NHB 1700.7A

Safety Policy and Requirements

For Payloads Using the Space Transportation System (STS)

NASA
National Aeronautics and Space Administration

Washington D.C. 20546

PREFACE

DATE: Dec. 9, 1980

The Space Transportation Operations (STO) safety policy is to minimize STO involvement in the payload and its GSE (ground support equipment) design process while maintaining the assurance of a safe operation. 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 safety policies and requirements while allowing for negotiation between the payload organization and the STO operator in the method of implementation of payload safety.

This revision provides for a relaxation in the monitoring requirements for inhibits, allows the payload organization to pursue new design options and reflects, additionally, same new requirements. As of the issue date of this NHB, payloads which have completed the formal safety assessment reviews of their preliminary design on the basis of the May 1979 issue will be reassessed for compliance with the above changes. Such payloads are requested to review their design and operations and submit updated safety analyses within 60 days. All other payloads must comply with this NHB in its entirety.

John F. Yardley
Associate Administrator for
Space Transportation Systems

Stanley I. Weiss
Associate Administrator for
Space Transportation Operations

TABLE OF CONTENTS

CHAPTER 1: GENERAL

100 PURPOSE. This document establishes the policy and safety requirements applicable to all STS payloads and their 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. For additional safety requirements which are unique to ground operations and GSE design, see the KSC Launch Site Accommodations Handbook for STS Payloads, K-STSM-14.1. In the event of differences between that handbook and this document, this document shall take precedence. These additional ground safety requirements will be deleted from the KSC handbook and incorporated as an appendix to this document at a subsequent revision.

102 RESPONSIBILITY.

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 STS operator on behalf of the group of individual payload elements or experiments. 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.

2. STS Operator. It is the responsibility of the STS operator to interface with the responsible payload organization to review the payload for adequate safety implementation. It is also the responsibility of the STS operator 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 detailed interpretation and implementation of safety requirements will be determined on a case-by-case basis and must be consistent with hazard potential. Supplementary documents have been issued to assist payload organizations in complying with the technical (chapter 2) and system safety (chapter 3) requirements of this document.

1. Safety Guidelines Handbook. To supplement the technical requirements, NASA has published the Space Transportation System Payload Safety Guidelines Handbook, JSC 11123, which suggests various methods of implementing safety in design which NASA has found to be acceptable. JSC 11123 does not represent requirements imposed by NASA as there are many alternative solutions to the control of any hazard; instead, it is provided to assist payload organizations in their design activities.

2. Implementation Procedure. The Implementation Procedure for STS Payloads System Safety Requirements, JSC 13830, has been published to assist the payload organization in implementing the system safety requirements and

further defines the safety analyses, data submittals, and safety assessment review meetings. JSC 13830 identifies the respective roles of the STS flight operator (JSC) and the STS launch/landing site operator (KSC) and is jointly issued. JSC 13830 reflects a basic policy of commonality, compatibility, and coordination between the STS flight and ground elements in the implementation effort.

CHAPTER 2: TECHNICAL REQUIREMENTS

200 GENERAL. The following requirements are applicable to all payloads. These requirements apply under worst-case natural and induced environments, including STS abort and emergency landing conditions. Payloads which are not planned for return must be compatible with the environments encountered during STS abort and emergency landing. When a requirement cannot be met, a waiver request must be submitted in accordance with JSC 13830.

201 FAILURE TOLERANCE. For hazardous functions, 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.

1. Critical Hazards. No single failure or operator error shall result in damage to STS equipment or in the use of contingency or emergency procedures.

2. Catastrophic Hazards. No combination of two failures, operator errors, or RF (radio frequency) signals shall result in the potential for personnel injury, loss of the Orbiter, ground facilities, or STS equipment.

202 CONTROL OF HAZARDOUS FUNCTIONS.

1. Functions Resulting in Critical Hazards. A function that could result in a critical hazard must be controlled by two independent inhibits, whenever the hazard potential exists. Monitoring of these inhibits and the requirement to return to a safe condition will be determined on a case-by-case basis. When required, these inhibits may be monitored by the Orbiter flight crew or the ground in near real time. For deployable payloads, monitoring and safing of the two inhibits will not be required when both inhibit power and control circuits for the function are connected to a bus that is not energized until the payload reaches a safe distance from the Orbiter.

