party results. Ground rules, assumptions, and modeling approaches shall be coordinated with PSRP technical support personnel prior to the start of the analysis. The safety assessment report shall identify: (a) the verification method to be used (test or analysis); (b) the need for independent parties; and (c) identification of safety margins for single party efforts.

The Phase II safety assessment report must contain a verification plan(s) which identifies the test and analytical efforts required to verify intended hardware performance for all systems with operational hazard potential. The plan(s) must identify the basic content of the test and/or analysis effort along with a summary of the pass/fail criteria and simplified orbiter/payload end-to-end schematics/diagrams depicting electrical, mechanical, fluid, and software controlled interfaces with clear and consistent nomenclature. The simplified end-to-end schematics/diagrams shall be derived from detailed design drawings which are under formal configuration control and shall be maintained current with flight system configuration changes.

The Phase III safety assessment report shall summarize the results achieved by the verification activity and compare the results from all independent verification activity. Payloads presently in the safety process must adjust their safety data to meet the intent of the review process described in this letter.

Hazard causes and controls will continue to be identified and tracked in individual hazard reports. Hardware performance verification is to be emphasized and highlighted with appropriate technical presentation material during the formal safety review.

During the past sixty Space Shuttle flights, both the government and the industry payload developers have experienced enormous success in achieving mission objectives and safe flight. The SSP credits this success to the integrity of the payload developers safety assessment.

In view of the hazardous event experienced on the STS-51 mission, it is important to stress that the payload organization has the ultimate responsibility for safety of the payload design and operation. Design compliance with payload safety requirements substantiated by a thorough safety hazards assessment and verification process by the payload organization is fundamental to maintaining flight safety.

The primary function of the PSRP is to assure that the payload organization's understanding and interpretation of the safety requirements are consistent with NASA payload safety policy. Additionally, the PSRP will assess the payload's design features which have been implemented for controlling identified hazards and the verification approach that confirms intended system performance.

Questions regarding implementation compliance should be directed to the Executive Secretary, Space Shuttle PSRP, Mail Code NS2, 483-4297.

***ORIGINAL SIGNED BY :***

Brewster H. Shaw, Jr.

Enclosure

National Aeronautics and  
Space Administration  
Washington, D. C.  
20546



Reply to Attn of :

MA2-98-135

December 5, 1998

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/Deputy Manager for Technical Development, International Space  
Station Program

SUBJECT: Verification/Reverification Requirements for On-Orbit Payloads

The information contained in this letter is considered an interpretation or clarification of the payload safety requirements of NSTS 1700.7B, "Safety Policy and Requirements for Payloads using the Space Transportation System (STS)," and NSTS 1700.7B Addendum, "Safety Policy and Requirements for Payloads Using the International Space Station" and will be utilized by the Payload Safety Review Panel in assessing payload design compliance. Please add this letter and updated Table of Contents to your copy of NSTS/ISS 18798, "Interpretation of STS Payload Safety Requirements," as being an applicable interpretation against NSTS 1700.7B and NSTS 1700.7B International Space Station (ISS) Addendum.

NSTS 1700.7B and NSTS 1700.7B ISS Addendum paragraphs 200 and 201 require safety features and inhibits to be in place whenever hazard potential exists. Unlike orbiter payloads, ISS payloads remain on orbit long enough to increase concerns about possible loss of payload safety features and inhibits and to generate concerns about subsequent on-orbit verifications and reverifications that will be needed to continue safe operations. Events and conditions of concern include payload reconfiguration from the as-launched condition, payloads remaining on orbit past the original period of certification of the safety features or inhibits (e.g., exercising soft seals, relief valves), and any other events or conditions that may be identified that will make verification/reverification necessary.

To address these concerns, the compatibility of the payload design with verification/reverification operations and paragraph 200 and 201 requirements must be demonstrated where applicable. Payload organizations must also provide specific plans, methods and schedules for on-orbit verification/reverification of affected safety features and inhibits. The schedule of verification/reverification operations must be consistent with safety feature and inhibit certification time limits.

