NSTS 1700.7B

Safety Policy and Requirements

IN-16-
317960
P-59

For Payloads Using the Space Transportation System

January 1989

(NASA-TM-103437) SAFETY POLICY AND REQUIREMENTS FOR PAYLOADS USING THE SPACE TRANSPORTATION SYSTEM (NASA) 59 p CSCL 22B

N91-12724

Unclas
G3/16 0317960

National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas

DESCRIPTION OF CHANGES TO
SAFETY POLICY AND REQUIREMENTS FOR PAYLOADS USING THE SPACE TRANSPORTATION SYSTEM

CHANGE NO.	DESCRIPTION/AUTHORITY	DATE	PAGES AFFECTED
--	Basic issue/R21700-1	1/13/89	All

This document replaces NHB 1700.7A as stipulated in preface.

The R21700 CR number is being used to facilitate the MICB Automated Payload Tracking System (AMPTS) and still retain NSTS 1700.7B as the document number.

PREFACE

DATE: JANUARY 13, 1989

The National Space Transportation System (NSTS) safety policy is to maintain the assurance of a safe operation while minimizing NSTS involvement in the design process of the payload and its ground support equipment. Requirements for assuring payload mission success are the responsibility of the payload organization and are beyond the scope of this document. The intent is to provide the overall STS safety policies and requirements while allowing the payload organization the latitude to determine the best design to meet mission objectives and still comply with those NSTS safety policies and requirements.

NSTS 1700.7B is an extensive revision of NHB 1700.7A that reflects the increased safety awareness of the NSTS that has resulted from the STS-51L Challenger mishap. The successful completion of the safety process will require positive feedback that all safety verification has been completed. Although paragraphs 200, 201, and 202 were completely rewritten, the basic philosophy of failure tolerance with inhibit monitoring to control hazards has not changed. Other paragraphs were changed to incorporate new or revised policy. Some of the paragraphs that may appear to contain new requirements are actually existing policies that were already being implemented through the safety review process and NHB 1700.7A. Those new requirements of this document that are considered mandatory for all payloads prior to the return of the STS to flight status have been issued to the STS payload community by separate letter.

The requirements of NSTS 1700.7B will be levied on new and existing NSTS payloads, if NSTS 1700.7B is specifically referenced in the approved payload integration plan (PIP) between the payload and the NSTS. Payload organizations which already have an approved PIP may elect to change the PIP and implement NSTS 1700.7B. Even if a payload is not required to comply with NSTS 1700.7B, it should be used extensively as a reference document since it contains significant clarifications of existing NHB 1700.7A requirements.

Subject to the provisions above, NSTS 1700.7B supersedes NHB 1700.7A, dated December 9, 1980.

Arnold D. Aldrich
Director, National Space Transportation System

TABLE OF CONTENTS

CHAPTER 3: SYSTEM PROGRAM REQUIREMENTS

CHAPTER 1: GENERAL

100 PURPOSE

This document establishes the safety policy and requirements applicable to Space Transportation System (STS) payloads and their ground support equipment (GSE).

101 SCOPE

These requirements are intended to protect flight and ground personnel, the STS, other payloads, GSE, the general public, public-private property, and the environment from payload-related hazards. This document contains technical and system safety requirements applicable to STS payloads (including payload-provided ground and flight support systems) during ground and flight operations.

101.1 **GSE Design and Ground Operations.** For additional safety requirements which are unique to ground operations and GSE design, one shall refer to the joint Space and Missile Test Organization (SAMTO)/Kennedy Space Center (KSC) Handbook, SAMTO HB S-100/KHB 1700.7.

101.2 **Flight Rules.** Flight rules will be prepared for each STS 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 STS flight consistent with crew safety. Compliance with minimum safety requirements of this document will not insure the mission success of a payload. For example, if an STS user only monitors two of three inhibits to a catastrophic hazardous function (this is the minimum requirement specified in paragraph 201.3), a flight rule related to the loss of a monitored inhibit may be imposed which is not favorable to the mission success of the payload.

102 RESPONSIBILITY

102.1 **Payload Organization.** It is the responsibility of each payload organization to assure the safety of its payload and to implement the requirements of this document. Where a payload integration or mission management organization is identified, that organization interfaces with the NSTS on behalf of the group of individual payload elements or experiments under its control. That organization has the responsibility to assure that the individual payload elements are safe and meet the requirements of this document. That organization also has the responsibility to assure that interaction among its payload elements does not create a hazard.

102.2 **NSTS.** It is the responsibility of the NSTS to interface with the responsible payload organization to review the payload for adequate safety implementation. It is also the responsibility of the NSTS to assure that interaction among mixed payloads, and between payloads and the STS, does not create a hazard.

103 IMPLEMENTATION

This document identifies the safety policy and requirements which are to be implemented by the payload organization. The implementation of safety requirements by the payload organization will be assessed by the NSTS during the safety review process and must be consistent with hazard potential. The NSTS assessment of safety compliance will include a complete review of the safety assessment reports (paragraph 301) and may include audits and safety inspections of flight hardware. The detailed interpretations of these safety requirements will be by the NSTS, and will be determined on a case-by-case basis consistent with the payload's hazard potential. The following supplementary documents have been issued to assist payload organization in complying with the requirements of this document.

103.1 **Implementation Procedure.** NSTS 13830, a jointly issued Johnson Space Center (JSC) and Kennedy Space Center (KSC) document, has been published to assist the payload organization in implementing the system safety requirements and to define further the safety analyses, data submittals, and safety assessment review meetings. NSTS 13830 identifies the respective roles of the NSTS flight operator and the NSTS launch/landing site operator. It reflects a basic policy of commonality, compatibility, and coordination between the NSTS flight and ground elements in the implementation effort.

103.2 **Interpretations of Requirements.** NSTS 18798 is a collection of interpretations of requirements relative to specific payload designs. These interpretations shall be applied to payloads that utilize similar design solutions. Addenda to NSTS 18798 are distributed to payload organizations as additional interpretations are generated.

104 GLOSSARY OF TERMS

For definitions applicable to this document, see Appendix A.

105 APPLICABLE DOCUMENTS

A list of documents which are referenced in this document is in Appendix B.

106 FIGURES

Figures referred to in the text are contained in Appendix C.

CHAPTER 2: TECHNICAL REQUIREMENTS

200 GENERAL.

The following requirements are applicable to all payloads. When a requirement cannot be met, a noncompliance report must be submitted in accordance with NSTS 13830 for resolution.

200.1 **Design to Tolerate Failures.** Failure tolerance is the basic safety requirement that shall be used to control most payload hazards. The payload must tolerate a minimum number of credible failures and/or operator errors determined by the hazard level. This criterion applies when the loss of a function or the inadvertent occurrence of a function results in a hazardous event.

200.1a **Critical Hazards.** Critical hazards shall be controlled such that no single failure or operator error can result in damage to STS equipment, a nondisabling personnel injury, or the use of unscheduled safing procedures that affect operations of the Orbiter or another payload.

200.1b **Catastrophic Hazards.** Catastrophic hazards shall be controlled such that no combination of two failures or operator errors can result in the potential for a disabling or fatal personnel injury or loss of the Orbiter, ground facilities or STS equipment.

200.2 **Design for Minimum Risk.** Payload hazards which are controlled by compliance with specific requirements of this document other than failure tolerance are called "Design for Minimum Risk" areas of design. Examples are structures, pressure vessels, pressurized line and fittings, functional pyrotechnic devices, mechanisms in critical applications, material compatibility, flammability, etc. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the payload organization and the NSTS. Minimum supporting data requirements for these areas of design have been identified in NSTS 13830.

200.3 **Environmental Compatibility.** A payload shall be certified safe in the applicable worst case natural and induced environments defined in the payload integration plan (PIP) and/or interface control document (ICD).

200.4 STS Services

200.4a **Safe Without Services.** Payloads shall be designed to maintain fault tolerance or safety margins consistent with the hazard potential without ground or flight NSTS services. During Orbiter emergency conditions, power will be provided temporarily to payloads for payload safing and verification if necessary. Subsequent to payload safing, power may not be available to payloads. Monitoring is not mandatory under these conditions.

200.4b **Critical Orbiter Services.** When NSTS services are to be utilized to control payload hazards, the integrated system must meet the failure tolerance requirements of paragraph 200.1 and adequate redundancy of the NSTS services must be negotiated. JSC 16979 specifies the fault tolerance of Orbiter-provided payload services which must be used when conducting payload hazard analyses. The payload organization must provide a summary of the hazards being controlled by STS services in the safety assessment report (see paragraph 301) and document in the individual hazard reports those Orbiter interfaces used to control and/or monitor the hazards. Those payload hazards being controlled by Orbiter-provided services will require post-mate interface test verification for both controls and monitors. In addition, the payload organization shall identify in the payload/Orbiter ICD those Orbiter interfaces used to control and/or monitor the hazards.

201 CONTROL OF HAZARDOUS FUNCTIONS

201.1 **General.** Hazardous functions are operational events (e.g., motor firings, appendage deployments, stage separations, and active thermal control) whose inadvertent operations or loss may result in a hazard.

201.1a **Inhibits.** An inhibit is a design feature that provides a physical interruption between an energy source and a function (a relay or transistor between a battery and a pyrotechnic initiator, a latch valve in the plumbing line between a propellant tank and a thruster, etc.). Two or more inhibits are independent if no single credible failure, event, or environment can eliminate more than one inhibit.

201.1b **Controls**. A device or function that operates an inhibit is referred to as a control for an inhibit. Controls do not satisfy the inhibit or failure tolerance requirements for hazardous functions. The "electrical inhibits" in a liquid propellant propulsion system ([paragraph 202.2a(3)]) are exceptions in that these devices operate the flow control devices (i.e., mechanical inhibits to propellant flow), but are referred to as inhibits and not as controls.