2. Functions Resulting in Catastrophic Hazards. A function that 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 RF command. Monitoring and safing of the three inhibits which prevent the occurrence of a catastrophic function will not be required when both the inhibit power and control circuits are connected to a bus that is not energized until the payload reaches a safe distance from the Orbiter. When the function power bus or control circuits are powered before achieving a safe distance from the Orbiter, monitoring shall be available to verify that at least two of the three inhibits are in place. Monitoring of these inhibits shall be available to the launch site when necessary to assure safe ground operations. In the following paragraphs specific commmand and monitoring requirements are defined for several identified catastrophic hazards. The monitoring provisions of these paragraphs do not apply if the nonenergized bus option above is used. Final separation from the Orbiter as used in the following paragraphs is the last physical interface of the payload structure with the Orbiter or ASE

(airborne support equipment). If the last physical interface is with an Orbiter deployment device (e.g. RMS), then the specific monitoring and safing requirements in the following paragraphs may be amended on a case-by-case basis. Specific monitoring and safing requirements for other catastrophic functions will be determined on a case-by-case basis.

a. Solid propellant rocket motors. The premature firing of a solid propellant rocket motor is a catastrophic hazard. Payloads with solid propellant rocket motors must coast at least 45 minutes with a minimum separation velocity of 1 foot per second before motor ignition (payloads not meeting this requirement must provide crew operated RF command to inhibit motor firing until a safe distance is assured). They shall be equipped with an S&A (safe and arm) device that provides a mechanical interrupt in the pyrotechnic train immediately downstream of the initiator. A minimum of two additional inhibits shall be provided. If the function power bus or control circuits are powered before achieving a safe distance from the Orbiter, monitoring of the S&A device status and the ability to return to a safe status shall be available to the flight crew until final separation from the Orbiter. Additional requirements are a function of the planned payload operations as follows:

(1) S&A device not rotated to the arm position until the payload has reached a safe distance. When the S&A device is not rotated to the arm position until the payload has reached a safe distance, the capability to monitor the status of two additional inhibits must be available to the flight crew or ground in near real time until final separation from the Orbiter.

(2) S&A device rotated to the arm position prior to the payload reaching a safe distance. When the S&A device is rotated to the arm position prior to the payload reaching a safe distance, at least three inhibits must remain until the payload reaches a safe distance. The S&A device must remain in the safe position during boost and entry. Rotation of the S&A device to the arm position must be a flight crew function and will be done only as part of the final deployment activities. Prior to rotation of the S&A device and separation of the payload from the Orbiter, the flight or ground crew must have continuous real-time monitoring capability to assure that two of the remaining inhibits are in the safe condition. If ground monitoring is used, continuous communication must be available to inform the flight crew of the inhibit status until final separation from the Orbiter. The initiator must meet the pyrotechnic requirements identified in paragraph 210.

b. Liquid propellant propulsion systems. The premature firing of a liquid propellant system or adiabatic detonation prior to achieving a safe distance is a catastrophic hazard. Each propellant delivery system must contain a minimum of three mechanically independent propellant flow control devices in series that remain closed during all ground and flight phases (except ground servicing) until the deployed payload has reached a safe distance from the Orbiter. A

flow control device shall isolate the propellant tank(s) from the remainder of the distribution system. This isolation valve may be opened under the provisions described in paragraph 202.2 b (2). A minimum of one of the three devices shall be fail-safe; i.e., return to the closed condition in the absence of an opening signal. The opening of any flow control device shall not result in adiabatic detonation. For liquid propellant engines of 10 pounds or less thrust, the minimum safe firing distance following deployment is 200 feet from the Orbiter. For large engines and any engine operable just prior to payload retrieval, the safe distance will be determined on a case-by-case basis. For bipropellant systems, these devices must prevent mixing or contact between the fuel and oxidizer as well as prevent expulsion through the thrust chamber(s). For monopropellant systems, these devices must prevent expulsion through the thrust chamber(s). The electrical inhibits and monitoring/safing requirements are a function of the planned payload operations as follows:

(1) Isolation valve not opened until the payload has reached a safe distance. When the isolation valve is not opened until the payload has reached a safe distance from the Orbiter, the opening of the mechanical devices shall be controlled by at least three independent electrical inhibits that prevent firing of the engine. Two of the three independent electrical inhibits must be monitored by the flight or ground crew in near real time until final separation of the payload from the Orbiter. One of the monitored inhibits must control the isolation valve.