Questions concerning this subject should be addressed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, Mail Code NC4, telephone (281) 483-8848.

***Original Signed By:***

William H. Gerstenmaier

Enclosure

***Original Signed By:***

Jay Greene

**Distribution:**

CB/G. D. Griffith  
DO12/J. M. Childress  
EA4/R. J. Wren  
MS3/K. B. Packard  
NC4/M. L. Ciancone  
OE/S. L. Thomas  
OZ3/D. W. Hartman  
SD2/M. E. Coleman

**cc:**

HQ/M-4/G. W. McClain  
HQ/M-7/W. F. Readdy  
HQ/ME/C. T. Holliman  
HQ/MO/R. L. Elsbernd  
KSC/AA-D/J. H. Morgan  
KSC/MK/D. R. McMonagle  
KSC/MK-SIO/R. L. Segert

## **9. OTHER**

<u>Title</u>	<u>JSC Letter Number</u>
9.1 Computer Control of Payload Hazards	MA2-97-083
9.2 Small Commonly Used Batteries	MA2-98-069

National Aeronautics and  
Space Administration  
Washington, D. C.  
20546



Reply to Attn of :

MA2-97-083

September 19, 1998

TO: Payload Safety Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/Deputy Manager for Technical Development, Space Station Program  
Office

SUBJECT: Computer Control of Payload Hazards

The information contained in this letter is an interpretation and clarification of the safety policy for the Space Shuttle Program (SSP) and the International Space Station Program (ISSP) regarding computer control of hazardous functions. This letter applies to all payloads; i.e., payloads required to comply with either NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System," or NSTS 1700.7B Addendum, "Safety Policy and Requirements for Payloads Using the International Space Station" and will be utilized by the Payload Safety Review Panel (PSRP) in assessing compliance. The safety requirements being clarified are in paragraph 201.1e of NSTS 1700.7B. Please add this letter to your copy of NSTS/ISS 18798B, "Interpretations of NSTS/ISS Payload Safety Requirements."

The existing practice of the PSRP has disallowed use of computer-based control systems to provide total hazard control. However, ISSP has developed a series of acceptable safety approaches for total computer control of station systems (defined in SSP-50038, "Computer-Based Control System Safety Requirements"). As a result of this, a computer-based control system now may be used to totally control a hazardous system. The "Fault Tolerant" approach, defined in NSTS 1700.7B, paragraph 201.1e (1), remains as the desired method of hazard control. A computer-based control system may be used for total control of a hazardous payload system only when the "Fault Tolerant" approach is infeasible and the hazardous payload system can be designed and verified to be "Fail Safe." The "Fail Safe" policy is embodied in the enclosure to this letter entitled "Fail Safe Approach for Computer-Based Control Systems."

Additionally, the Fault Containment approach identified in SSP-50038 can be applied to payloads only when the "Fault Tolerant" approach is infeasible and the hazardous payload system can be designed and verified to comply with the requirements defined in SSP-50038 sections 3.1.1 and 3.1.3.1.

Questions concerning this subject should be addressed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, Mail Code NS2, telephone (281) 483-4297.

*Original signed by*

Richard N. Richards

*Original signed by*

Jay H. Greene

Enclosure

cc:

HQ/M-4/G. W. McClain  
HQ/M-7/S. S. Oswald  
HQ/ME/H. L. Smith  
HQ/MO/R. A. Parker  
KSC/AD/J. H. Morgan  
KSC/MK/D. R. McMonagle  
KSC/MK/W. I. Wiley  
KSC/MK-SIO/R. L. Segert  
KSC/PH/J. F. Harrington  
MSFC/EJ41/J. A. Jones  
MSFC/FA51/R. W. Hughes  
MSFC/JA01/C. S. Griner

bc:

AC/S. H. Garman  
CA/D. C. Leestma  
CB/R. D. Cabana  
DA/B. R. Stone  
EA/L. S. Nicholson  
EA4/J. W. Aaron  
MA/T. W. Holloway  
MG/R. H. Heselmeyer  
MM/J. B. Costello  
MM/T. W. Logan  
MM3/M. S. Soots  
MQ/M. D. Erminger  
MS/L. D. Austin, Jr.  
MT/R. M. Swalin  
MV/R. D. Dittimore  
OA/R. H. Brinkley  
XA/G. J. Harbaugh  
YA/F. L. Culbertson, Jr.