201.1c **Monitors**. Monitors are used to ascertain the safe status of payload functions, devices, inhibits and parameters. 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. In addition, loss of input or failure of the monitor should cause a change in state of the indicator. Monitoring shall be available to the launch site when necessary to assure safe ground operations. Notification of changes in the status of safety monitoring shall be given to the flightcrew in either near-real-time or real-time.

201.1c(1) **Near-Real-Time Monitoring**. Near-real-time monitoring (NRTM) is defined as notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). NRTM may be accomplished via ground crew monitored telemetry data. Switch talk backs shall not be used as the only source of safety monitoring when the hazard exists during crew sleep periods.

201.1c(2) **Real-Time Monitoring**. Real-time monitoring (RTM) is defined as immediate notification to the crew. RTM shall be accomplished via the use of the Orbiter failure detection and annunciation system or by ground crew monitored telemetry data. An exception to this would be where RTM is necessary only during payload operations. Under these conditions, switch panel talk back monitoring is acceptable. Real-time monitoring of inhibits to a catastrophic hazardous function is required when changing the configuration of the applicable payload system or when the provisions of paragraph 204 are implemented for flightcrew control of the hazard. If ground monitoring is used to meet real-time monitoring, a continuous real-time data link (containing the applicable safety parameters) must be assured by the payload and continuous communications between the flight and ground crews must be established and maintained during the required period.

201.1c(3) **Unpowered Bus Exception.** Monitoring and safing of inhibits for a catastrophic hazardous function will not be required if the function power is deenergized (i.e., an additional fourth inhibit is in place between the power source and the three required inhibits) and the control circuits for the three required inhibits are disabled (i.e., no single failure in the control circuitry will result in the removal of an inhibit) until the hazard potential no longer exists.

201.1d **Use of Timers.** When timers are used on deployable payloads to control inhibits to hazardous functions, complete separation of the payload from the Orbiter must be achieved prior to the initiation of the timer. If credible failure modes exist that could allow the timer to start prior to a complete separation, a safing capability must be provided. If this safing is via a radio frequency (RF) command, then the command capability must be provided to the flightcrew.

201.1e **Computer-Based Control Systems.**

201.1e(1) **Active Processing to Prevent a Catastrophic Hazard.** While a computer system is being used to actively process data to operate a payload system with catastrophic potential, the catastrophic hazard must be prevented in a two-failure tolerant manner. One of the methods to control the hazard must be independent of the computer system. A computer system shall be considered zero fault tolerant in controlling a hazardous system (i.e., a single failure will cause loss of control), unless the system utilizes independent computers, each executing uniquely developed instruction sequences to provide the remaining two hazard controls.

201.1e(2) **Control of Inhibits.** The inhibits to a hazardous function may be controlled by a computer-based system used as a timer, provided the system meets all the requirements for independent inhibits.

201.2 **Functions Resulting in Critical Hazards.** A function whose inadvertent operation could result in a critical hazard must be controlled by two independent inhibits, whenever the hazard potential exists. Requirements for monitoring (paragraph 201.1c) of these inhibits and for the capability to restore inhibits to a safe condition are normally not imposed, but may be imposed on a case-by-case basis. Where loss of a function could result in a critical hazard, no single credible failure shall cause loss of that function.

201.3 **Functions Resulting in Catastrophic Hazards.** A function whose inadvertent operation could result in a catastrophic hazard must be controlled by a minimum of three independent inhibits, whenever the hazard potential exists. One of these inhibits must preclude operation by an RF command or the RF link must be encrypted. In addition, the ground return for the function circuit must be interrupted by one of the independent inhibits. At least two of the three required inhibits shall be monitored (paragraph 201.1c). If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

202 SPECIFIC CATASTROPHIC HAZARDOUS FUNCTIONS

In the following subparagraphs, specific requirements related to inhibits, monitoring, and operations are defined for several identified potentially catastrophic hazardous functions.

202.1 **Solid Propellant Rocket Motors.** Premature firing of a solid propellant rocket motor, while the payload is closer to the Orbiter than the minimum safe distance, is a catastrophic hazard.

202.1a **Safe Distance.** The safe distance for firing a solid rocket motor is defined as the separation distance achieved 45 minutes after deployment with the payload coasting with a minimum separation velocity of 1 foot per second. Payloads with a positive separation velocity less than 1 foot per second either:

(1) Shall provide an RF command capability as a flight crew function to inhibit automatic sequencing until a safe distance is assured; or

(2) Shall initiate payload sequencing (such as, starting a timer that will remove inhibits to cause

engine firing) by a real-time RF command with prior NSTS coordination and approval and the RF command to start sequencing shall not be sent until a safe separation distance is assured. For payloads deployed with the Remote Manipulator System (RMS), sequencing shall be initiated by a real time RF command.

202.1b **Safe and Arm (S&A) Device.** All solid propellant rocket motors shall be equipped with an S&A device that provides a mechanical interrupt in the pyrotechnic train immediately downstream of the initiator. The S&A device shall be designed and tested in accordance with provisions of MIL-STD-1576. If the S&A device is to be rotated to the arm position prior to the payload achieving a safe distance from the Orbiter: rotation must be a flightcrew function and must be done as part of the final deployment activities of the payload; and the initiator must meet the requirements of paragraph 210. The S&A must be in the safe position during Orbiter boost and entry. There must be a capability to resafe the S&A device: if the S&A device is to be rotated to the arm position while the payload is attached to the Orbiter; or if the solid rocket motor propulsion subsystem does not qualify for the unpowered bus exception of paragraph 201.1c(3). In determining compliance with paragraph 201.1c(3), the S&A device in the "safe" position shall be counted as one of the required inhibits.

202.1c **Electrical Inhibits.** In addition to the S&A, there shall be at least two independent electrical inhibits, to prevent firing of the motor if the S&A device will be in the "safe" position until the payload reaches a safe distance from the Orbiter. There shall be at least three independent electrical inhibits, in addition to the S&A, if the S&A device will be rotated to the arm position prior to the payload reaching a safe distance from the Orbiter.

202.1d **Monitoring.** Monitoring requirements are a function of the design and operations as follows:

202.1d(1) **No Rotation of the S&A Prior to a Safe Distance.** The capability to monitor the status of the S&A device and one electrical inhibit in near real-time is required until final separation of the payload from the Orbiter. No monitoring is required if the payload qualifies for the unpowered bus exception of paragraph 201.1c(3).

202.1d(2) **S&A Will be Rotated to Arm Prior to a Safe Distance.** Prior to rotation of the S&A and separation of the payload from the Orbiter, the flight or ground crew must have continuous real-time monitoring to determine the status of the S&A and to assure that two of the three electrical inhibits are in place (paragraph 201.1c(2)).

202.2 **Liquid Propellant Propulsion Systems.**

202.2a **Premature Firing.** The premature firing of a liquid propellant propulsion system before the payload reaches a safe distance from the Orbiter is a catastrophic hazard. Each propellant delivery system must contain a minimum of three mechanically independent flow control devices in series to prevent engine firing. A bipropellant system shall contain a minimum of three mechanically independent flow control devices in series both in the oxidizer and fuel sides of the delivery system. These devices must prevent contact between the fuel and oxidizer as well as prevent expulsion through the thrust chamber(s). Except during ground servicing and as defined in paragraph 202.2a(2)(a), these devices will remain closed during all ground and flight phases until the payload reaches a safe distance from the Orbiter. A minimum of one of the three devices will be fail-safe, i.e., return to the closed condition in the absence of an opening signal.

202.2a(1) **Safe Distance Criteria.** The hazard of engine firing close enough to inflict damage to the Orbiter due to heat flux, contamination, and/or perturbation of the Orbiter, is in proportion to the total thrust imparted by the payload in any axis and shall be controlled by establishing a safe distance for the event. The safe distance shall be determined using Figure 1 (see Appendix C). For large thruster systems with greater than 10 pounds total thrust, the collision hazard with the Orbiter must be controlled by considering the safe distance criteria in Figure 1, together with the correct attitude at time of firing. For small reaction control system (RCS) thrusters with less than 10 pounds total thrust, the collision hazard must be controlled by the safe distance criteria in Figure 1 with consideration of many variables such as deployment method, appendage orientation, and control authority.

202.2a(2) Isolation Valve. One of the flow control devices shall isolate the propellant tank(s) from the remainder of the distribution system.

202.2a(2)(a) Opening the Isolation Valve. If a payload with a large liquid propellant thruster system also uses a small reaction control thruster system for attitude control, the isolation valve in a common distribution system may be opened after the payload has reached a safe distance for firing the reaction control thrusters provided the applicable requirements of paragraphs 202.2a(3) and 202.2a(4) have been met and two mechanical flow control devices remain to prevent thrusting of the larger system.

202.2a(2)(b) Pyrotechnic Isolation Valves. If a normally closed pyrotechnically initiated valve is used, it may be considered equivalent to two propellant flow control devices if the following requirements are fulfilled: The structural design must preclude operation by vibration. The valve must use parent metal in which the inlet and the first flow barrier are a continuous unit of nonwelded metal and the outlet and the last flow barrier are also a continuous unit of nonwelded metal. The valve must be controlled by at least two independent electrical inhibits (three electrical inhibits will be required if paragraph 202.2b is applicable).

202.2a(3) Electrical Inhibits. While the payload is closer to the Orbiter than the minimum safe distance for engine firing, there shall be at least three independent electrical inhibits that control the opening of the flow control devices. The electrical inhibits shall be arranged such that the failure of one of the electrical inhibits will not open more than one flow control device. If the isolation valve will be opened under the conditions of paragraph 202.2a(2)(a) prior to the payload achieving a safe distance for firing a large thruster, three independent electrical inhibits must control the opening of the remaining flow control devices for the large thruster system.