(2) Isolation valve opened prior to the payload reaching a safe distance. When the isolation valve is opened prior to the payload reaching a safe distance from the Orbiter, a minimum of three independent electrical inhibits must prevent the firing of any engine until the payload has reached a safe distance from the Orbiter. The isolation valve must remain in the closed condition during boost and entry and will be opened only by flight crew command as a part of the final deployment activities. Prior to opening the isolation valve, a minimum of two remaining inhibits must be verified safe by flight or ground crew monitoring and must remain available in real time until final separation of the payload from the Orbiter. If ground monitoring is used, continuous communication must be available to inform the flight crew of the inhibit status. When the liquid propulsion system cannot be returned to a safe condition by crew command, single failure tolerant deployment capability must be provided.

c. Deployment and/or separation. The premature deployment or separation of a payload, stage, appendage, or separable device to a condition where it cannot withstand STS-induced loads (including landing) or will prevent safe entry of the Orbiter is a catastrophic hazard. Three independent inhibits to the function must be provided and must remain in the safe condition until performance of the function does not present a hazard to the Orbiter or crew.

These devices must be designed to preclude inadvertent mechanical operation in the induced environments. If pyrotechnic devices are employed, the initiators must meet the special pyrotechnic requirements in accordance with paragraph 210. Additional requirements are a function of the planned payload operations as follows:

(1) Deployment/separation function performed after final separation of the payload from the Orbiter. When the deployment/separation functions are planned to be performed after final separation of the payload from the Orbiter, the functions shall not be performed until the payload is at a safe distance from the Orbiter. Monitoring of the status of two inhibits must be available to the flight crew or ground in near real time until final separation of the payload from the Orbiter.

(2) Deployment/separation function performed before the final separation of the payload from the Orbiter. When the deployment/separation functions are planned to be performed before the final separation of the payload from the Orbiter, the three inhibits must remain in the safe condition for boost and entry. Removal of the inhibits must be by crew command and will be removed only in preparation for the planned deployment/separation activity. Command and monitoring of the inhibits must be available to the flight crew for performance of the function. The ability to return the inhibits to a safe status must be available to the flight crew in the event the function is not performed.

d. Deployment/extension preventing payload bay door closure. If during planned payload operations an element of the payload or any payload support equipment violates the payload bay door envelope, the hazard of preventing door closure must be controlled by independent primary and backup methods, and this combination must be two failure tolerant.

e. RF energy radiation. Cargo-produced radiated fields from payload transmitter antenna systems in excess of levels defined for payload bay door open operations in JSC 07700, Volume XIV, attachment I is a catastrophic hazard. Three independent inhibits to radiation in excess of these levels must be provided. There are no command and monitoring requirements for the inhibits.

203 RETRIEVAL OF PAYLOADS. Deployable and freeflying payloads that are to be retrieved shall have the capability to return hazardous systems to a safe condition (i.e., meet the requirements of paragraphs 201 and 202). They shall provide verification to the Orbiter or the ground that safing has been accomplished prior to their retrieval and while still a safe distance from the Orbiter. Verification must establish that hazardous systems are at least single failure tolerant.

204 HAZARD DETECTION AND SAFING. The need for hazard detection and safing by the flight crew to control time-critical hazards shall be minimized and will be implemented only when an alternate means of reduction or control of

hazardous conditions is not available. When implemented, these functions shall be capable of being tested for proper operations during both ground and flight phases.

205 CONTINGENCY RETURN OF PAYLOADS. Deployable payloads must provide the capability at all times prior to separation to safe the payload for contingency return. This safing includes performing contingency operations to reconfigure the payload to a safe condition for landing, and maintaining or resafing inhibits of hazardous functions to meet requirements of paragraph 202.

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 arranged so that the probability of propagation of failure of one to the other is minimized.