MA2/AMLarsen:km:6/12/97:31207

Retyped: MA2/AMLarsen:km:8/20/97:31207

# **FAIL SAFE APPROACH** **FOR** **COMPUTER-BASED CONTROL SYSTEMS**

**FAIL SAFE COMPUTER-BASED CONTROL SYSTEMS.** The use of "Fail Safe" control systems shall be limited to those applications where a computer-based control system can be interrupted after a failure occurs without resulting in an impending hazard to the orbiter, International Space Station, or crew. The intent of the "Fail Safe" concept is to allow validated computer-based control system designs that have multiple functionally unique computers (and/or firmware controllers) that reliably detect the first failure and transition the system to a safe state when a failure is detected. In order to meet the requirements of the "Fail Safe" approach, the Payload Organization must comply with all ten of the following items:

1. **FORMAL DEVELOPMENT PROCESS.** The hardware and software shall be developed under a formal development process that ensures that the system and safety requirements are met throughout the life cycle of the system.
2. **FAULT CONTAINMENT.** A "Fail Safe" computer-based control system shall be designed with an architecture that prevents the propagation of faults (which affect function) from one computer to another computer. A failure occurring within a computer or its interfaces shall not prevent other computers from performing their intended safety functions. All expected (normal) computer-to-computer interactions must be verified safe during developmental testing and analysis. Design features shall be in place that provide detection for each unexpected interaction. The quantity and complexity of computer-to-computer interactions shall be minimized.
3. **FAILURE/ERROR DETECTION.** A function must be implemented that monitors the status of the hardware and/or software components within the computers, detects failures/errors, and provides notification of error messages. The failure/error detection program shall actively monitor the system during hazardous control operations. During power-up or restart, the system shall initiate self-test functions to ensure that computers are healthy and ready for operation. Integrity checks must be performed when data or commands are retrieved from memory or when data or commands are exchanged between entities such as computers, transmission/reception lines, and devices.
4. **CONTROLLED SYSTEM FAILURE DETECTION.** The system must contain the capability for real-time detection of failures in the controlled system. When a detector is used for closed loop control a different detector must be used to satisfy the requirement for real-time detection of failures in the controlled system.
5. **FAILURE RESPONSE.** When a failure is detected, a system failure will be declared and system activity will be halted. The remaining computers will assist in the immediate issuance of the appropriate safing actions consistent with Paragraph 201, independent of the failed computer or hazard control. After a failure, system operations must be suspended until the failure is resolved or substitute component(s) can be brought on line. A computer cannot be solely responsible for detecting and safing its own hardware failures or software corruptions that can affect the safe operation of the payload.
6. **INDEPENDENCE.** Each computer, as a minimum, shall have independent power and independent clocks unless the system can be verified to be safe during power and/or timing anomalies. Each computer shall be unique in functionality and implementation of the software/firmware. A single computer shall be incapable of satisfying all of the requirements for the initiation of a hazardous event without concurrence from another computer. Additionally, a single computer shall not control more than one of the system hazard controls for a specific hazard without concurrence from another computer.

Enclosure  
Page 1 of 2



7. **PREREQUISITE CHECKS.** The system (in at least one computer) shall verify prerequisites prior to command issuance to ensure that each command is valid and in the proper sequence.
8. **PROCEDURAL FAULT TOLERANCE.** The operator interface shall be designed such that deliberate actions are required (consistent with the hazard level) to initiate a hazardous event.
9. **RECONFIGURATION FOR SAFE RETURN.** Fail Safe control system designs which present no immediate hazard after a failure, but must be reconfigured to permit orbiter safe return, shall have design features that permit safing for return. The design features that permit safing for return shall be independent of the failed control system and provide a level of fault tolerance appropriate to the hazard potential associated with orbiter return.
10. **HAZARD DETECTION AND SAFING.** The need for hazard detection and safing by a computer-based control system to control time-critical hazards will be minimized and implemented only when an alternate means of reduction or control of hazardous conditions is not available. Hazard detection and safing may be utilized to support control of hazardous functions provided that adequate system response time is available and demonstrated by test.