202.2a(4) Monitoring. At least two of the three required independent electrical inhibits shall be monitored by the flight or ground crew until final separation of the payload from the Orbiter. The position of a mechanical flow control device may be monitored in lieu of its electrical inhibit, provided the two monitors used to meet the above requirement are independent. Either near real-time or real-time monitoring will be required as defined in paragraphs 201.1c(1) and 201.1c(2). One of the monitors must be the electrical inhibit or mechanical position of the isolation valve. Monitoring will not be required if the payload qualifies for the unpowered bus exception of paragraph 201.1c(3). If the isolation valve will be opened prior to the payload achieving a safe distance from the Orbiter, all three of the electrical inhibits that will remain after the opening of the isolation valve must be verified safe during final predeployment activities by the flight or ground crew.

202.2b **Adiabatic/Rapid Compression Detonation.** While the payload is inside the Orbiter cargo bay, the inadvertent opening of isolation valves in a hydrazine (N_2H_4) propellant system shall be controlled as a catastrophic hazard unless the outlet lines are completely filled with hydrazine or the system is shown to be insensitive to adiabatic or rapid compression detonation. Hydrazine systems will be considered sensitive to compression detonation unless insensitivity is verified by testing on flight hardware or on a high fidelity flight type system that is constructed and cleaned to flight specifications. Test plans must be submitted to the NSTS as part of the appropriate hazard report. If the design solution is to fly wet downstream of the isolation valve, the hazard analysis must consider other issues such as hydrazine freezing or overheating, leakage, single barrier failures, and back pressure relief.

202.2c **Propellant Overheating.** Raising the temperature of a propellant above the fluid compatibility limit for the materials of the system is a catastrophic hazard. Components in propellant systems that are capable of heating the system (e.g., heaters, valve coils, etc.) shall be two-failure tolerant to heating the propellant above the material/fluid compatibility limits of the system. These limits shall be based on test data derived from NHB 8060.1 test methods or on data furnished by the payload supplier and approved by the NSTS. Propellant temperatures less than the material/fluid compatibility limit, but greater than 200 degrees Fahrenheit must be approved by the NSTS.

The use of inhibits, cutoff devices, and/or crew safing actions may be used to make the system two failure tolerant to overheating. Monitoring of inhibits (paragraphs 201.1c and 201.3) or of propellant temperature will be required.

202.2d **Propellant Leakage.** A payload shall be two failure tolerant to prevent leakage of propellant into the Orbiter cargo bay past seals, seats, etc., if the leak has a flow path to the storage vessel. If the leak is in an isolated segment of the distribution system, failure tolerance to prevent the leak will depend on the type and quantity of propellant that could be released. As a minimum such a leak will be one failure tolerant.

202.3 **Inadvertent Deployment, Separation, and Jettison Functions.** Inadvertent deployment, separation or jettison of a payload, payload element or appendage is a catastrophic hazard unless it is shown otherwise. The general inhibit and monitoring requirements of paragraph 201 shall apply.

202.4 **Planned Deployment/Extension Functions.**

202.4a **Preventing Payload Bay Door Closure.** If during planned payload operations an element of the payload or any payload airborne support equipment (ASE) violates the payload bay door envelope, the hazard of preventing door closure must be controlled by independent primary and backup methods. The combination of these methods must be two-fault tolerant. Two methods are considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

202.4b **Cannot Withstand Subsequent Loads.** If during planned operations an element of a payload or its ASE is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent STS induced loads, there shall be two-failure tolerant design provisions to safe the payload. Safing may include deployment, jettison or provisions to change the configuration of the payload to eliminate the hazard.

202.5 **RF Energy Radiation.** Allowable levels of radiation from payload transmitter antenna systems are defined in the ICD, NSTS 07700, Volume XIV, Attachment 1 (ICD-2 19001). These levels define payload-to-RMS, payload-to-Orbiter, and payload-to-payload limits. Radiation from payload transmitter antenna systems will not be allowed while the payload bay doors are closed and will be permitted with the payload bay doors open only if the ICD limits are not exceeded. The requirements to prevent inadvertent radiation are as follows:

202.5a **Payload Bay Doors Open.** With the payload bay doors opened, there shall be three independent inhibits whenever the impinging radiation would exceed the ICD limits.

202.5b **Payload Bay Doors Closed.** With the payload bay doors closed, there shall be two independent inhibits if the impinging radiation would be below the ICD limits and three independent inhibits if the radiation would be above the limits.

202.5c **Monitoring.** The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachment 1 (ICD-2-19001) limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

203 RETRIEVAL OF PAYLOADS

203.1 **Safing.** Deployable and/or free flying payloads that are designed to be retrieved or revisited shall have the capability to return systems which are hazardous to a safe condition (i.e., meet all the applicable requirements of this document).

203.2 **Substantiating Failure Tolerance.** Payloads must be designed so as to allow substantiation of safing by the Orbiter flightcrew or ground crew prior to retrieval and while the payload is still a safe distance from the Orbiter. By direct or indirect means, it must be substantiated that catastrophic hazardous functions are at least two-failure tolerant. Specific plans to be used to determine the safe status of a retrievable payload must be approved by the NSTS.

203.3 **Monitoring.** After retrieval, the monitoring requirements of paragraphs 201.1c and 201.3 will apply.

203.4 **Certification.** Prior to the NSTS retrieval or revisit mission, the payload organization must certify the safety of the payload. This certification must be based upon a hazard analysis that considers the effect of the current condition of the payload (including the impact of all anomalies) during all subsequent flight and ground operations with the STS.

204 HAZARD DETECTION AND SAFING

The need for hazard detection and safing by the flightcrew 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. When implemented, these functions will be capable of being tested for proper operations during both ground and flight phases and shall use existing Orbiter systems for fault detection and annunciation. Likewise, payload designs should be such that real-time monitoring is not required to maintain control of hazardous functions. With NSTS approval, real-time monitoring and hazard detection and safing may be utilized to support control of hazardous functions provided that adequate crew response time is available and acceptable safing procedures are developed.

205 CONTINGENCY RETURN AND RAPID SAFING

All payloads must be safe for aborts and contingency return and shall include design provisions for rapid safing. Hazard controls may include deployment, jettison or design provisions to change the configuration of the payload.

206 FAILURE PROPAGATION

The design shall preclude propagation of failures from the payload to the environment outside the payload.

207 REDUNDANCY SEPARATION

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.

208 STRUCTURES

208.1 **Structural Design.** The structural design shall provide ultimate factors of safety equal to or greater than 1.4 for all STS mission phases except emergency landing. This includes loads incurred during payload and Orbiter operations for all payload configurations or while changing configuration as specified in the PIP. Verification of design compliance shall be in accordance with NSTS 14046. When failure of structure can result in a catastrophic event, the design shall be based on fracture control procedures to prevent structural failure because of the initiation or propagation of flaws or crack-like defects during fabrication, testing, and service life. Requirements for fracture control are specified in NHB 8071.1.

208.2 **Emergency Landing Loads.** The structural design shall comply with the ultimate design load factors for emergency landing loads that are specified in the ICD's between the Orbiter and the payload. Structural verification for these loads may be certified by analysis only.

208.3 **Stress Corrosion.** Materials used in the design of payload structures, support bracketry, and mounting hardware shall be rated for resistance to stress corrosion cracking (SCC) in accordance with the tables in MSFC-HDBK-527/JSC 09604 and MSFC-SPEC-522. Alloys with high resistance to SCC shall be used whenever possible and do not require NSTS approval. When failure of a part made from a moderate or low resistance alloy could result in a critical or catastrophic hazard. a Material Usage Agreement that includes a Stress Corrosion Evaluation Form from MSFC-HDBK-527/JSC 09604 must be attached to the applicable stress corrosion hazard report contained in the safety assessment report (see paragraph 301). When failure of a part made from a moderate or low resistance alloy would not result in a hazard, rationale to support the nonhazard assessment must be included in the stress corrosion hazard report. Approval of the hazard report shall constitute NSTS approval for the use of the alloy in the documented applications. Controls that are required to prevent SCC of components after manufacturing shall be identified in the hazard report and closure shall be documented in the verification log (see paragraph 214.2) prior to flight.

208.4 **Pressure Systems.** The maximum design pressure (MDP) for a pressurized system shall be the highest pressure defined by maximum relief pressure, maximum regulator pressure or maximum temperature. Transient pressures shall be considered. Design factors of safety shall apply to MDP. Where pressure regulators, relief devices, and/or a thermal control system (e.g., heaters) are used to control pressure, collectively they must be two-fault tolerant from causing the pressure to exceed the MDP of the system. Pressure integrity shall be verified at the system level.

208.4a **Pressure Vessels.** Pressure vessels shall comply with the pressure vessel requirements of MIL-STD-1522A (including revisions as of December 1984) as modified by the paragraphs (1), (2), (3), (4) and (5) below. Particular attention shall be given to insure compatibility of vessel materials with fluids used in cleaning, test, and operation. Data requirements for pressure vessels are listed in NSTS 13830.

(1) Approach "B" of figure 2 is not acceptable.

(2) In addition to other required analyses, composite pressure vessels shall be assessed for adequate stress rupture life.

(3) Nondestructive evaluation (NDE) of pressure vessels shall include inspection of welds after proof testing.

(4) MDP as defined above (see paragraph 208.4) shall be substituted for all references to maximum expected operating pressure (MEOP).

(5) A proof test of each flight pressure vessel to a minimum of 1.5 x MDP and a fatigue analysis showing a minimum of 10 design lifetimes may be used in lieu of testing a certification vessel to qualify a vessel design that in all other respects meets the requirements of this document and MIL-STD-1522A, Approach A.

208.4b **Dewars.** Dewar/cryostat systems are a special category of pressurized vessels because of unique structural design and performance requirements. Pressure containers in such systems shall be subject to the requirements for pressure vessels specified in paragraphs 208.4 and 208.4a as supplemented by the requirements of this section.

(1) Pressure containers shall be leak-before-burst (LBB) designs where possible as determined by a fracture mechanics analysis. Containers of hazardous fluids and all non-LBB designs must employ a fracture mechanics safe-life approach to assure safety of operation.