208 STRUCTURAL.

1. Structural Design. The structural design shall provide ultimate factors of safety equal to or greater than 1.40 for all STS mission phases except emergency landing. When failure of structure can result in a catastrophic event, 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.

2. Emergency Landing Loads. The structural design shall comply with the ultimate design load factors for emergency landing loads that are specified in JSC 07700, Volume XIV, attachment I.

3. Stress Corrosion. The selection of materials used in the design of payload structures, support bracketry, and mounting hardware shall comply with the stress corrosion requirements of MSFC-SPEC-522. For those applications in which MSFC-SPEC-522 requires the submittal of a materials usage agreement, the data shall be submitted as a waiver request in accordance with JSC 13830.

4. Pressure Vessels. Pressure vessels shall meet the ASME Boiler and Pressure Vessel Code, Section VIII, Divisions 1 and 2, or MIL-STD-1522. Where weight limitations prohibit meeting the above standards for flight vessels, NSS/HP 1740.1 shall be used as the standard with an ultimate safety factor of 1.5 or greater. Pressure vessels using MIL-STD-1522 or NSS/HP 1740.1 shall also be qualification tested to demonstrate no failure at the design burst pressure level. Pressure vessels using the ASME Code or MIL-STD-1522 shall also be qualification tested to demonstrate a life cycle capability of at least twice the maximum predicted number of operating cycles. Particular attention shall be given to insure compatibility of fluids used in cleaning, test, and operation with pressure vessels.

5. Pressurized Lines and Fittings. Pressurized lines and fittings with less than a 1.5-inch inside diameter shall have an ultimate factor of

safety equal to or greater than 4.0. Those with a 1.5-inch or greater inside diameter shall have an ultimate factor of safety equal to or greater than 1.5. Other pressure system components not considered pressure vessels, lines, and/or fittings shall have an ultimate factor of safety equal to or greater than 2.5.

6. Decompression. Payloads located within manned pressurized volumes designed to withstand decompression or subsequent repressurization shall be capable of tolerating the differential pressure without resulting in a hazard.

7. Sealed Containers. Sealed containers shall be analyzed to establish hazard potential. Containers with hazardous potential must be proof tested to 1.5 times the nominal pressure differential.

209 MATERIALS. Materials test data for hazardous fluid compatibility, flammability, and offgassing are contained in JSC 02681. JSC 09604 contains a listing of materials (both metals and nonmetals) with a "rating" indicating acceptability for each material's characteristics. The payload material requirements for hazardous materials, flammability, and offgassing are as follows:

1. HAZARDOUS MATERIALS.

   a. General. Hazardous materials shall not be released or ejected in or near the Orbiter. Hazardous fluid systems must contain the fluids after exposure to all STS environments unless the use of the Orbiter vent/dump provisions have been negotiated with the STS operator. Particular attention should be given to materials used in systems containing hazardous fluids. These include gaseous oxygen, liquid oxygen, propellants, oxidizers, and other fluids that could theoretically cause an exothermic reaction. Those materials within the system exposed to oxygen (liquid and gaseous), both directly and by a single failure, must meet the requirements of NHB 8060.1 for type D materials at the maximum use temperature and pressure. Materials within the system exposed to other hazardous fluids, both directly and by a single failure, must pass the fluid compatibility requirements of NHB 8060.1 for type J materials at maximum use pressure and temperature. The payload supplier's compatibility data on hazardous fluids may be used to accept materials in this category if approved by NASA.

   b. Mercury. The use of mercury or its compounds shall be minimized. Where used, the following information shall be documented prior to NASA approval:

      1) A list of equipment containing mercury to be used with justification for each use.

      2) The amount of mercury contained in the equipment.

      3) How the equipment is protected to prevent release of the mercury.

4) A defined plan to accomplish decontamination if mercury is released.

2. Orbiter Cabin Materials. Payload materials which are to be carried within the Orbiter cabin must meet the requirements of NHB 8060.1, "Flammability, Odor, and Offgassing Requirements and Test Procedures for Materials in Environments that Support Combustion" and the requirements of SE-R-0006, "General Specification, NASA JSC Requirements for Materials and Processes" or an approved equivalent. Payload elements carried in areas other than the Orbiter cabin are not required to meet the requirements of NHB 8060.1.