National Aeronautics and  
Space Administration

**Lyndon B. Johnson Space Center**  
2101 NASA Road 1  
Houston, Texas 77058-3696



Reply to Attn of :

MA2-98-069

September 11, 1998

TO: Distribution

FROM: MA2/Manager, Space Shuttle Program Integration  
OA/Deputy Manager for Technical Development International Space Station  
Program

SUBJECT: Small Commonly Used Batteries

The information contained in this letter is an interpretation and clarification of the safety policy for the Space Shuttle Program (SSP) and the International Space Station Program (ISSP). This letter applies to all SSP and ISSP payloads; i.e., payloads required to comply with either NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System (STS)," or NSTS 1700.7B Addendum, "Safety Policy and Requirements for Payloads Using the International Space Station," and will be utilized by the flight Payload Safety Review Panel in assessing compliance. The safety requirements being clarified are in paragraph 213.2. Please add this letter to your copy of NSTS/ISS 18798B, "Interpretations of NSTS/ISS Payload Safety Requirements."

This letter is intended to clarify the safety policy regarding the design conditions and acceptance tests required when "small commonly used batteries" are used in space applications. Meeting the design conditions and acceptance test criteria exempts the payload organization from submitting a detailed hazard report as well as incorporating special design features such as fuses, thermostats, and electrolyte absorbent material for these batteries. Upon meeting the design conditions below, readily replaceable flight batteries must undergo a preflight Acceptance Test. The Acceptance Test shall include an open circuit voltage measurement, cell loaded voltage test, dimensional check, and inspection for leakage before and after an exposure to vacuum, e.g., 6 hours at 0.1 psia.

The batteries identified as "small commonly used batteries" are of two types. The first type are button cells of 200 milliamp hours or less. Only button cell batteries made from lithium-carbon monofluoride, lithium-iodine, lithium-manganese dioxide, nickel-cadmium, nickel-metal hydride, silver-zinc, and zinc-air qualify for inclusion, dependent on capacity and design conditions. These batteries are typically used for memory back-up and appear to be widely used in payload hardware, especially in commercial off-the-shelf components. Button cell batteries soldered into commercial hardware and meeting the design condition requirements may be accepted with a visual inspection of battery condition and a hardware functional test. The specific design condition requirements for button cells are that they include no more than three per circuit with no series-parallel combinations, they are not enclosed in a sealed compartment, and they have no potential for hazardous charging.

The second type batteries are the alkaline-manganese, carbon-zinc, and zinc-air batteries of sizes D or smaller. The specific design condition requirements for this type are that they include no more than six per circuit with no series-parallel combinations, they are not enclosed in a sealed compartment, and they have no potential for hazardous charging from other circuits or designed-in charging circuits.

Assurance of adequate shelf life for the mission should be considered for mission success and evaluated for the payload application. Prolonged storage may cause cell deterioration which is not readily evident, but may have safety implications. This shall be addressed in the Safety Data Package.

These criteria are intended to provide savings in the payload safety review process without compromising payload safety. Payload providers shall describe their usage of these batteries including installed locations, quantities and spares, purpose, type, capacity, and manufacturers, within their safety data submittal. They shall also affirm full compliance with the design conditions and safety requirements herein or describe any coordinated exceptions within their safety data submittal.

