SPACE SHUTTLE PAYLOAD DESIGN AND DEVELOPMENT

(NASA-TM-108231) SPACE SHUTTLE PAYLOAD DESIGN AND DEVELOPMENT. VOLUME 7: SAFETY GUIDELINES AND REQUIREMENTS (NASA) 56 p

SAFETY GUIDELINES AND REQUIREMENTS

Rev 1 9/84

National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
SYSTEM PAYLOAD GROUND SAFETY HANDBOOK
— SAMTO HB S-100/KHB 1700.7, "SPACE TRANSPORTATION
SAFETY REQUIREMENTS"
— JSC 18798, "INTERPRETATIONS OF STS PAYLOAD
HANDBOOK"
— JSC 11123, "STS PAYLOAD SAFETY GUIDELINES
PAYLOADS SYSTEM SAFETY REQUIREMENTS"
— JSC 13830A, "IMPLEMENTATION PROCEDURE FOR STS
REFERENCE DOCUMENTATION
SYSTEM SAFETY REQUIREMENTS
TECHNICAL REQUIREMENTS
SYSTEM (STS)
PAYLOADS USING THE SPACE TRANSPORTATION
NHB 1700.7A, "SAFETY POLICY AND REQUIREMENTS FOR
STS REQUIREMENTS
DESIGN AND DEVELOPMENT
VNSA
SHUTTLE SPACE
PAYLOAD
● NASA
  ● REVIEW PAYLOAD FOR ADEQUATE SAFETY IMPLEMENTATION
  ● ENSURE THAT THE TOTAL MIXED CARGO COMPLEMENT DOES NOT CREATE A HAZARD

● PAYLOAD ORGANIZATION
  ● ENSURE THE SAFETY OF TOTAL PAYLOAD, INCLUDING INTERACTION BETWEEN PAYLOAD ELEMENTS
  ● ENSURE IMPLEMENTATION OF THE REQUIREMENTS OF NHB 1700.7A

*(REFERENCE NHB 1700.7A PARA. 102)*
SAFETY RESPONSIBILITY
SEVERAL EXPERIMENTS ON THE SAME PALLET

PROGRAM MANAGER OR MISSION
MANAGER RESPONSIBLE FOR INTEGRATED
PAYLOAD — EXPERIMENTS, CARRIER,
AND SUPPORT EQUIPMENT.
GROUND SUPPORT EQUIPMENT
CARGO INSTALLATION
RANGE SAFETY
BIOENGINEERING
FUEL/CRYO HANDLING
GROUND PROCESSING

MEMBERS FROM THE FOLLOWING TECHNICAL AND OPERATIONAL DISCIPLINES

CHAIRMAN - FROM KSC SYSTEMS ENGINEERING OFFICE

PROCESsING

KSC - GROUND SUPPORT EQUIPMENT DESIGN AND GROUND SUPPORT

LIFE SCIENCES
GROUND OPERATIONS
ENGINEERING
SAFETY
OPERATIONS
ORBITER INTEGRATION

MEMBERS FROM THE FOLLOWING TECHNICAL AND OPERATIONAL DISCIPLINES

CHAIRMAN - FROM JSC PAYLOAD INTEGRATION OFFICE

JSC - PAYLOAD DESIGN AND FLIGHT OPERATIONS

STS PAYLOAD SAFETY REVIEW PANELS

VNAV

DESIGN AND DEVELOPMENT
Schedule Phase 0 Safety Review

Briefing on Implementation Procedure and Safety Reviews

Provide Safety Documents

(PIP) Meeting

Concurrent with Initial Payload Integration Plan

Initial Contract Meeting with Payload Organization Design and Development
SAFETY REVIEWS

• FORMAL MEETINGS WITH PAYLOAD ORGANIZATION TO ASSESS COMPLIANCE WITH THE REQUIREMENTS OF NHB 1700.7A
  • PAYLOAD DESIGN AND FLIGHT OPERATIONS
  • GSE DESIGN AND GROUND OPERATIONS
• DEPTH AND NUMBER OF REVIEWS DETERMINED BY PAYLOAD HAZARD POTENTIAL AND PAYLOAD MATURITY
• SCHEDULE FOR REVIEWS
  • ESTABLISHED BY PAYLOAD ORGANIZATION
  • COORDINATED WITH JSC PAYLOAD INTEGRATION OFFICE OR KSC CARGO PROJECTS OFFICE
• DATA SUBMITTED TO JSC/KSC
  • REVIEWED BY PANEL
  • ACTUAL REVIEW DATE ESTABLISHED AFTER SUBMITTAL OF REVIEW MATERIAL
• MEETING MINUTES
  • PHASE O — PREPARED BY SAFETY OFFICE
  • PHASE I, II, III — PREPARED BY SAFETY OFFICE
    — SIGNED BY PANEL CHAIRMAN AND PAYLOAD ORGANIZATION
  • DISTRIBUTED BY SAFETY OFFICE
DATA REQUIREMENTS