3. Flammable Materials. In areas other than the Orbiter cabin, the following good practices are required to be followed. Flammable materials exposed to the ambient atmosphere shall be separated to prevent flame propagation paths. Similarly, separation of flammable materials from possible ignition sources is required to the maximum extent practicable. Minimizing the use of flammable materials shall be the preferred means of hazard reduction. Materials are considered nonflammable or self-extinguishing if they meet the applicable flammability test requirements of NHB 8060.1. Reference may also be made to JSC 02681 for current flammability test data and to JSC 09604 and JSC 11123 for materials selection lists and guidelines. For materials which have no prior NASA flammability test data, the payload organization shall present other flammability test results for NASA review or request assistance from NASA in conducting applicable tests.

4. Material Offgassing. Usage of materials which produce toxic offgassing 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 selection and control to avoid unacceptable offgassing is a negotiable alternative to black-box level testing. NHB 8060.1 or an STS operator approved equivalent shall be used for the black-box level offgassing test.

210 PYROTECHNICS.

1. General. All pyrotechnic subsystems and devices shall meet the design and test requirements of MIL-STD-1512, "Electroexplosive subsystems, electrically initiated, design requirements and test methods."

2. Catastrophic Hazards. Special safety requirements apply to pyrotechnic initiators used for functions when premature firing is catastrophic. It must be thoroughly demonstrated that such initiators are not susceptible to premature firing from electrostatic discharge. These special requirements do not apply where an S&A device provides a mechanical interrupt of the pyrotechnic train immediately downstream of the initiator and where the S&A device stays in the "SAFE" position until after the payload has been deployed and reaches a safe distance from the Orbiter. These requirements do apply, however, when an S&A device is not provided or when an S&A device is provided but actuated to the "ARM" position before deployment. These special requirements apply even

though multiple interlocks or inhibits are provided in the electrical firing circuit in accordance with paragraph 202. The special requirements are given in paragraph 210-4.

3. NASA Standard Initiators. Due to concern about the electrostatic discharge sensitivity of initiators used for functions such as described in paragraph 210-2, NASA has developed NSI-type standard initiators (NASA Standard Initiators) which fully comply with these special safety requirements and which require no further demonstration. NSI-type initiators are single bridgewire units with a ceramic insulating cup for the explosive mix and a hermetically sealed spark gap protective feature to bypass electrostatic discharges around (rather than through) the explosive mix.

4. Transition Payloads. For payloads where the preliminary design has been approved by the responsible payload organization, NSI-type initiators are preferred for functions such as described in paragraph 210-2 and require no further demonstration. Where this is not practicable or cost effective, other initiators are acceptable if they meet the criteria and demonstration requirements listed below:

   a. Flight unit acceptance test. Each flight initiator 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. The resistor of the MIL-STD has been specified to simulate the impedance of human skin to electrostatic charge transfer when people are the charge generators or carriers of concern. However, other charge carriers are of concern for orbital space operations in the payload bay, where there might be little or no transfer impedance thus significantly affecting the voltage rise rate seen by the initiator. All initiators must pass this acceptance test without firing. The entire lot is to be rejected if there is a single failure. However, if it can be shown that the failure is an isolated case and that the failure mechanism is fully understood, a waiver may be submitted for consideration.

   b. Design configuration. Single bridgewire initiators are preferred. Dual bridgewire initiators are inherently more sensitive because they negate the insulating advantage of the charge cup provided in single bridgewire designs. If dual bridgewire initiators are used, the paragraph 210-4a test applies 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.

   c. 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.

5. New Payloads. For new payloads in which preliminary design has not been approved by the responsible payload organization, NSI-type initiators should be used for functions such as deployment from the Orbiter, stage separation, and SRM ignition, where premature firing is catastrophic. Alternate equivalent initiator designs will be considered on a case-by-case basis and will require approval by the STS.

6. Electrical Connection of Pyrotechnic Devices. Payloads with pyrotechnic devices, which if prematurely fired may cause injury to people or damage to property, shall be designed to be electrically connected in the Orbiter and to have electrical interfaces verified before connecting the pyrotechnic devices. Exceptions to this require specific approval of the launch site safety office.