In summary, the acceptance test required and design conditions for "small commonly used batteries," coupled with the flight crews' ability to recognize faulty batteries (hot, swollen, or leaking battery case), and their ability to take appropriate action, will provide adequate measures to ensure safety has not been compromised. For future payloads, these battery criteria will be applied by the Payload Safety Review Panel. The payload organization should use the JSC Form 1230, "Flight Payload Standardized Hazard Control Report," as a simplified method for reporting of "small commonly used batteries."

Questions concerning this subject should be addressed to the Executive Secretary, Space Shuttle Payload Safety Review Panel, mail code NC4, telephone (281) 483-8848.

William H. Gerstenmaier

Jay H. Greene

Distribution:

CB/G. D. Griffith  
DO12/J. M. Childress  
EA4/R. J. Wren  
MS3/K. B. Packard  
NC4/M. L. Ciancone  
OE/S. L. Thomas  
OZ3/D. W. Hartman  
SD2/M. E. Coleman

cc:  
See List

cc:

HQ/M-4/G. W. McClain  
HQ/M-7/W. F. Readdy  
HQ/ME/C. T. Holliman  
HQ/MO/R. L. Elsbernd  
KSC/AA-D/J. H. Morgan  
KSC/MK/D. R. McMonagle  
KSC/MK-SIO/R. L. Segert

bc:

CA/D. C. Leestma  
CB/K. D. Cockrell  
DA/B. R. Stone  
EA/L. S. Nicholson  
EA4/J. W. Aaron  
MA/T. W. Holloway  
MG/R. H. Heselmeyer  
MM/J. B. Costello  
MM3/M. S. Soots  
MQ/M. D. Erminger  
MS/L. D. Austin, Jr.  
MT/R. M. Swalin  
MV/R. D. Dittmore  
NS2/R. G. Alexander  
OA/R. H. Brinkley  
XA/G. J. Harbaugh  
YA/F. L. Culbertson, Jr.

MA2/AMLarsen:cdm:31207

## **NSTS 18798 Rev A - Interpretation Letter Disposition Summary (Appendix A)**

## NSTS 18798 Rev A - Interpretation Letters Disposition Summary (Appendix A)

Letter No.	Disposition	Title	Synopsis	Category	Comments
1	Delete; Rev. A group letter	Mandatory Requirement Changes for Payloads Using NHB 1700.7A (TA-87-079)	Return to flight. Basic content incorporated into "B" Rev. Enclosed letter TA-87-050 content in para. 218 and hazardous command list required by 13830.	Payload Design	NSTS 1700.7B includes intent.
2	Delete	Pressure Vessel Safety in Abort Condition (ES52-87-238M)	Heating conditions at contingency landing sites and affect on pressure vessels.	Pressure	Superseded by TA-90-008
3	Delete; Rev. A group letter	Orbiter Failure Modes with Payload Impact (NS2/89-MO31)	NSTS 16979 issued to define credible Orbiter failure modes for consideration during payload failure analyses.	Orbiter Systems	Included in JSC 16979 (FMFT for Orbiter)
4	Delete	Payload Power Feeder Reliability (PH-M139-80)	Configuration and failure modes of the four Orbiter fused main DC power feeds.	Payload Operations	Included in JSC 16979 (FMFT for Orbiter)
5	Keep	Monitoring for Safety (TA-88-018)	Requirements for real-time monitoring and near-real-time monitoring.	Payload Operations	
6	Delete	Rotation of a Payload S&A Device (NS2/82-L095)	S&A rotation prior to launch/testing on ground	Payload Operations	Responsibility of KSC ground operations, not the flight PSRP
7	Delete; Rev. A group letter	Safe Distance for Operation of Liquid Propellant Thrusters (TA-89-009)	Combines two curves from previous letters into one.	Propellant Systems	Rev. B of 1700.7 includes curves.
8	Superseded	Pyrotechnically Operated Isolation Valves (NS/87-L051)	Use of pyro isolation valves as equivalent of more than one propellant flow control device.	Pyros	Replaced by TA-92-049 (#34)
9	Delete	Latch Valve Overheating in Hydrazine Systems (NS2/85-L274)	Tests/verifications to qualify materials for hydrazine systems based on worst case system temperatures.	Propellant Systems	1700.7B, para. 202.2c includes intent.
10	Delete	Increased Catalytic Effect of Materials on Hydrazine Decomposition (NS2/83-L069)	Decomposition potential must be evaluated at peak system temperatures.	Propellant Systems	1700.7B para. 202.2c includes intent.
11	Delete	Temperature Limits in Bipropellant Systems (NS2/86-L206)	Over temperature limits for MMH and N2O4 propulsion systems.	Propellant Systems	Incorporated in 1700.7B para. 202.2c
12	Delete	Cargo Produced Radiation from Transmitter Antenna Systems (NS2/85-L187)	Expands requirements in 1700.7A by defining limits for 2 & 3 inhibits.	Radiated Emissions	NSTS 1700.7B includes intent in para. 202.5