(2) MDP of the pressure container shall be as determined in paragraph 208.4 or the pressure achieved under maximum venting conditions whichever is higher. Relief devices must be sized for full flow at MDP.

(3) Outer shells (i.e., vacuum jackets) shall have pressure relief capability to preclude rupture in the event of pressure container leakage. If pressure containers do not vent external to the dewar but instead vent into the volume contained by the outer shell, the outer shell relief devices must be capable of venting at a rate to release full flow without outer shell rupture. Relief devices must be redundant and individually capable of full flow.

(4) Pressure relief devices which limit maximum design pressure must be certified to operate at the required conditions of use. Certification shall include testing of the same part number from the flight lot under the expected use conditions.

(5) Nonhazardous fluids may be vented into the cargo bay if analysis shows that a worst case credible volume release will not affect the structural integrity or thermal capability of the Orbiter.

(6) The proof test factor for each flight pressure container shall be a minimum of 1.1 times MDP. Qualification burst and pressure cycle testing is not required if all the requirements of paragraphs 208.4, 208.4a and 208.4b are met. The structural integrity for external load environments must be demonstrated in accordance with NSTS 14046.

208.4c **Pressurized Lines, Fittings, and Components.**

(1) Pressurized lines and fittings with less than a 1.5-inch outside diameter and all flex-hoses shall have an ultimate factor of safety equal to or greater than 4.0. Lines and fittings with a 1.5-inch or greater outside diameter shall have an ultimate factor of safety equal to or greater than 1.5.

(2) All line-installed bellows and all heat pipes shall have an ultimate safety factor equal to or greater than 2.5.

(3) Other components (e.g., valves, filters, regulators, sensors, etc.) and their internal parts (e.g., bellows, diaphragms, etc.) which are exposed to system pressure shall have an ultimate factor of safety equal to or greater than 2.5.

(4) Secondary compartments or volumes that are integral or attached by design to the above parts and which can become pressurized as a result of a credible single barrier failure must be designed for safety consistent with structural requirements. These compartments shall have a minimum safety factor of 1.5 based on MDP. If external leakage would not present a catastrophic hazard to the Orbiter, the secondary volume must either be vented or equipped with a relief provision in lieu of designing for system pressure.

208.4d **Flow Induced Vibration.** Flexible hoses and bellows shall be designed to exclude flow induced vibrations which could result in a catastrophic hazard to the STS.

208.5 **Sealed Compartments.** Payload sealed compartments within a habitable volume, including containers which present a safety hazard if rupture occurs, shall be capable of withstanding the maximum pressure differential associated with emergency depressurization of the habitable volume. Payloads located in any other region of the Orbiter shall be designed to withstand the decompression and repressurization environments associated with ascent or decent.

209 MATERIALS

MSFC-HDBK-527/JSC 09604 contains a listing of materials (both metals and nonmetals) with a "rating" indicating acceptability for each material's characteristic. For materials which create potential hazardous situations as described in the paragraphs below and for which no prior

NASA test data or rating exists, the payload organization shall present other test results for NSTS review or request assistance from the NSTS in conducting applicable tests. The payload material requirements for hazardous materials, flammability, and offgassing are as follows:

209.1 **Hazardous Materials.** Hazardous materials shall not be released or ejected in or near the Orbiter. During exposure to all STS environments, hazardous fluid systems must contain the fluids unless the use of the Orbiter vent/dump provisions has been negotiated with the NSTS.

209.1a **Fluid Systems.** Particular attention shall be given to materials used in systems containing hazardous fluids. These hazardous fluids include gaseous oxygen, liquid oxygen, fuels, oxidizers, and other fluids that could chemically or physically degrade the system or cause an exothermic reaction. Those materials within the system exposed to oxygen (liquid and gaseous), both directly and by a credible single barrier failure, must meet the requirements of NHB 8060.1 at MDP and temperature. Materials within the system exposed to other hazardous fluids, both directly and by a credible single barrier failure, must pass the fluid compatibility requirements of NHB 8060.1 at MDP and temperature. The payload supplier's compatibility data on hazardous fluids may be used to accept materials in this category if approved by the NSTS.

209.1b **Chemical Releases.** The use of chemicals which would create a toxicity problem (including irritation to skin or eyes) or cause a hazard to STS hardware if released should be avoided. If use of such chemicals cannot be avoided, adequate containment shall be provided by the use of an approved pressure vessel as defined in paragraph 208.4 or the use of two or three redundantly sealed containers, depending on the toxicological hazard for a chemical with a vapor pressure below 15 psia. The payload organization must assure that each level of containment will not leak under the maximum use conditions (i.e., vibration, temperature, pressure, etc.). Mercury is an example of such a chemical, since it produces toxic vapors and can amalgamate with metals or metal alloys used in spacecraft hardware. Documentation of chemical usage, along with the containment methods, will be supplied for review and approval.

209.2 **Flammable Materials.** A payload must not constitute an uncontrolled fire hazard to the STS or other payloads. The minimum use of flammable materials shall be the preferred means of hazard reduction. The determination of flammability shall be in accordance with NHB 8060.1. Guidelines for the conduct of flammability assessments are provided in NSTS 22648. A flammability assessment shall be documented in accordance with NSTS 13830.

209.2a **Orbiter Cabin.** Materials used in the Orbiter cabin must be tested in accordance with NHB 8060.1 at the use condition of 10.2 psi total pressure and 30 percent oxygen concentration (worst case Orbiter cabin condition). When flammable materials are used in quantities where the weight or surface area is greater than 0.1 pounds or 10 square inches respectively, the methods of control of flame propagation must be described in the flammability assessment report.

209.2b **Other Habitable Areas.** Materials used in habitable areas other than the Orbiter cabin shall be tested in accordance with NHB 8060.1 in the worst case atmosphere (i.e., oxygen concentration). Propagation path considerations of paragraph 209.2a apply.

209.2c **Outside Habitable Areas.** Materials used outside the Orbiter cabin shall be evaluated for flammability in an air environment at 14.7 psi. Propagation path considerations of NSTS 22648 apply for material usages of greater than 1 pound and/or dimensions exceeding 12 inches.

209.3 **Material Offgassing in Habitable Areas.** Usage of materials which produce toxic levels of offgassing products shall be avoided in habitable areas. Payload elements going into such areas are required to be subjected to offgassing tests (black-box levels) for safety validation prior to integration with STS elements. Rigorous material control to insure that all selected materials have acceptable offgassing characteristics is a negotiable alternative to black-box level testing. The offgassing test specified in NHB 8060.1 or an NSTS approved equivalent shall be used for the black-box level offgassing test. The document MSFC-HDBK-527/JSC 09604 contains a listing of materials and black boxes that have been subjected to offgassing tests.

210 PYROTECHNICS

If premature firing of a pyrotechnic device or failure of a pyrotechnic device to fire will cause a hazard to the STS, the pyrotechnic subsystem and devices shall meet the design and test requirements of MIL-STD-1512.

210.1 **Initiators.** NASA Standard Initiators (NSI's) should be used for functions where premature firing is catastrophic such as deployment from the Orbiter, stage separation, and SRM ignition. Alternate equivalent initiator designs will be considered on a case-by-case basis and will require approval by the NSTS. When alternate initiators are used, it must be thoroughly demonstrated that such initiators are not susceptible to premature firing from electrostatic discharge. This demonstration will not be required: if the pyrotechnic subsystem contains an S&A device that provides a mechanical interrupt of the pyrotechnic train immediately downstream of the initiator; and the S&A device stays in the "SAFE" position until after the payload has been deployed and reaches a safe distance from the Orbiter. When the S&A exception does not apply, alternate initiators must meet the following minimum criteria and demonstration requirements:

210.1a **Flight Unit Acceptance Test.** All the initiators in the lot from which the flight initiators are taken must meet the static discharge sensitivity test requirement of Method 205 of MIL-STD-1512 without a resistor in the test firing circuit. Single bridgewire initiators shall not be subjected to the pin-to-pin test.

210.1b **Design Configuration.** Single bridgewire initiators are preferred. If dual bridgewire initiators are used, the electrostatic discharge sensitivity test described in paragraph 210.1a shall be conducted between bridgewires as well as bridgewire-to-case (three tests). It is preferred that the electrostatic protection feature be hermetically sealed to insure protection stability under all environments.

210.1c **Design Verification.** If a hermetic seal is not used to provide environmental stability, test or analysis must demonstrate that the electrostatic discharge protection exists under all environments including space vacuum. It is also required to demonstrate that the above flight unit acceptance test does not degrade the protection features of the unit under subsequent exposure to electrostatic discharge or other phenomena which could cause premature firing.

210.2 **Pyrotechnic Operated Devices.**

210.2a **Debris Protection.** Pyrotechnic devices that are to be operated in the Orbiter or that do not meet the criteria of this document to prevent inadvertent operation, shall be designed to preclude hazards due to effects of shock, debris, and hot gasses resulting from operation. Such devices shall be subjected to a "locked-shut" safety demonstration test (i.e., a test to demonstrate the capability of the devices to safely withstand internal pressures generated in operation with the moveable part restrained in its initial position).

210.2b **Must Function Safety Critical Devices.** Where failure to operate will cause a catastrophic hazard, pyrotechnic operated devices shall be designed, controlled, inspected, and certified to criteria equivalent to those specified in NSTS 08060. The data required for NSTS review are identified in NSTS 13830. If the device is used in a redundant application where the hazard is being controlled by the use of multiple independent methods, then in lieu of demonstrating compliance with criteria equivalent to NSTS 08060, sufficient margin to assure operation must be demonstrated. When required, pyrotechnic operated devices shall demonstrate performance margin using a single charge or cartridge loaded with 85 percent (by weight) of the minimum allowable charge or other equivalent margin demonstrations.

210.2c **Electrical Connection.** Payloads with pyrotechnic devices which if prematurely fired may cause injury to people or damage to property shall be designed such that these devices can be electrically connected in the Orbiter after all payload/Orbiter electrical interface verification tests have been completed. Ordnance circuitry must be verified safe prior to connection of pyrotechnic devices. Exceptions to this require specific approval of the Launch Site Safety Office.