211 DESTRUCT SYSTEMS. Destruct systems will be used only when approved by the STS operator and must comply with the requirements of paragraphs 202 and 204.

212 RADIATION.

1. Ionizing Radiation. All 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 JSC 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.

2. Nonionizing Radiation. Payloads shall not emit electromagnetic radiation (including x-rays) which presents a hazard. Maximum acceptable cargo-produced radiated fields are specified in JSC 07700, Volume XIV, attachment I. The payload design shall be compatible with the payload bay environment as specified in JSC 07700, Volume XIV, attachment I. Transmitter antenna systems shall not be turned on during Orbiter ascent and descent.

213 ELECTRICAL SYSTEMS. 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. Where lightning protection is required to avoid a catastrophic hazard, document JSC 07636 shall be used as a guide for payload design.

214 VERIFICATION REQUIREMENTS. The safety aspect of any hazardous payload safety-critical equipment shall be satisfactorily verified. Test, analysis, and inspection are techniques for verification. The methods of verification shall be documented, maintained, and submitted in support of the incremental safety assessment reviews (paragraph 304).

215 HAZARDOUS PROCEDURES. Potentially hazardous operations shall be identified and technical operating procedures shall be prepared, for assembly, test, and use. Such procedures shall be verified to demonstrate control of the hazard.

216 REFLOWN HARDWARE. STS payloads and elements of STS payloads to be reflown on another STS mission shall be reviewed for:

1. Correction of any safety deficiency encountered on previous missions.

2. Safety impact of any changes made to the hardware or operating procedures.

3. Any maintenance and/or refurbishment affecting safety.

4. Appropriate design and verification features for reuse.

5. Safety of reuse in view of gradual wearout of the hardware or subtle degradation (including fatigue) in previous use.

6. Any limited life items that may affect safety.

217 EXTRAVEHICULAR ACTIVITY. Payload organizations who plan to use crew EVA for payload operations shall comply with the design requirements of JSC 10615.

218 SERIES PAYLOADS. Subsequent payloads of a series that are intended to be flown on the STS will be reviewed for:

1. Safety impact of all changes to the subsequent payload including modifications to the hardware and revisions to the payload operating procedures.

2. Correction of any safety deficiency encountered on previous members of the series.

3. Any limited life items that may affect safety.

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.

CHAPTER 3: SYSTEM SAFETY 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 STS operator in accordance with paragraph 304. Detailed instructions for the safety analysis and safety assessment reports are provided in JSC 13830.

302 HAZARD LEVELS. Hazards are classified according to potential as follows:

1. Critical Hazard. Results in damage to STS equipment, or the use of contingency or emergency procedures.

2. Catastrophic Hazard. Results in the potential for 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:

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.

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.

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 or 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 personnel reaction to the signal.

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. Safety assessment reviews will be conducted by the STS flight operator (JSC) and the STS launch/landing site operator (KSC) 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. These meetings will be held at JSC and KSC. 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 safety review process must be completed, and the certificate of payload safety compliance must be signed in accordance with paragraph 305.1 prior to the installation of the payload in the Orbiter.

1. Data Submittal. Data shall be submitted prior to each meeting in support of these reviews. Data items shall include those necessary to certify that all safety requirements have been satisfied. Waiver requests and supporting rationale will normally be submitted at the time the need is identified. In addition, data submittal items shall include those specified in paragraph 305 applicable to the existent phase of the program at the time of each review with other data as requested, including safety-related design and operations data, schematics of hazardous systems, and manufacturing assembly and handling procedures.

2. Concurrence and Approval. The basis for review concurrence and approval will be documented in minutes issued jointly after each meeting; these minutes will also list action items and open items. When a hazardous system, associated operation, verification method, or related documentation is modified, approval becomes invalid and a new review and approval are required. Detailed responsibilities, review procedures, and data submittal requirements are given in JSC 13830.

305 SAFETY COMPLIANCE DATA. A safety compliance data package shall precede the delivery of the payload to the launch site by 30 days and shall contain the following items. The items marked with an asterisk shall be included in the data package submitted for the phase III review.

1. A statement signed by the payload organization certifying the compliance of the payload with the safety requirements of this document.

*2. A safety assessment report which documents the results of the paragraph 301 Safety Analysis, including hazard description, controls, and safety verification methods (see JSC 13830).