- CONCEPTUAL DESCRIPTION OF THE PAYLOAD/GSE AND ITS OPERATIONS
- CONCEPTUAL DESCRIPTION OF SAFETY-CRITICAL SUBSYSTEMS
- CONCEPTUAL DESCRIPTION OF GROUND OPERATIONS FLOW
- REQUIREMENTS MATRIX
- PHASE 0 HAZARD REPORTS

PHASE 0 SAFETY REVIEW MEETING

- DESCRIPTION OF SAFETY CRITICAL SUBSYSTEMS
- APPLICABLE SAFETY REQUIREMENTS
- PHASE 0 HAZARD REPORTS
- DATA REQUIREMENTS FOR THE PHASE I SAFETY REVIEW
- BRIEFING ON LAUNCH AND LANDING SITE SAFETY
Review and Disposition of Phase I Hazard Reports

Assessment of Applicable Requirements

GSF/Ground Operations

Overview of Payload Including Mission Scenario and

Phase I Safety Review Meeting

— Description of GSF and Ground Operations

— Ionizing Radiation Source Data Sheets (JSC Form 44)

New Data Required

— Hazard Reports

Operations

— Description of Safety-Critical Subsystems Including

Payload Description and Mission Scenario

Update As Required

Data Requirements

(S-84-01814)

Phase I Safety Review

Design and Development
DATA REQUIREMENTS

- UPDATE AS REQUIRED
  - PAYLOAD DESCRIPTION AND MISSION SCENARIO
  - DESCRIPTIONS OF SAFETY-CRITICAL SUBSYSTEMS AND OPERATIONS INCLUDING GSE AND GROUND OPERATIONS
  - HAZARD REPORTS
  - IONIZING RADIATION SOURCE SHEET

NEW DATA REQUIRED

- SAFETY-RELATED FAILURES OR ACCIDENTS
- LISTING OF EQUIPMENT GENERATING HAZARDOUS RADIATION
- ADDITIONAL HAZARD REPORTS, IF ANY

PHASE II SAFETY REVIEW MEETING

- STATUS OF PHASE I ACTION ITEMS
- OVERVIEW OF PAYLOAD WITH SPECIAL EMPHASIS ON DESIGN CHANGES SINCE PHASE I
- UPDATED ASSESSMENT OF APPLICABLE REQUIREMENTS
- REVIEW AND DISPOSITION OF HAZARD REPORTS
See JSC 13830A para 6.0, Payload Safety Noncompliance Report

- Review and disposition of safety compliance data
- Status of open action items

Phase III Safety Review Meeting

- Listing of pyrotechnics
- Pressure vessel logbook
- Approved waivers/deviations
- Listing of open safety items
- Summary of safety-related failures or accidents
- New data requirements

Data requirements (Safety Compliance Data Package)

Update as required

S-84-01817

Phase III Safety Review

Design and Development
THE PAYLOAD ORGANIZATION HEREBY CERTIFIES THAT

(1) THE PAYLOAD IS SAFE

(2) THE PAYLOAD COMPLIES WITH ALL APPLICABLE REQUIREMENTS OF NHB 1700.7A, "SAFETY POLICY AND REQUIREMENTS FOR PAYLOADS USING THE SPACE TRANSPORTATION SYSTEM" EXCEPT AS DEFINED IN THE FOLLOWING WAIVERS

WAIVER NO. _______

_______

_______

APPROVED: ____________________________

PAYLOAD ORGANIZATION DATE

PAYLOAD MANAGER
CERTIFICATION OF BASELINE

ZERO OR MINIMAL CHANGES

(PAYLOADS)

STANDARD ELEMENTS (SERIES AND REFLOW)

NO Formal REVIEW

MINIMUM INTERFACES

SIMPLE DESIGN

LOW HAZARD POTENTIAL

Telecon REVIEW

STS PAYLOAD EXPERIENCE

COMPLEXITY

DESIGN MATURITY

COMBINED PHASES

NUMBER AND DEPTH OF REVIEWS MAY BE TAILORED
CRITICAL HAZARDS

- No single failure or operator error shall result in contingency or emergency procedures
- Functions must be controlled by two independent inhibits
- Monitoring on a case-by-case basis