210.3 **Traceability.** The payload organization shall furnish the NSTS a list of all safety critical pyrotechnic initiators installed or to be installed on the payload, giving the function to be performed, the part number, the lot number, and the serial number.

211 DESTRUCT SYSTEMS

Destruct systems will be used only when approved by the NSTS and must comply with the requirements of paragraphs 200, 201, 202, 204, and 210.

212 RADIATION

212.1 **Ionizing Radiation.** Payloads containing or using radioactive materials or that generate ionizing radiation shall be identified and approval obtained for their use. Descriptive data shall be provided in accordance with NSTS 13830. Major radioactive sources require approval by the Interagency Nuclear Safety Review Panel through the NASA coordinator for the panel. DOD payloads involving radioactive materials will be processed through their own established procedures. Radioactive materials shall comply with appropriate license requirements at the planned launch and landing sites.

212.2 **Nonionizing Radiation.** Payloads shall not emit electromagnetic radiation which presents a hazard. The payload design shall be compatible with the payload bay environment as specified in the ICD between the payload and the Orbiter.

212.3 **Lasers.** Lasers used on STS payloads shall be designed and operated in accordance with American National Standard for Safe Use of Lasers, ANSI-Z-136.1.

213 ELECTRICAL SYSTEMS

213.1 **General.** Electrical power distribution circuitry shall be designed so that faults internal to the payload do not damage STS circuitry and do not create ignition sources for adjacent Orbiter or payload flammable materials. Payload circuits should contain protection devices sized to prevent undamaged wire segments from exceeding the temperature rating of the wire insulation while being subjected to a current at the ultimate trip limit of the protection device for an indefinite period of time. Bent pins or conductive contamination in an electrical connector will not be considered a credible failure mode if a postmate functional verification is performed to assure that shorts between adjacent connector pins or from pins to connector shell do not exist. If this test cannot be performed, then the electrical design must insure that any pin if bent prior to or during connector mating cannot invalidate more than one inhibit and that conductive contamination is precluded by proper inspection procedures.

213.2 **Batteries.** Batteries used on STS payloads shall be designed to control applicable hazards caused by buildup or venting of flammable, corrosive or toxic gasses and reaction products; the expulsion of electrolyte; and by failure modes of overtemperature, shorts, reverse current, cell reversal, leakage, cell grounds, and overpressure. Safety guidelines for STS payload batteries are contained in NSTS 20793. Since lithium batteries have uniquely hazardous failure modes, their use is discouraged where the use of other types of cells is feasible. When lithium batteries are used, the NSTS will require extensive testing and analyses to demonstrate their safety under all applicable failure modes.

213.3 **Lightning.** Payload electrical circuits may be subjected to the electromagnetic fields described in NSTS 07700, Volume XIV, Attachment 1 (ICD-2-19001) due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall be hardened against the environment or insensitive devices (relays) shall be added to control the hazard.

214 VERIFICATION

Test, analysis, and inspection are common techniques for verification of design features used to control potential hazards. The successful completion of the safety process will require positive feedback of completion results for all verification items associated with a given hazard. Reporting of results by procedure/report number and date is required.

214.1 **Mandatory Inspection Points (MIP's).** When procedures and/or processes are critical steps in controlling a hazard and the procedure and/or process results will not be independently verified by subsequent test or inspection, it will be necessary to insure the procedure/process is independently verified in real-time. Critical procedure/process steps must be identified in the appropriate hazard report as MIP's requiring independent observation.

214.2 **Verification Tracking Log.** A payload safety verification tracking log (see NSTS 13830) is required to properly status the completion steps associated with hazard report verification items.

215 HAZARDOUS OPERATIONS

215.1 **Hazard Identification.** The payload organization shall assess all payload flight and ground operations and determine their hazard potential to the STS. The hazardous operations identified shall be assessed in the applicable flight or ground safety assessment report.

215.2 **Exposure to Risk.** STS exposure to increased risk as a result of ground or flight operations shall be minimized. Those ground operations (e.g., armplug installation in a payload pyrotechnic system, final ordnance connection, radioisotope thermoelectric generator (RTG) installation, etc.) which place the payload in a configuration of increased hazard potential shall be accomplished as late as practicable during the payload processing flow at the launch site.

215.3 **Access.** Payloads shall be designed such that any required access to hardware during flight or ground operations can be accomplished with minimum risk to personnel.

216 SERIES PAYLOADS AND REFLOWN HARDWARE

"Reflown hardware" are payloads or elements of payloads which are made up of hardware items that have already physically flown on the STS and are being manifested for reflight. "Series payloads" are payloads or elements of payloads which are of the same or similar design to previously flown STS payloads.

216.1 **Recertification of Safety.** Series payloads and reflown hardware must be recertified safe and must meet all the safety requirements of this document. Caution should be exercised in the use of previous safety verification data for the new usage.

216.2 **Previous Mission Safety Deficiencies.** All anomalies during the previous payload missions must be assessed for safety impact. Those anomalies affecting safety critical systems must be reported and corrected. Rationale supporting continued use of the affected design, operations or hardware must be provided for NSTS approval.

216.3 **Limited Life Items.** All safety critical age sensitive equipment must be refurbished or replaced to meet the requirements of the new STS mission.

216.4 **Refurbishment.** Safety impact of any changes, maintenance or refurbishment made to the hardware or operating procedures must be assessed and reported in the safety assessment reviews (paragraph 304). Hardware changes include changes in the design of the payload, changes of the materials of construction, changes in sample materials that may be processed by the payload, etc.

216.5 **Safety Waivers and Deviations.** The acceptance rationale for all deviations from the previous flight must be revalidated by the payload organization. Waivered conditions from the previous STS flight must be corrected.

217 EXTRAVEHICULAR ACTIVITY (EVA)

All payload requirements for EVA must be defined and documented in the PIP. Any agreed to EVA task used to satisfy the failure tolerance criteria of this document can be used only as a third level of protection to safe a payload. Payload organizations which plan to use crew EVA for mission enhancement, mission success, or safety critical payload operations will comply with the requirements of NSTS 07700, Volume XIV, Appendix 7.

218 PAYLOAD COMMANDING

All hazardous commands that can be sent to the payload shall be identified. Hazardous commands are those that can remove an inhibit to a hazardous function or activate an unpowered hazardous payload system. Failure modes associated with payload flight and ground operations including hardware, software, and procedures used in commanding from payload operations control centers (POCC's) and other ground equipment must be considered in the safety assessment to determine compliance with the requirements of paragraphs 200.1, 201, and 202. NSTS 19943 treats the subject of hazardous commanding and presents the guidelines by which it will be assessed.

219 FLAMMABLE ATMOSPHERES

During Orbiter entry, landing, and 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.

220 CREW HABITABLE PAYLOADS

This paragraph establishes additional safety requirements applicable to NSTS crew habitable payloads. A crew habitable payload is defined as a space capsule (spacecraft or module) which when docked or mated with the Orbiter and provided with atmospheric support from Orbiter systems, is capable of supporting intravehicular activity (IVA) in a shirt sleeve environment for a limited period of time. The crew habitable payload may either be an orbiting capsule visited by the Orbiter or a capsule launched and returned within the Orbiter cargo bay.

220.1 **Atmosphere.**

220.1a **Verification of Habitability.**

220.1a(1) **Offgassing.** The payload design shall assure the offgassing load to the internal manned compartment will not exceed the spacecraft maximum allowable concentrations (SMAC's) of atmospheric contaminants specified in JSC 20584 at the time of ingress. All crew habitable payload hardware will be tested for offgassing characteristics according to NHB 8060.1B as required by paragraph 209.3 of this document and will include measurement of the internal atmosphere of a full scale, flight configured payload as a final verification of acceptability. Time periods prior to crew ingress during which the payload does not have active atmospheric contamination control must be considered.

220.1a(2) **Verification for Revisit Missions.** Payloads that remain in orbit for extended periods must ensure that the manned compartment is environmentally safe prior to crew ingress during any revisit.

Additionally, provisions for sampling of the representative payload internal atmosphere prior to crew ingress shall be provided. Post flight ground analysis of this sample by the NSTS is required prior to the next revisit to determine any unusual gas buildup and the need to define toxic gas detection requirements prior to the subsequent revisit missions.

220.1a(3) **Experiment Leakage.** Experiments conducted during manned operations must meet the containment requirements of paragraph 209.1b. Experiment configurations during unmanned operations are not restricted; however, the manned compartment must be environmentally safe for crew ingress during any revisit. Safe conditions for entry may be established by review of the containment design features, proof of adequate atmospheric scrubbing for the chemical involved, vacuum evacuation, use of payload provided equipment capable of detecting toxic chemicals prior to crew exposure, or other techniques suitable for the particular experiment involved.

220.1b **Internal Environment.** A safe and habitable internal environment shall be provided within the payload throughout all manned operational phases. The payload system shall provide proper mixing and circulation of the atmosphere to assure adequate atmosphere revitalization by the Orbiter Environmental Control and Life Support Subsystem (ECLSS) and distribution throughout the payload.

220.1c **Cross Contamination.** The payload shall be designed so as not to create a contamination hazard in the atmosphere being shared with the Orbiter. The payload shall provide a scrubber and filter system with sufficient capacity to cleanse the payload internal atmosphere of the expected vapor and particulate contamination load. SMAC's of atmospheric contaminates are specified in JSC 20584. The scrubber and filter system shall be capable of being activated prior to crew ingress into the payload.

220.1d **Evacuation.** The capability to isolate the payload from the Orbiter and non-propulsively vent the payload internal atmosphere shall be provided. The activation of the vent system shall be available to the crew in the Orbiter whenever the payload is attached to the Orbiter.