## NSTS 18798 Rev A - Interpretation Letters Disposition Summary (Appendix A)

13	Delete	Effects of Orbiter Ku-Band Radiation (TJ2-87-136)	Orbiter-produced radiated fields from Ku-band transmitter and affect on payloads, ordnance, critical circuitry and personnel.	Radiated Emissions	Information letter only
14	Superseded	Rapid Safing (TA-88-025)	Emergency deorbit: close PLBD in 20 minutes; Next Primary Landing Site: Close PLBD in 50 min.	Payload Operations (Rapid Safing)	Superseded by MA3-94-020 (#42)
15	Delete	Fracture Control for Payloads (ES52-89-015L)	NHB 8071.1, "Fracture Control Requirements for Payloads Using the NSTS."	Structures/ Materials	Intent included in NASA-STD-5003
16	Delete	Fracture Control Ductile Screening and Visual Inspection (ES52-88-200L)	Applies to 1700.7A customers.	Structures/ Materials	Intent included in NASA-STD-5003
17	Delete	Certification Requirements for Beryllium (ES2-47-87)	Use of beryllium for primary structure in shuttle payloads.	Structures/ Materials	Included in NSTS 14046
18	Keep	Fault Tolerance of Systems Using Specially Certified Burst Disks (TA-88-074)	When burst-disks are considered single fault tolerant.	Pressure	
19	Delete/error	Standards for Pyrotechnics on NSTS Payloads (PE5-88-L278)	Further explanation of MIL-STD	Pyros	Letters not needed when using MIL-STD 1576 which is now required.
20	Delete	Shielding Payload Pyrotechnics Devices (NS2-85-L303)	Shielding requirements relaxed for MIL-STD-1512.	Pyros	Not needed when using MIL-STD-1576 (see #19).
21	Superseded	Protection of Power Distribution Circuitry (ER-87-326)	Payload Wire Sizing and Circuit Protection.	Electrical	Superseded by TA-92-038.
22	Keep	Ignition of Flammable Payload Bay Atmosphere (NS2/81-MO82)	Prevented by control of ignition sources.	Flammable Atmosphere	
23	Delete	Protecting Windows from Damage (ES2-89-10)	Micrometeoroid and space debris environments and window protections methods.	Structures/ Materials	NSTS 1700.7B para 220.7a includes intent.
24	Keep	Pressure Stabilized Tanks (TA-89-064)	Existence of minimum required tank pressure must be verified prior to application of safety critical loads.	Pressure	
25	Delete	Payload Malfunction Procedures (DH-89-149)	Malfunction procedures must be in agreement with documented payload hazard reports.	Payload Operations	Operations in the presence of failure is the responsibility of Mission Operations.
26	Delete	Pressure Vessel Safety in Abort Condition (TA-90-008)	Supersedes # 2, ES52-87-238M. MDP shall be maintained under any conditions at any landing site.	Pressure	Only purpose was to cancel letter #2; now it's not needed.