*3. Approved waivers to safety requirements.

*4. A listing of radioactive materials in accordance with JSC 13830.

*5. A list which identifies and characterizes all RF transmitters and all electromagnetic radiation which exceeds the limit for cargo-produced radiated fields as specified in JSC 07700, Volume XIV, attachment I. In addition, the list shall include equipment capable of producing a field strength more than 10 milliwatts per square centimeter for ground safety purposes.

*6. A log book maintained on each pressure vessel/system showing pressurization history, fluid exposures and other pertinent data shall be delivered with the payload. (For the phase III safety review, a summary of the log book is sufficient.)

*7. A summary of all safety-related failures or accidents related to payload processing, test and checkout, including an assessment of their potential impact to STS, elements of STS, and to ground safety, together with action taken to prevent recurrence.

*8. Detailed technical operating procedures for launch and landing site (including contingency sites) operations which are hazardous in nature. There shall be step-by-step directions covering items such as personnel access controls, emergency procedures, and weather restrictions.

*9. A list of all uses of mercury and its compounds in accordance with the data requirements of paragraph 209-1b.

*10. 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.

306 ACCIDENT/INCIDENT/MISSION FAILURES INVESTIGATION AND REPORTING. Accident/incident/mission failures investigation and reporting for NASA equipment will be handled under the provisions of NMI 8621.1 and NHB 1700.1(VI). For accident/incident/mission failures involving non-U.S. Air Force 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 STS operator to be pertinent. For U. S. Air Force payloads, the "Air Force-NASA Agreement on Joint Space Program Accident Investigations" will be the controlling document.

APPENDIX A: GLOSSARY OF TERMS

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

ADIABATIC 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) - See PSE.

CARGO - Everything contained in the Shuttle payload bay, plus other equipment located elsewhere in the Orbiter which is payload unique and not carried in the standard baseline Orbiter weight budget. This includes payloads and payload-support equipment.

CATASTROPHIC HAZARD - See paragraph 302.

CERTIFICATE OF SAFETY COMPLIANCE - A formal documented approval of the safety assessment effort. Includes a statement that all safety requirements of this document have been met or, if not, what waivers are applicable.

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 herein.

CRITICAL HAZARD - See paragraph 302.

EMERGENCY - Any condition which can result in crew injury or threat to life and requires immediate corrective action, including predetermined crew response.

EVA - Extravehicular activity by the flight crew.

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

FLIGHT CREW - Any personnel onboard the Space Shuttle engaged in flying the Space Shuttle and/or managing resources onboard (e.g., commander, pilot, mission specialist).

FLIGHT PERSONNEL - All personnel carried on the Space Shuttle vehicle including flight crew, passengers, and payload specialists.

FREEFLYING PAYLOAD - A payload which is deployed and separated from the Orbiter.

GSE - Ground support equipment.

HAZARD - The presence of a potential risk situation caused by an unsafe act or condition.

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 a single event or environment cannot eliminate more than one inhibit, and all inhibits cannot be removed by the same type of event or environment.

INHIBIT - A design feature that prevents operation of a function.

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

KSC - Kennedy Space Center, NASA, Florida 32899.

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

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

NEAR REAL TIME - Available to the crew within one earth orbit.

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).

NSI-TYPE - NSI configuration pyrotechnic initiators from specific lots which have been predetermined to be acceptable to NASA from a safety standpoint.

OFFGASSING - The emanation of volatile matter of any kind from materials into a manned pressurized volume.

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 freeflying automated spacecraft, individual experiments or instruments, PSE, etc. As used in this document, the term payload also includes payload-provided GSE and systems and flight and ground systems software.

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

PAYLOAD ELEMENTS - Experiments, instruments, or other individual payload items which are subsets of an integrated, multipayload cargo complement on missions such as Spacelab, 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 Center the authority for formal interface with the STS operator in the implementation of this document. Other payload organizations include, but are not limited to, the following: DOD, other U. S. Government agencies, non-U.S. Government public organizations, private persons or private organizations, international organizations, European Space Agency, foreign governments, etc.