220.2 **Habitability.** The habitability of the payload directly affects the crewmember's ability to perform efficiently and safely. Payload design features related to habitability shall be compatible with and equivalent to those provided by the Orbiter. NASA-STD-3000 defines guidelines for the design of crew-related systems. NASA-STD-3000 does not represent requirements imposed by NASA on manned payloads, but rather, is provided to assist payload organizations in identifying desirable habitability subsystem design goals. Specific agreements on habitability design will be developed in the payload integration process. However, if payload environment is jeopardizing crew safety (e.g., affecting crew health, inducing fatigue to the point that safety critical tasks could be affected, interfering with voice communication, etc.), the crew will egress and isolate the payload atmosphere from the Orbiter.

220.2a **Acoustic Noise.** The maximum continuous acoustic noise sound pressure level in the payload crew habitable area during manned operations shall not exceed the NR-50 contour of the International Organization of Standardization (ISO) Noise Rating, or the NC-50 contour of the United States Noise Criteria Standard, whichever is higher, except that the noise level in the octave bands of 63 hertz and below is limited to a maximum of 75 dB. The maximum sound pressure level of any narrow band continuous component shall be at least 10 dB less than the broad band sound pressure level of the octave band which contains the component. These acoustic noise limits shall apply to the sound pressure levels produced by the summation of all the individual sound pressure levels from all operating systems.

220.2b **Ionizing Radiation.** The payload shall include the radiation protection features/mass shielding required to insure that the crewmember dose rates from naturally occurring space radiation are kept as low as reasonably achievable (ALARA). Exposure levels shall not exceed the limits defined in Figure 5.7.2.2.1-2 of NASA-STD-3000.

220.2c **Mechanical Hazards.** Payload and equipment design shall protect crewmembers from sharp edges, protrusions, etc. during all crew operations. Translation paths and adjacent equipment shall be designed to minimize the possibility of entanglement or injury to crewmembers.

220.2d **Thermal Hazards.** During normal operations, crewmembers shall not be exposed to high or low surface temperature extremes. Protection shall be provided against continuous skin contact with surfaces above 45 degrees Centigrade (113 degrees Fahrenheit) or below 4 degrees Centigrade (39 degrees Fahrenheit). Safeguards such as warning labels, protective devices or special design features to protect the crew from surface temperatures outside these safe limits, shall be provided for both nominal and contingency operations.

220.2e **Electrical Hazards.** Grounding, bonding, and insulation shall be provided for all electrical equipment to protect the crew from electric shock during nominal and contingency operational phases while the crew is in the payload.

220.2f **Lighting.** The lighting illumination level provided throughout the payload shall permit planned crew activities without injury. A backup/secondary lighting system shall be provided consistent with emergency egress requirements or in case of failure of the primary lighting system.

220.3 **Fire Protection.** A fire protection system comprised of fire detection, warning, and Halon 1301 or equivalent suppression devices shall be provided in the payload. The fire protection system shall encompass both hardware and crew procedures for adequate control of the fire hazard within the cabin volume as well as within equipment racks within the pressurized hull. The fire protection system shall incorporate test and checkout capabilities such that the operational readiness of the entire system can be verified by the crewmembers. The fire protection system shall have redundant electrical power sources and shall incorporate redundant detection and warning capability and redundant activation of suppressant devices. Fire detection annunciation and control of the payload fire protection system shall be provided to the crew in both the Orbiter and payload during all Orbiter/payload attached mission phases.

220.4 Emergency Safing.

220.4a **Crew Egress.** The payload design shall be compatible with emergency safing and rapid crew escape. Crewmembers shall be provided with clearly defined escape routes for emergency egress in the event of a hazardous condition. Where practical, dual escape routes from all activity areas shall be provided. Payload equipment location shall provide for protection of compartment entry/exit paths in the event of an accident. Routing of hardlines, cables, or hoses through a tunnel or hatch which could hinder crew escape or interfere with hatch operation for emergency egress is not permitted. Payload hatches which could impede crew escape must remain open during all crew operations.

220.4b **Electrical System.** The payload electrical power distribution system shall have the capability to remove all electrical power from the payload including termination of power from both the payload and Orbiter sources. This capability shall be available to the crew in both the payload and the Orbiter. Separate safing systems, however, shall be used for nominal payload functions and for essential/emergency functions (e.g., the fire protection, caution and warning, and emergency lighting, etc.). Essential/emergency functions shall be powered from a dedicated electrical power bus with redundant power sources.

220.5 **Hatches.** A hatch shall be provided to isolate the payload from the Orbiter cabin. Payload hatch design shall be compatible with emergency crew egress. Payloads shall provide a capability to allow a visual inspection of the interior of the payload prior to hatch opening and crew ingress. All operable hatches that could close and latch inadvertently, thereby blocking an escape route, shall have a redundant (backup) opening mechanism and shall be capable of being operated from both sides. External pressure hatches shall be self-sealing. Hatches shall have a pressure difference indicator clearly visible to the crewmember operating the hatch and a pressure equalization device. All hatches shall nominally be operable without detachable tools or operating devices and shall be designed to prevent inadvertent opening prior to complete pressure equalization. The payload/Orbiter interface shall provide for Orbiter crew EVA access to the payload bay while the payload is attached to the Orbiter.

220.6 **Caution and Warning.** The payload shall incorporate a caution and warning system. All crew safety caution and warning parameters shall be redundantly monitored and shall cause annunciation in both the Orbiter and payload. As a minimum, payload total pressure, cabin fan differential pressure, fire detection, oxygen partial pressure and carbon dioxide partial pressure shall be monitored. The status of all monitored parameters shall be available to the crew in the Orbiter prior to entry into the payload. The caution and warning system shall include test provisions to allow the payload crewmembers to verify proper operation of the system. The payload provided alert system shall be consistent with Orbiter annunciation practices.

220.7 **Windows.**

220.7a **Structural Design.** Windows shall be provided in the payload only when necessary for essential mission operation, and all assemblies shall provide a redundant pressure pane. The pressure panes shall be protected from damage by external impact. The structural design of window panes in the pressure hull shall provide a minimum initial ultimate factor of safety of 3.0 and an end-of-life minimum factor of safety of 1.4. Window design shall be based on fracture mechanics considering flaw growth over the design life of the payload.

220.7b **Transmissivity.** The transmissivity of payload windows shall be based on protection of the crew from exposure to excess levels of naturally occurring nonionizing radiation. Exposure of the skin and eyes of crewmembers to nonionizing radiation shall not exceed the threshold limit values (TLV's) set and proposed by the American Conference of Governmental Industrial Hygienists (ACGIH) as specified in "Threshold Limit Values and Biological Exposure Indices for 1987-1988" or its subsequent revisions. Window design shall be coordinated with other shielding protection design to comply with the ionizing radiation limits specified in paragraph 220.2b.

220.8 **Communications.** Voice communications, compatible with the Orbiter communications system, shall be provided between the Orbiter crew and payload crewmembers during all manned operations.

220.9 **Pressure Hull**. The design of the manned pressure compartment shall comply with the structural design requirements of paragraphs 208.1 and 208.2. The hull maximum design pressure (MDP) shall be determined as defined in paragraph 208.4. The ultimate factor of safety of hull design shall be equal to or greater than 2.0 for both the MDP and the maximum negative pressure differential the hull may be subjected to during normal and contingency operations or as the result of two credible failures. The pressure hull shall be designed to leak-before-burst criteria. Structural verification shall be in accordance with NSTS 14046.

CHAPTER 3: SYSTEM PROGRAM REQUIREMENTS

300 GENERAL

The following requirements are applicable to all payloads.

301 SAFETY ANALYSIS

A safety analysis shall be performed in a systematic manner on each payload, its GSE, related software, and ground and flight operations to identify hazardous subsystems and functions. The safety analysis shall be initiated early in the design phase and shall be kept current throughout the development phase. A safety assessment report which documents the results of this analysis, including hazard identification, classification, and resolution, and a record of all safety-related failures, shall be prepared, maintained, and submitted in support of the safety assessment reviews conducted by the NSTS in accordance with paragraph 304. Detailed instructions for the safety analysis and safety assessment reports are provided in NSTS 13830.

302 HAZARD LEVELS

Hazards are classified according to potential as follows:

302.1 **Critical Hazard.** Can result in damage to STS equipment, a nondisabling personnel injury or the use of unscheduled safing procedures that affect operations of the Orbiter or another payload.

302.2 **Catastrophic Hazard.** Can result in the potential for a disabling or fatal personnel injury, loss of the Orbiter, ground facilities or STS equipment.

303 HAZARD REDUCTION

Action for reducing hazards shall be conducted in the following order of precedence:

303.1 **Design for Minimum Hazard.** The major goal throughout the design phase shall be to insure inherent safety through the selection of appropriate design features. Damage control, containment, and isolation of potential hazards shall be included in design considerations.

303.2 **Safety Devices.** Hazards which cannot be eliminated through design selection shall be reduced and made controllable through the use of automatic safety devices as part of the system, subsystem, or equipment.

303.3 **Warning Devices.** When it is not practical to preclude the existence or occurrence of known hazards or to use automatic safety devices, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal, coupled with emergency controls of corrective action for operating personnel to safe or shut down the affected subsystem. Warning signals and their application shall be designed to minimize the probability of wrong signals or of improper reaction to the signal.

303.4 **Special Procedures.** Where it is not possible to reduce the magnitude of an existing or potential hazard through design or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of personnel safety.