CATASTROPHIC HAZARDS

- No combination of two failures, operator errors, or RF signals shall result in the potential for personnel injury, or loss of the orbiter, ground facilities, or STS equipment
- Functions must be controlled by three independent inhibits whenever hazard potential exists
- If payload is attached and powered, monitoring of two inhibits is generally required
Envelopes
- RF energy Radiation above ICD levels at orbiter

Closure
- Deployment/Extension preventing payload bay door

Payload cannot withstand landing environment
- Premature separation or deployment so that

200 feet separation for > 10 lb thrust
- Three independent flow control devices
- Propellant propulsion system
- Premature firing or adiabatic detonation of liquid

45-minute coast prior to ignition
- Safe and arm in safe for boost and entry
- Premature firing of solid rocket motor

The following are classified as catastrophic hazards

Catastrophic Hazards (cont)
PAYLOAD RETRIEVAL
- Establish safe configuration prior to orbiter approach

PAYLOAD CONTINGENCY RETURN
- Payload capability to return to safe configuration until separation from orbiter

FAILURE PROPAGATION
- Design to preclude propagation of failures to environment outside payload

REDUNDANCY SEPARATION
- Design to minimize propagation of failures between safety-critical subsystems

STRUCTURAL
- Factor of safety 1.4 (except emergency landing)
- Fracture control procedures for catastrophic function
- Factor of safety of 1.0 for emergency landing
OF FUGA SING TESTS FOR COMPONENTS IN ORBITER CABIN

CONTROL

GOOD DESIGN PRACTICE IN PAYLOAD BAY FOR FLAMMABILITY

ORBITER CABIN USAGE MUST MEET NHB 8060.1B

MINIMIZE USE OF MERCURY

REACTION FOR SYSTEMS CONTAINING HAZARDOUS MATERIALS

SINGLE BARRIER FAILURE SHOULD NOT CAUSE HAZARDOUS

DESIGN TO CONTAIN EFFLUENTS

MATERIALS

IF HAZARDOUS

- Sealed container proof tested to F.O.S. of 1.5
- Qual test to design burst
- NSS/HF 1740.1 with factor of safety (F.O.S.) 1.5
- MIL-STD-1522
- ASME Boiler Code
- Pressure vessels

ACCORDANCE WITH MSFC SPEC-522

MATERIAL SELECTION TO PREVENT STRESS CORROSION IN

STRUCTURAL (CONT)

TECHNICAL REQUIREMENTS SUMMARY (CONT)

DESIGN AND DEVELOPMENT

NAS
• STRUCTURED TO PAYLOAD DEVELOPMENT
• COST EFFECTIVE
• FLEXIBLE
• ACCOMMODATE STANDARD DESIGNS/APPLICATIONS (JSC 13830 REV. A PARA. 8.0)
• STREAMLINE SERIES/REFLOWN HARDWARE CERTIFICATION (NHB 1700.7A PARA. 216 AND 218)
Special Issue/Question Disposition As Required

Requirements

JSC 18798, "Interpretations of STS Payload Safety

Requirements

Safety Panel Interpretations of Policy/

Specific Issues

Coordinate Detailed Technical Assistance

Issue/Question Discussion

Pre-Review Consultation

Single Point of Contact for Safety

Safety Engineer Support

Help Available To Customer

Design and Development

_payload

Shuttle Space
APPROVAL BY THE STS OF A DEVIATION OR WAIVER
NONCOMPLIANCE TO THESE REQUIREMENTS REQUIRES

LANDING CONDITIONS
COMPATIBLE WITH CONTINGENCY ABORT AND EMERGENCY
PAYLOADS PLANNED TO BE DEPLOYED MUST BE
MISSION INCURRING ABORT AND EMERGENCY LANDING
NATURAL AND INDUCED ENVIRONMENTS OF THE STS
THOSE REQUIREMENTS APPLY UNDER WORST CASE

FLOWN ON THE STS
THOSE REQUIREMENTS APPLY TO ALL PAYLOADS THAT ARE

GENERAL (200)

TECHNICAL REQUIREMENTS (NHB 1700.74)
SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT
FAILURE TOLERANCE (201)