## NSTS 18798 Rev A - Interpretation Letters Disposition Summary (Appendix A)

27	Superseded	Spacelab Module Rapid Safing (TA-89-085)	Expand on TA-88-025 rapid safing letter for Spacelab.	Payload Operations (Rapid Safing)	Superseded by MA3-94-020 (#42)
28	Keep	Separation of Redundant Safety-Critical Circuits (ET12-90-115)	Wire bundles are considered any group of wires spot-tied or clamped together.	Electrical	
29	Delete	Cargo Bay Power Feeder Fault Tolerance (TA-91-006)	Expands on PH-M139-80. Conditions where separate branches of payload power distribution circuit derived from a single 0 AWG Orbiter power feeder are considered single fault tolerant.	Orbiter Systems	Included in JSC 16979 (FMFT for Orbiter)
30	Keep	Structural Requirements for Contingency Deorbit (NS2/90-208)	Payload must maintain positive structural margin under contingency deorbit conditions without preconditioning.	Structures/Materials	
31	Keep	Payload Commanding (POCC) (TA-91-062)	Hazard report required for issuance of hazardous commands from POCC or ground equipment.	Payload Operations	
32	Keep	Circuit Design for Payloads Using Energy Storage Devices for Pyrotechnic Firing Circuits (TA-91-077)	Warning on energy storage NSI firing device (PIC's, etc.)	Pyros	
33	Delete	Low Risk Fracture Parts (TA-92-013)	Requirements for low risk fractures parts.	Structures/Materials	NASA-STD-5003 covers this subject
34	Keep	Pyrotechnically Operated Isolation Valves for Payloads (TA-92-049)	Criteria under which failure of pyrovalve with minimum of one flow barrier is considered noncredible single barrier failure.	Pyros	
35	Keep	Protection of Payload Electrical Power Circuits (TA-92-038)	Supersedes ER-87-326; EH5-83-88; EH13-82-191	Electrical	ISS uses SSP 52000 (See 1700.7b ISS Addendum, para 213.1)
36	Delete	Payload Use of Orbiter General Purpose Computer (TC3-93-017)	Requirement for payloads using GPC to command inhibits to hazardous functions.	Orbiter Systems	Included in JSC 16979 (FMFT for Orbiter)
37	Keep	Structural Integrity Following Mechanism Failures (TA-93-037)	Payloads should provide two-failure tolerance against load redistribution caused by credible mechanism failures.	Structures/Materials	



## NSTS 18798 Rev A - Interpretation Letters Disposition Summary (Appendix A)

38	Keep	Safety Policy for Detecting Payload Design Errors (TA-94-018)	ACTS/TOS firing of primary and secondary SUPER*ZIP explosive cords. Need for vigorous verification of function versus design.	Pyros	
39	Keep	Mechanical Systems Safety (TA-94-041)	Consolidates major PSRP policy decisions regarding design and operation of electro-mechanical systems.	Structures/ Materials	
40	Delete	Modified Fracture Control Criteria and Guidelines for Payloads (TA-94-057)	Pressure vessels; rotating parts; sealed containers; low released mass; containment of loose parts; batteries.	Structures/ Materials	Intent included in NASA-STD-5003
41	<del>Keep</del> Delete	Crew Mating/Demating of Powered Connectors ( <del>MA2-97-093</del> ) <del>A3-94-002</del>	Elimination of potentially hazardous levels of energy by limiting energy of power source.	Payload Operations	Superseded by MA2-99-17097-093, dated <del>March 17, 1998</del> <u>February 10, 2000</u>
42	Delete	Contingency Return (MA3-94-020)	Supersedes TA-88-025 and TA-89-085.	Payload Operations (Rapid Safing)	
43	Keep	Thermal Limits for Intravehicular Activity (IVA) Touch Temperatures (MA2-95-048)	Intentional contact and incidental contact.	Crew IVA Hazards (Touch Temperature)	
44	Keep	Low Risk Fracture Part Clarification (MA2-96-174)	Expands use of low risk fracture part classification to parts and resolve interpretation problems encountered with TA-92-013.	Structures/ Materials	
45	Keep	Contingency Return and Rapid Safing (MA2-96-190)	Supersedes MA3-94-020	Payload OPS (Rapid) Safing	