304 SAFETY ASSESSMENT REVIEWS AND SAFETY CERTIFICATION

Safety assessment reviews will be conducted by the NSTS flight operator and the NSTS launch/landing site operator to determine compliance with the requirements of this document. An initial contact meeting will be held at the earliest appropriate time and will be followed by formal review meetings spaced throughout the development of the payload and its GSE. The depth, number, and scheduling of reviews will be negotiated with the payload organization and will be dependent on complexity, technical maturity, and hazard potential. The KSC and JSC phase III safety reviews and ground safety certification must be completed 30 days prior to delivery of the payload, ASE, and GSE to the launch site except as noted in NSTS 13830. The ground safety certification shall include statements that the payload GSE and ground operations are safe and in compliance with NSTS ground safety requirements and that open safety verification from the JSC safety reviews for payload design and flight operations will not affect safe ground operations. Rationale for acceptance of open flight verification (see paragraph 214.2) during ground operations must be submitted by the payload organization with the ground safety certification statement and approved by the NSTS launch/landing site operator prior to the start of ground processing. The flight safety certification shall be submitted at least 10 days prior to the Flight Readiness Review (FRR). The flight safety certification shall include statements that the payload design and flight operations are safe and are in compliance with the NSTS safety requirements of this document.

305 SAFETY COMPLIANCE DATA

Safety compliance data packages shall be prepared by the payload organization to support ground operations of the payload at the launch and landing sites and inflight operations of the payload with the STS.

305.1 **For GSE and Ground Operations.** The data listed below shall be submitted to the NSTS launch/landing site operator as part of the data package for the phase III ground safety review.

a. A payload safety verification tracking log.

b. A safety assessment report for GSE design and ground operations. See paragraph 301.

c. Approved waivers and deviations.

d. A log book maintained on each pressure vessel/system showing pressurization history, fluid exposure, and other pertinent data.

e. A summary and safety assessment of all safety-related failures or accidents applicable to payload processing, test, and checkout.

305.2 **For Payload Design and Flight Operations.** The data listed below shall be submitted to the NSTS flight operator as part of the data package for the phase III flight safety review.

a. A safety assessment report for payload design and flight operations. See paragraph 301.

b. A payload safety verification tracking log.

c. Approved waivers and deviations.

d. A summary and safety assessment of all safety related failures and accidents applicable to payload processing, test, and checkout.

e. A list of all pyrotechnic initiators installed or to be installed on the payload, giving the function to be performed, the part number, the lot number, and the serial number. Submittal of this list may be delayed to be concurrent with the submittal of the flight safety certification statement.

305.3 **Post-Phase III Compliance**. When the flight certification statement of paragraph 304 is submitted, it shall be included with an updated payload safety verification tracking log that documents the closeout of all required safety verification. The verification tracking log and the certification statements must reflect the final configuration of the payload that includes all post phase III safety activity.

306 MISHAP/INCIDENT/MISSION FAILURES INVESTIGATION AND REPORTING

Mishap/incident/mission failures investigation and reporting for NASA equipment will be handled under the provisions of NASA Headquarters policy documents NMI 8621.1 and NHB 1700.1 Volume 1. For mishap/incident/mission failures involving non-DOD payloads occurring after delivery to NASA facilities, investigation and reporting will be in compliance with the above NASA documents. The payload organization and the individual payload element or experiment contractors will cooperate fully with the investigation and provide any records, data, and other administrative or technical support and services that may be deemed by the NSTS to be pertinent. For DOD payloads, the "Agreement Between the Department of Defense and the National Aeronautics and Space Administration for Joint Investigation of Aircraft or Space System Mishaps" will be the controlling document.

APPENDIX A: GLOSSARY OF TERMS

ADIABATIC COMPRESSION DETONATION. An observed phenomenon whereby the heat obtained by compressing the vapors from fluids (e.g., hydrazine) is sufficient to initiate a self-sustaining explosive decomposition. This compression may arise from advancing liquid columns in sealed spacecraft systems.

ASE. Airborne support equipment. The flight equipment and systems needed to support the payload such as data recording, control functions, instrumentation, and payload cradles.

CATASTROPHIC HAZARD. A hazard which can result in the potential for: a disabling or fatal personnel injury; or loss of the Orbiter, ground facilities or STS equipment.

CERTIFICATE OF SAFETY COMPLIANCE. (Appendix C, Figure 3). A formal written statement by the payload organization attesting that the payload is safe and that all safety requirements for this document have been met and, if not, what waivers and deviations are applicable.

CONTROL. A device or function that operates an inhibit is referred to as a control for an inhibit and does not satisfy inhibit requirements. The electrical devices that operate the flow control devices in a liquid propellant propulsion system are exceptions in that they are referred to as electrical inhibits.

CORRECTIVE ACTION. Action taken to preclude occurrence of an identified hazard or to prevent recurrence of a problem.

CREDIBLE. A condition that can occur and is reasonably likely to occur. For the purposes of this document, failures of structure, pressure vessels, and pressurized lines and fittings are not considered credible failure modes if those elements comply with the applicable requirements of this document.

CREDIBLE SINGLE BARRIER FAILURE. (Material/Fluid Compatibility). Potential leaks within a component that permit fluid to directly contact the materials behind the barrier or expose secondary compartments to system pressure conditions shall be considered in single barrier failure analysis (e.g., leaks from a fluid enclosure to an adjacent enclosure such as through mechanical joints, O-rings, gaskets, bladders, bellows, and diaphragms). Redundant seals in series which have been acceptance pressure tested individually prior to flight shall not be considered credible single barrier failures. Failures of structural parts such as pressure lines and tanks, and properly designed and tested welded or brazed joints are not considered single barrier failures. Metallic bellows and diaphragms designed for and tested to demonstrate sufficiently high margins can be considered for exclusion from the category of credible single barrier failure. In order to be classified as a noncredible failure, the item must be designed for a safety factor 2.5 on the maximum design pressure, pass appropriate manufacturing inspections (such as dye penetrant, radiographic, and visual inspections) and leak checks, and be certified for all the operating environments including fatigue conditions.

CRITICAL HAZARD. A hazard which can result in damage to STS equipment, a nondisabling personnel injury, or the use of unscheduled safing procedures that affect operations of the Orbiter or another payload.

DEPLOYABLE PAYLOAD. A payload which is planned for release from the Orbiter.

DEVIATION. Granted use or acceptance for more than one mission of a payload aspect which does not meet the specified requirements. The intent of the requirement should be satisfied and a comparable or higher degree of safety should be achieved.

EMERGENCY. (Flight Personnel). Any condition which can result in flight personnel injury or threat to life and requires immediate corrective action, including predetermined flight personnel response.

EVA. Extravehicular activity by the flightcrew.

FACTOR OF SAFETY. The factor by which the limit load is multiplied to obtain the ultimate load. The limit load is the maximum anticipated load or combination of loads, which a structure may be expected to experience. Ultimate load is the load that a payload must be able to withstand without failure.

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

FAILURE TOLERANCE. The number of failures which can occur in a system or subsystem without the occurrence of a hazard. Single failure tolerance would require a minimum of two failures for the hazard to occur. Two-failure tolerance would require a minimum of three failures for a hazard to occur.

FINAL SEPARATION. Final separation from the Orbiter is achieved when the last physical connection between the payload and the Orbiter and/or payload ASE is severed and the payload becomes a free-flying payload.

FLIGHTCREW. Any personnel onboard the Space Shuttle engaged in flying the Space Shuttle and/or managing resources onboard, e.g., commander, pilot, and mission specialist.

GPC. Orbiter's General Purpose Computer.

GSE. Ground support equipment.

GROUND CREW. With respect to inflight monitoring, the term includes any personnel supporting the payload officer from a console in the Mission Control Center (MCC), remote POCC, or other support area.

HAZARD. The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of an activity, condition, or circumstance which can produce adverse or harmful consequences.

HAZARD DETECTION. An alarm system used to alert the crew to an actual or impending hazardous situation for which the crew is required to take corrective or protective action.

INDEPENDENT INHIBIT. Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

INHIBIT. A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.).

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

KSC. Kennedy Space Center, NASA, Florida.

MANNED PRESSURIZED VOLUME. Any module in which a person can enter and perform activities in a shirt-sleeve environment.

MISHAP/INCIDENT. An unplanned event which results in personnel fatality or injury; damage to or loss of the STS, environment, public property or private property; or could result in an unsafe situation or operational mode. A mishap refers to a major event, whereas an incident is a minor event or episode that could lead to a mishap.

MCC. Mission Control Center.

MONITOR. Ascertain the safety status of payload functions, devices, inhibits, or parameters.

NONCOMPLIANCE REPORT. A report documenting a condition in which a requirement cannot be met. It is the report used to request a waiver or deviation. See NSTS 13830 and Appendix C Figure 2.

NORMAL STS MISSION PHASES. All portions of the mission to be performed by the STS, excluding STS abort and emergency landing.

NSI. NASA standard initiator (pyrotechnic). The NSI is provided to the payload customer by NASA.

OFFGASSING. The emanation of volatile matter of any kind from materials into habitable areas.

OPERATOR ERROR. Any inadvertent payload operation by either flight personnel or the ground crew that affects either the Orbiter or a payload.

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

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

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

PERSONNEL INJURY. With respect to catastrophic hazard levels for STS payloads, personnel injury will be limited to loss of life or major injury which can lead to either temporary or permanent incapacitation of the crew (e.g., bone fractures, second or third degree burns, severe lacerations, internal injury, severe (greater than 1Gy) radiation exposure, and unconsciousness). Other personnel injuries are related to a critical hazard level provided the injury does not impact the flightcrew's capability to accomplish safety critical tasks.

POCC. Payload Operations Control Center.

PRESSURE VESSEL. A container designed primarily for pressurized storage of gases or liquids and: (1) contains stored energy of 14,240 foot-pounds (0.01 pounds trinitrotoluene (TNT) equivalent) or greater based on adiabatic expansion of a perfect gas; or(2) will experience a design limit pressure greater than 100 pounds per square inch absolute (psia); or (3) contains a fluid in excess of 15 psia which will create a hazard if released.

RF. Radio frequency.

SAFE. A general term denoting an acceptable level of risk, relative freedom from, and low probability of: personal injury; fatality; damage to property; or loss of the function of critical equipment.

SAFETY ANALYSIS. The technique used to systematically identify, evaluate, and resolve hazards.

SAFETY CRITICAL. Containing an element of risk. Necessary to prevent a hazard.