- Payloads must tolerate applicable number of credible failures and/or operator errors for hazardous functions depending on hazard level.
- Applicable for hazards resulting from
  - Loss of function
  - Inadvertent occurrence of function
- Hazard level
  - Critical hazard — No single failure or error shall result in damage to STS equipment or contingency or emergency procedures
  - Catastrophic hazards — No combination of two failures, errors, or radio frequency signals shall result in the potential for personnel injury, loss of the orbiter, ground facilities, or STS equipment
are connected to unpowered bus—no monitoring if power and control circuits

time, when required—flight or ground crew monitor in near-real

case-by-case basis—monitor and return to safe condition on a

two independent inihbition functions resulting in critical hazards

control of hazardous functions (20)

TECHNICAL REQUIREMENTS

SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT
• CONTROL OF HAZARDOUS FUNCTIONS (202) (CONT)
  • FUNCTIONS RESULTING IN CATASTROPHIC HAZARDS
    — THREE INDEPENDENT INHIBITS
    — NO MONITORING AND SAFING REQUIRED IF POWER
      AND CONTROL CIRCUITS CONNECTED TO UNPOWERED
      BUS
    — MONITOR AT LEAST TWO OF THREE INHIBITS WHEN
      POWER AND/OR CONTROL BUS POWERED
    — SPECIFIC MONITORING AND SAFING REQUIREMENTS
      FOR IDENTIFIED CATASTROPHIC HAZARDS BASED ON
      PLANNED OPERATIONS

(BASIC APPROACH IS TO DESIGN TO TWO-FAILURE
TOLERANCE AND MAINTAIN KNOWLEDGE THROUGH REAL
OR NEAR REAL-TIME MONITORING OF SINGLE FAILURE
TOLERANCE)
SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- SOLID PROPELLANT ROCKET MOTORS
  - PREMATURE FIRING IS A CATASTROPHIC HAZARD
  - COAST 45 MINUTES AT 1 FT/SEC PRIOR TO FIRING OR CREW OPERATED RADIO FREQUENCY (RF) INHIBIT
  - SAFE AND ARM (S&A) WITH MECHANICAL INTERRUPT IN PYRO TRAIN
  - TWO ADDITIONAL INHIBITS
  - IF POWER OR CONTROL BUS POWERED PROVIDE CREW MONITORING AND CAPABILITY TO COMMAND S&A DEVICE
  - ADDITIONAL REQUIREMENTS BASED ON WHEN THE SAFE AND ARM IS TO BE ROTATED

  - S&A DEVICE NOT ROTATED UNTIL PAYLOAD REACHES SAFE DISTANCE
    - FLIGHT OR GROUND CREW MONITOR OF TWO ADDITIONAL INHIBITS IN NEAR REAL TIME

  - S&A DEVICE ROTATED PRIOR TO PAYLOAD REACHING SAFE DISTANCE
    - S&A DEVICE IN SAFE POSITION FOR BOOST AND ENTRY
    - FLIGHT CREW ROTATES S&A DEVICE TO ARM JUST BEFORE DEPLOYMENT
    - MINIMUM THREE INHIBITS REMAIN SAFE
    - FLIGHT OR GROUND CREW REAL-TIME MONITOR OF TWO ADDITIONAL INHIBITS
    - PYRO INITIATOR MUST MEET SPECIAL REQUIREMENTS
MIXING OR EXPULSION THROUGH THRUST CHAMBERS
FOR BIPROPELLANT SYSTEM DEVICES MUST PREVENT PROPELLANT
(SEE FOLLOWING PAGE)

DEFINED IN NASA LETTER NS 2/83-L167 DATED JUNE 10, 1983
SAFE DISTANCE FOR GREATER THAN 10 POUNDS THRUST
10 POUNDS
SAFE DISTANCE IS 200 FT FOR THRUST LESS THAN OR EQUAL TO
ADIBATIC DETONATION
OPENING OF ANY FLOW CONTROL DEVICE SHALL NOT RESULT IN
MINIMUM OF ONE FLOW CONTROL DEVICE "FAIL SAFE"
MINIMUM OF THREE FLOW CONTROL DEVICES (INHIBITS) IN SERIES WHICH REMAIN CLOSED
FLOW CONTROL DEVICE TO ISOLATE TANK(S) FROM
CATASTROPIC HAZARD
PREMATURE FIRING OR ADIBATIC DETONATION IS A
LIQUID PROPELLANT PROPELLATION SYSTEMS

TECHNICAL REQUIREMENTS
SAFETY POLICY AND REQUIREMENTS
DESIGN AND DEVELOPMENT
REQUIRED IF SYSTEM CANNOT BE SAFE BY CREW COMMAND