PERSONNEL INJURY - With respect to catastrophic hazard levels for STS payloads, personnel injury shall be limited to loss of life or major injury which results in the incapacitation of the crew (e.g., bone fractures, second or third degree burns, severe lacerations, internal injury, severe radiation exposure, unconsciousness, etc.).

PRESSURE VESSEL - A container that stores pressurized fluids and:

(1) Contains stored energy of 14,240 foot-pounds (19,310 joules) or greater based on adiabatic expansion of a perfect gas; or

(2) Contains a gas or liquid which will create a hazard if released; or

(3) Will experience a design limit pressure greater than 100 psi.

PSE (Payload-Support Equipment) - The flight equipment and systems needed to support the payload such as caution and warning, data recording, controlled functions, instrumentation, payload cradles, etc.

REAL TIME - Available to the crew upon demand.

RISK - The chance (qualitative) of personnel injury or fatality, damage to or loss of equipment or property.

SAFE DISTANCE - The distance that must be obtained between the Orbiter and a freeflying payload to permit performance of a function without presenting a hazard to the Orbiter and/or crew.

SAFETY - Freedom from chance of personnel injury or fatality, and damage to or loss of equipment or property.

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

SAFETY CRITICAL - Containing an element of risk.

SAFING - (1) Action to retreat from an armed condition.

(2) 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.

STS (Space Transportation System) - The Space Shuttle, Spacelab, IUS (inertial upper stage), and the ground sites needed to support these elements.

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

STS OPERATOR - The NASA Headquarters/STS Operations Directorate is the STS operator. NASA/JSC is the STS flight operator and is responsible for the safety of payload flight systems and flight operations. NASA/KSC is the STS launch/landing site operator and is responsible for the safety of payload GSE and ground operations. The JSC STS Operations Program Office is the primary point of contact for formal interface between the STS operator and the payload organization in the implementation of this document. JSC accomplishes this with the participation and concurrence of KSC. Further delineation of STS implementation roles and responsibilites is given in JSC 13830.

USER - See "PAYLOAD ORGANIZATION."

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

APPENDIX B: APPLICABLE DOCUMENTS

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 shall be considered superseding requirements. Copies of these documents can be obtained from Code JM61, Johnson Space Center, NASA, Houston, Texas 77058.

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
KSC-K-STSM-14.1, "Launch Site Accommodations Handbook for STS Payloads"	101
JSC 11123, "STS Payload Safety Guidelines Handbook"	103-1, 209-3
JSC 13830, "Implementation Procedure for STS Payloads System Safety Requirements"	103-2, 200, 208-3, 212-1, 301, 304-2, 305-2, 305-4
JSC 07700, Volume XIV, Attachment I, "Shuttle Orbiter/Cargo Standard Interfaces"	208-2, 212-2, 305-5 202-2e
MSFC-SPEC-522, "Design Criteria for Controlling Stress Corrosion Cracking"	208-3
ASME Boiler and Pressure Vessel Code, Section VIII, Divisions 1 and 2	208-4
MIL-STD-1522, "Standard General Requirement for Safe Design and Operation of Pressurized Missile and Space Systems"	208-4
NSS/HP-1740.1, "NASA Aerospace Pressure Vessel Safety Standard"	208-4
JSC 09604, "JSC Government-Furnished Equipment Materials Selection List and Materials Documentation Procedures"	209, 209-3
JSC 02681, "Nonmetallic Materials Design Guidelines and Test Data Handbook"	209, 209-3
NHB 8060.1, "Flammability, Odor, and Offgassing Requirements and Test Procedures for Materials in Environments That Support Combustion"	209-1 209-2, 209-3, 209-4
SE-R-0006, "NASA JSC Requirements for Materials and Processes"	209-2
MIL-STD-1512, "Electroexplosive Subsystems, Electrically Initiated, Design Requirements, and Test Methods"	210, 210-4a

JSC 07636, "Space Shuttle Program Lightning Protection Criteria Document"	213
JSC 10615, "Shuttle EVA Description and Design Criteria"	217
NMI 8621.1, "Policy Directive Accident/Incident/ Mission Failures Investigation and Reporting"	306
NHB 1700.1 (V1), "NASA Safety Manual"	306
"Air Force-NASA Agreement on Joint Space Program Accident Investigations"	306