SAFING. Actions which eliminate or control hazards.

SEALED CONTAINER. A housing or enclosure designed to retain its internal atmosphere and which does not meet the pressure vessel definition (e.g., an electronics housing).

SPACE SHUTTLE. The Orbiter, solid rocket boosters and external tank.

STRUCTURE. Any assemblage of materials which is intended to sustain mechanical loads.

STS ABORT. An abort of the STS mission wherein flight personnel, payload, and vehicle are returned to a landing site.

WAIVER. Granted use or acceptance of a payload aspect which does not meet the specified requirements; a waiver is given or authorized for one mission only. Safety waivers could include acceptance of increased risk.

APPENDIX B: APPLICABLE DOCUMENTS

Except as noted below the latest revision of the following documents form a part of this document to the extent specified herein. In the event of conflict between the reference documents and the contents of this document, the contents of this document will be considered superseding requirements. Copies of these documents can be obtained from Johnson Space Center, Customer Service Center, Code TC12, NASA, Houston, Texas 77058.

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
SAMTO HB S-100/KHB 1700.7, Space Transportation System Payload Ground Safety Handbook.	101.1
NSTS 13830, Implementation Procedure for NSTS Payloads System Safety Requirements.	103.1, 200, 200.2, 208.4, 210.2, 212.1, 214.2, 301, 304
NSTS 18798, Interpretations of NSTS Payload Safety Requirements.	103.2
NSTS 16979, Part 1, Shuttle Orbiter Failure Modes and Fault Tolerances for Interface Services. Part 2, Failure Modes and Fault Tolerances for STS Payload Optional Service Kit Hardware.	200.4
MIL-STD-1576, July 31, 1984, Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems.	202.1
NHB 8060.1, Flammability, Odor, and Offgassing Requirements and Test Procedures for Materials in Environments that Support Combustion.	202.2
NSTS 07700, Volume XIV, Attachment 1, (ICD 2-19001), Shuttle Orbiter/Cargo Standard Interfaces.	202.5, 213.3, 220.1b, 220.2a
NSTS 14046, Payload Verification Requirements.	208.1, 208.4, 220.9
NHB 8071.1, Fracture Control Requirements for Payloads Using the National Space Transportation System (NSTS).	208.1

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
MSFC-SPEC-522, Revision B, Design Criteria for Controlling Stress Corrosion Cracking.	208.3
MSFC-HDBK-527/JSC 09604, Materials Selection List for Space Hardware Systems.	208.3, 209, 209.3
MIL-STD-1522, Revision A, including changes as of December 1984, Standard General Requirement for Safe Design and Operation of Pressurized Missile and Space Systems.	208.4
NSTS 22648, Flammability Configuration Analysis for Spacecraft Systems.	209.2
MIL-STD-1512, March 21, 1972, Electroexplosive Subsystems Electrically Initiated, Design Requirements, and Test Methods.	210, 210.1
NSTS 08060, Space Shuttle System Pyrotechnic Specification.	210.2
NSTS 20793, Manned Space Vehicle, Battery Safety Handbook.	212.2
ANSI-Z-136.1, American National Standard for Safe Use of Lasers.	212.3
NSTS 07700, Volume XIV, Appendix 7, System Description and Design Data - Extravehicular Activities.	217
NSTS 19943, Command Guidelines for STS Customers.	218
JSC 20584, Listing of Spacecraft Maximum Allowable Trace Gas Concentrations.	220.1a, 220.1c
NASA-STD-3000, Volume 1, Man-Systems Integration Standards.	220.2, 220.2b
American Conference of Governmental Industrial Hygienists (ACGIH), "Threshold Limit Values and Biological Exposure Indices for 1987-1988."	220.7b
NMI 8621.1, Mishap Reporting and Investigating.	306
NHB 1700, Volume I, NASA Basic Safety Manual.	306

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
Agreement Between the Department of Defense and the National Aeronautics and Space Administration for Joint Investigation of Aircraft or Space System Mishaps.	306

APPENDIX C: FIGURES

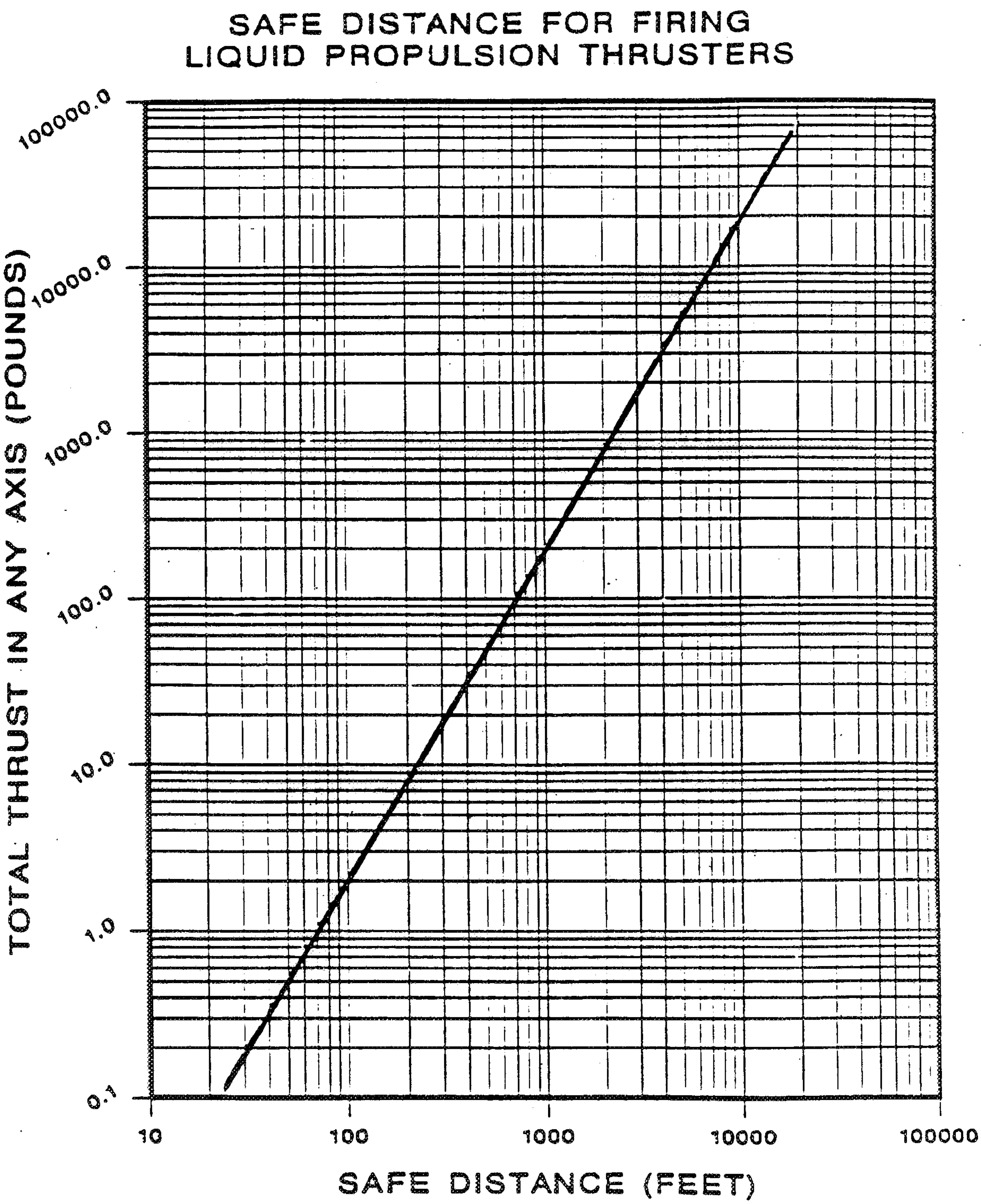

Figure 1.- Safe distance for firing liquid propulsion thrusters.

PAYLOAD SAFETY NONCOMPLIANCE REPORT	NO.	DATE
TITLE (Brief reference to noncompliance)		
PAYLOAD IDENTIFICATION (Include reference to applicable payload element, subsystem, and/or component)		
APPLICABLE REQUIREMENT		
DESCRIPTION OF NONCOMPLIANCE (Specify how the design or operation does not meet the safety requirements.)		
HAZARD OR HAZARD CAUSE (Include reference to Payload Hazard Report)		
REASON REQUIREMENT CANNOT BE FULFILLED		
RATIONALE FOR ACCEPTANCE (Define the design feature or procedure used to conclude that the noncompliance condition is safe. Attach applicable support data, i.e. drawings, test reports, analyses, etc.)		

APPROVAL SIGNATURES			
PAYLOAD ORGANIZATION			DATE
WAIVER APPROVAL		DEVIATION APPROVAL	
EFFECTIVITY		EFFECTIVITY	
STS OPERATOR	DATE	STS OPERATOR	DATE

JSC Form 542C (Rev Mar 83) NASA-JSC

Figure 2.- Payload Safety Noncompliance Report.

CERTIFICATE OF NSTS PAYLOAD SAFETY COMPLIANCE FOR

____

(PAYLOAD)

☐ PAYLOAD DESIGN AND FLIGHT OPERATIONS

OR

☐ GSE DESIGN AND GROUND OPERATION

THE PAYLOAD ORGANIZATION HEREBY CERTIFIES THAT:

(1) THE PAYLOAD IS SAFE.

(2) THE PAYLOAD COMPLIES WITH ALL APPLICABLE REQUIREMENTS OF NSTS 1700.7 (CURRENT ISSUE), "SAFETY POLICY AND REQUIREMENTS FOR PAYLOADS USING THE NATIONAL SPACE TRANSPORTATION SYSTEM."

LIST OF APPROVED WAIVERS / DEVIATIONS

APPROVED: (PAYLOAD ORGANIZATION PAYLOAD MANAGER)	DATE:

Figure 3.- Certificate of NSTS Payload Safety Compliance.