- Single Failure-Tolerant Deployment Capability
- Controls by Flight or Ground Crew
- Continuous Real-Time Monitoring of Two Electrical Safe Prior to Isolation Valve Opening
- Two of Three Remaining Electrical Controls Verified
- Opened Only by Flight Crew Command for Deployment
- Isolation Valve Closed During Boost and Entry
- Firing Engine Until Payload Reaches Safe Distance
- Minimum Three Independent Electrical Controls To Minimum Distance

- Isolation Valve Opened Prior to Payload Reaching Safe
- One Monitor Must Be Isolation Valve Control
- Two of Three Electrical Controls in Near Real Time
- Flight or Ground Crew Monitoring of Minimum Of
- Firing Engine
- Minimum Three Independent Electrical Controls To Safe Distance
- Isolation Valve Not Opened Until Payload Reaches
- Requirements Are a Function of Planned Operations
- Electrical Controls, Monitoring, and Safing

- Liquid Propellant Propulsion Systems (Cont)
DEPLOYMENT AND/OR SEPARATION

- Premature deployment or separation to condition in which payloads cannot withstand STS-induces loads (including landing), or which prevents safe orbiter entry, is a catastrophic hazard.

- Three independent inhibits to function must remain safe until function is not a hazard to orbiter or crew.

- Designed to preclude inadvertent mechanical operation in induced environments.

- Pyro devices must meet special requirements.

- Additional requirements are a function of planned operations.
  - Function performed after final separation from orbiter
    - Function not performed until payload at safe distance
    - Flight or ground crew monitor of two inhibits in near real time.

  - Function performed before final separation from orbiter
    - Three inhibits safe for boost and entry
    - Removed only by crew command to perform function
    - Command and monitor of inhibits available to flight crew
    - Ability to return to safe status available to flight crew
These inhibits

No command and monitoring requirements for

Three independent inhibits to radiation

In volume X, IV, Attachment 4, is catastrophic
Cargo radiation in excess of "doors open" levels

RF energy radiation

Combination must be two-failure tolerant

Backup method

Hazard controlled by independent primary and

Door closure

Deployment/extension preventing payload bay

Technical requirements

Safety policy and requirements

Design and development
● RETRIEVAL OF PAYLOADS (203)
  ● CAPABILITY TO RETURN SYSTEMS TO A SAFE CONDITION
  ● VERIFICATION OF SAFE CONDITION TO ORBITER OR GROUND CREW WHILE STILL A SAFE DISTANCE
  ● VERIFICATION MUST ESTABLISH AT LEAST SINGLE-FAULT TOLERANCE

● HAZARD DETECTION AND SAFING (204)
  ● MINIMIZE THE NEED FOR TIME-CRITICAL FLIGHT CREW MONITORING AND CONTROL OF HAZARDOUS FUNCTIONS/SYSTEMS
  ● WHEN USED, PROVIDE GROUND CHECKOUT CAPABILITY

● CONTINGENCY RETURN OF PAYLOADS (205)
  ● DEPLOYABLE PAYLOADS MUST PROVIDE CAPABILITY TO RETURN TO SAFE CONDITION AT ALL TIMES PRIOR TO SEPARATION
  ● SAFE CONDITION MUST MEET REQUIREMENTS OF PARA. 202, “CONTROL OF HAZARDOUS FUNCTIONS”
ONE TO THE OTHER IS MINIMIZED
ARRANGED SO THAT PROPAGATION OF FAILURE FROM
SAFETY-CRITICAL REDUNDANT SUBSYSTEMS SHOULD BE

REDUNDANCY SEPARATION (207)

PAYLOAD

FROM THE PAYLOAD TO THE ENVIRONMENT OUTSIDE THE
DESIGN SHALL PRECLUDE PROPAGATION OF FAILURES

FAILURE PROPAGATION (206)

TECHNICAL REQUIREMENTS

SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT
• STRUCTURAL (208)
  • STRUCTURAL DESIGN
    — ULTIMATE FACTORS OF SAFETY GREATER THAN OR EQUAL TO 1.4 FOR ALL PHASES EXCEPT EMERGENCY LANDING
  • EMERGENCY LANDING LOADS
    — DESIGN SHALL COMPLY WITH EMERGENCY LANDING LOAD FACTORS SPECIFIED IN VOLUME XIV, ATTACHMENT 1
  • STRESS CORROSION
    — MATERIALS MUST COMPLY WITH MSFC-SPEC-522
    — NONCOMPLIANCE REPORT REQUIRED FOR POTENTIAL CATASTROPHIC HAZARDS
  • FRACTURE CONTROL
    — REQUIRED FOR STRUCTURES WHOSE FAILURE WOULD RESULT IN CATASTROPHIC HAZARD
    — REF. - FRACTURE CONTROL GUIDELINES FOR STS PAYLOADS, JSC 18327
STRUCTURAL (208) (CONT)

- PRESSURE VESSELS
  - 3 ACCEPTABLE DESIGN ALTERNATIVES
    - DESIGN TO ASME BOILER AND PRESSURE VESSEL CODE, SECTION VIII, DIV 1 AND 2
      - PROVIDES A 4 TO 1 SAFETY FACTOR
    - DESIGN TO MIL-STD-1522
    - DESIGN TO NSS/HP-1740.1
      - SAFETY FACTOR ≥ 1.5
      - FRACTURE CONTROL PROCEDURES
    - QUAL TEST TO NO FAILURE AT DESIGN BURST FOR MIL-STD-1522 OR NSS/HP 1740.1
    - QUAL TEST TO DEMONSTRATE 2 TIMES PREDICTED LIFE CYCLES FOR ASME CODE OR MIL-STD-1522
      - FLUID COMPATIBILITY FOR CLEANING, TEST, AND OPERATION
GREATER THAN OR EQUAL TO 2.5
OTHER COMPONENTS SHALL HAVE FACTOR OF SAFETY
EQUAL TO 1.5
DIAMETER SHALL HAVE FACTOR OF SAFETY GREATER THAN OR
FITTINGS AND LINES GREATER THAN 1.5 INCHES INSIDE
TO 4.0
FITTINGS AND LINES LESS THAN 1.5 INCHES INSIDE DIAMETER
PRESSURIZED LINES AND FITTINGS

STRUCTURAL (208) (CONT)

TECHNICAL REQUIREMENTS (CONT)

SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT
STRUCTURAL (208) (CONT)

- DECOMPRESSION
  - PAYLOADS IN MANNED VOLUMES DESIGNED FOR DECOMPRESSION AND REPRESSURIZATION MUST WITHSTAND DIFFERENTIAL PRESSURE WITHOUT RESULTING IN A HAZARD
  - AIRLOCK IS AN EXAMPLE

- SEALED CONTAINERS
  - ANALYZED TO ESTABLISH HAZARD POTENTIAL
  - PROOF TEST 1.5 NOMINAL DIFFERENTIAL IF A HAZARD

MATERIALS (209)

- TEST DATA FOR HAZARDOUS FLUID COMPATIBILITY, FLAMMABILITY, AND OFFGASSING IN JSC 02681
- JSC 09604 PROVIDES "ACCEPTABILITY" RATING FOR MATERIALS CHARACTERISTICS
DATA DOCUMENTED PRIOR TO NASA APPROVAL

USE OF MERCURY SHALL BE MINIMIZED WHEN USED SPECIFICALLY

HAZARDOUS MATERIALS - MERCURY

APPROVED BY NASA

COMPATIBILITY DATA BY PAYLOAD MAY BE USED IF

BARRIER FAULT CONTRACT OF FLUIDS

COMPATIBILITY IS REQUIRED FOR DIRECT OR SINGLE

PRESSURE AND TEMPERATURE

OF NHB 8060.1B FOR TYPE J MATERIALS AT MAXIMUM

MATERIALS MUST MEET COMPATIBILITY REQUIREMENTS

OTHER HAZARDOUS FLUIDS SYSTEMS

PRESSURE AND TEMPERATURE

OF NHB 8060.1B FOR TYPE D MATERIALS AT MAXIMUM

MATERIALS MUST MEET COMPATIBILITY REQUIREMENTS

OXYGEN SYSTEMS

MATERIALS USED IN HAZARDOUS FLUID SYSTEMS

VENTING MAY BE NEGOTIATED WITH STS OPERATOR

ENVIRONMENTS

SYSTEMS MUST CONTAIN FLUIDS THROUGHOUT ALL MISSION

SHALL NOT BE RELEASED OR EXCEDED IN OR NEAR ORBIT

HAZARDOUS MATERIALS - GENERAL

TECHNICAL REQUIREMENTS

SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT

NASA
• MATERIALS (209) (CONT)
  • ORBITER CABIN MATERIALS
    — MUST MEET REQUIREMENTS FOR FLAMBABILITY, ODOR, AND OFFGASSING
      • NHB 8060.1B, SE-R-006, OR AN APPROVED EQUIVALENT
    — USAGE OTHER THAN IN ORBITER CABIN NOT REQUIRED TO MEET NHB 8060.1B
  • FLAMMABLE MATERIALS
    — FOR USES OTHER THAN IN THE ORBITER CABIN, GOOD PRACTICES ARE REQUIRED TO MINIMIZE USAGE OF FLAMMABLE MATERIALS WHERE POSSIBLE
    • FLAMMABLE MATERIALS SEPARATED TO PREVENT FLAME PROPAGATION
    • SEPARATE FLAMMABLE MATERIALS FROM IGNITION SOURCES TO MAXIMUM EXTENT PRACTICABLE
      - MATERIALS THAT MEET NHB 8060.1B CONSIDERED NONFLAMMABLE
      - JSC 02681, JSC 09604, AND JSC 11123 PROVIDE TEST DATA, MATERIAL SELECTION LISTS, AND GUIDELINES
      - USER OR NASA TESTS FOR OTHER MATERIALS
NHB 8060.1 OR STS OPERATOR-APPROVED EQUIVALENT TESTS

RIGOROUS MATERIAL SELECTION NEGOTIABLE ALTERNATIVE

TO STS INTEGRATION

OFFGASSING TESTS FOR SAFETY VALIDATION PRIOR

IN HABITABLE AREAS

AVOID MATERIALS WITH TOXIC OFFGASSING

• MATERIAL OFFGASSING (CABIN MATERIALS ONLY)

• MATERIALS (209) (CONT)

TECHNICAL REQUIREMENTS

SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT

NVIDIA PAYLOAD

SHUTTLE SPACE
SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- PYROTECHNICS (210)
  - ALL PYRO SUBSYSTEMS AND DEVICES SHALL MEET MIL-STD-1512 (SEE JSC 18798)

- CATASTROPHIC HAZARDS
  - SPECIAL SAFETY REQUIREMENTS TO DEMONSTRATE THAT DEVICES ARE NOT SUSCEPTIBLE TO PREMATURE FIRING FROM ELECTROSTATIC DISCHARGE
  - EXCEPTION WHEN SAFE AND ARM DEVICE REMAINS SAFE UNTIL PAYLOAD IS AT A SAFE DISTANCE

- NASA STANDARD INITIATORS (NSI)
  - FULLY COMPLY WITH SPECIAL REQUIREMENTS AND REQUIRE NO FURTHER DEMONSTRATION
DETECTION AND SAFETY REQUIREMENTS
MUST COMPLY WITH HAZARD CONTROL AND HAZARD
USE ONLY WHEN APPROVED BY STS OPERATOR
DESTRUCT SYSTEMS (211)

APPROVAL
— EXCEPTIONS REQUIRE SPECIFIC LAUNCH SITE SAFETY OFFICE
INTERFUSE VERIFICATION COMPLETED
AFTER INSTALLATION IN ORBITER AND ELECTRICAL
OR PROPERTY, DESIGN TO BE ELECTRICALLY CONNECTED
— IF PREMATURE FIRING IS HAZARDOUS TO PERSONNEL
— PROCESSING
ELECTRICAL CONNECTION OF PRO DEVICES FOR GROUND
— USE NSI INITIATORS OR STS-APPROVED ALTERNATIVE
NEW PAYLOADS
— USE NSI INITIATORS OR STS-APPROVED ALTERNATIVE
(210) CONT

TECHNICAL REQUIREMENTS
SAFETY POLICY AND REQUIREMENTS
DETECTION AND DEVELOPMENT
RADIATION (212)

IONIZING RADIATION

- ALL PAYLOADS THAT CONTAIN OR USE RADIOACTIVE MATERIALS, OR THAT GENERATE IONIZING RADIATION, REQUIRE STS APPROVAL PRIOR TO USE
- DATA PER JSC 13830
- APPROVAL VIA NASA COORDINATOR TO INTERAGENCY NUCLEAR SAFETY PANEL
- DEPARTMENT OF DEFENSE (DOD) USES ITS OWN PROCEDURES
- MUST COMPLY WITH LICENSE REQUIREMENTS AT LAUNCH SITE

NONIONIZING RADIATION

- PAYLOADS SHALL NOT EMIT ELECTROMAGNETIC RADIATION (INCLUDING X-RAYS) THAT PRESENTS A HAZARD
- MAXIMUM ACCEPTABLE CARGO-PRODUCED FIELDS, PER VOLUME XIV
- COMPATIBLE WITH INDUCED ENVIRONMENT, PER VOLUME XIV
- TRANSMITTERS OFF DURING BOOST AND ENTRY
METHODS DOCUMENTED IN SAFEY REVIEWS
TEST, ANALYSES, AND INSPECTION ARE TECHNIQUES SATISFACTORY VERIFIED

SAFETY ASPECTS OF HAZARDOUS PAYLOAD EQUIPMENT SHALL BE

VERIFICATION REQUIREMENTS (214)

HAZARD, USE JSC 07636 AS DESIGN GUIDE WHEN LIGHTNING PROTECTION REQUIRED FOR CATASTROPHIC FOR PAYLOAD OR ORBITER MATERIAL DESIGN SO THAT FAULTS DO NOT CREATE IGNITION SOURCES INTERNAL TO PAYLOAD DO NOT DAMAGE STS CIRCUITS ELECTRICAL POWER DISTRIBUTION DESIGNED SO THAT FAULTS ELECTRICAL SYSTEMS (213)

TECHNICAL REQUIREMENTS SAFETY POLICY AND REQUIREMENTS DESIGN AND DEVELOPMENT
SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

• HAZARDOUS PROCEDURES (215)
  • POTENTIALLY HAZARDOUS OPERATIONS SHALL BE IDENTIFIED AND OPERATING PROCEDURES PREPARED FOR ASSEMBLY, TEST, AND USE
  • PROCEDURES SHALL BE VERIFIED TO DEMONSTRATE CONTROL OF THE HAZARD

• REFLOWN HARDWARE (216)
  • HARDWARE TO BE REFLOWN SHALL BE REVIEWED FOR
    — CORRECTION OF ANY SAFETY DEFICIENCY ON PREVIOUS MISSIONS
    — SAFETY IMPACT OF ANY CHANGES TO HARDWARE OR PROCEDURES
    — MAINTENANCE AND/OR REFURBISHMENT AFFECTING SAFETY
    — APPROPRIATE DESIGN AND VERIFICATION FEATURES FOR REUSE
    — SAFETY OF REUSE IN VIEW OF WEAROUT OR SUBTLE DEGRADATION (INCLUDING FATIGUE) IN PREVIOUS USE
    — ANY LIMITED-LIFE ITEMS THAT MAY AFFECT SAFETY

• EXTRAVEHICULAR ACTIVITY (217)
  • PAYLOADS THAT PLAN EXTRAVEHICULAR ACTIVITY (EVA) SHALL COMPLY WITH DESIGN REQUIREMENTS OF JSC 10615
INGESTION OF FLUIDS

ATMOSPHERES, WHICH MAY RESULT FROM LEAKAGE OR
NOT CAUSE INGESTION OF A FLAMMABLE PAYLOAD BAY
OR CONTINGENCY (NORMAL PAYLOAD FUNCTIONAL SHALT
DURING ENTRY, LANDING, OR POST-LANDING (PLANNED

FLAMMABLE ATMOSPHERES) (219)

— ANY LIMITED-LIFE ITEMS THAT AFFECT SAFETY
PREVIOUS MISSIONS
— CORRECTION OF ANY SAFETY DEFICIENCIES ON
MODIFICATION OF HARDWARE OR PROCEDURES
— SAFETY IMPACT OF ALL CHANGES INCLUDING
SERIES PAYLOADS SHALL BE REVIEWED FOR

SERIES PAYLOADS (218)

TECHNICAL REQUIREMENTS

SAFETY POLICY AND REQUIREMENTS

DESIGN AND DEVELOPMENT
BASIC APPROACH

- Establish failure tolerance for hazardous events and functions by independent inhibits/devices to protect against occurrence
  - One-failure tolerance for critical hazards
  - Two-failure tolerance for catastrophic hazards

- For catastrophic hazards establish monitoring to assure knowledge of single-failure tolerance to permit corrective action

- For catastrophic hazards, such as structural failure, fire, or toxicity, establish design criteria and margin requirements that preclude their occurrence

- Design to minimize NASA participation in the payload development process and still provide confidence in the safety of flight
LIMITATIONS

- REQUIREMENTS ARE BASED ON NASA EXPERIENCE WITH CURRENT SPACE DESIGN TECHNOLOGY AND TYPICAL SYSTEMS/SUBSYSTEMS

- SAFETY ANALYSIS BY THE PAYLOAD DEVELOPER IS REQUIRED TO IDENTIFY AND CONTROL HAZARDS IN ANY SPECIFIC PAYLOAD