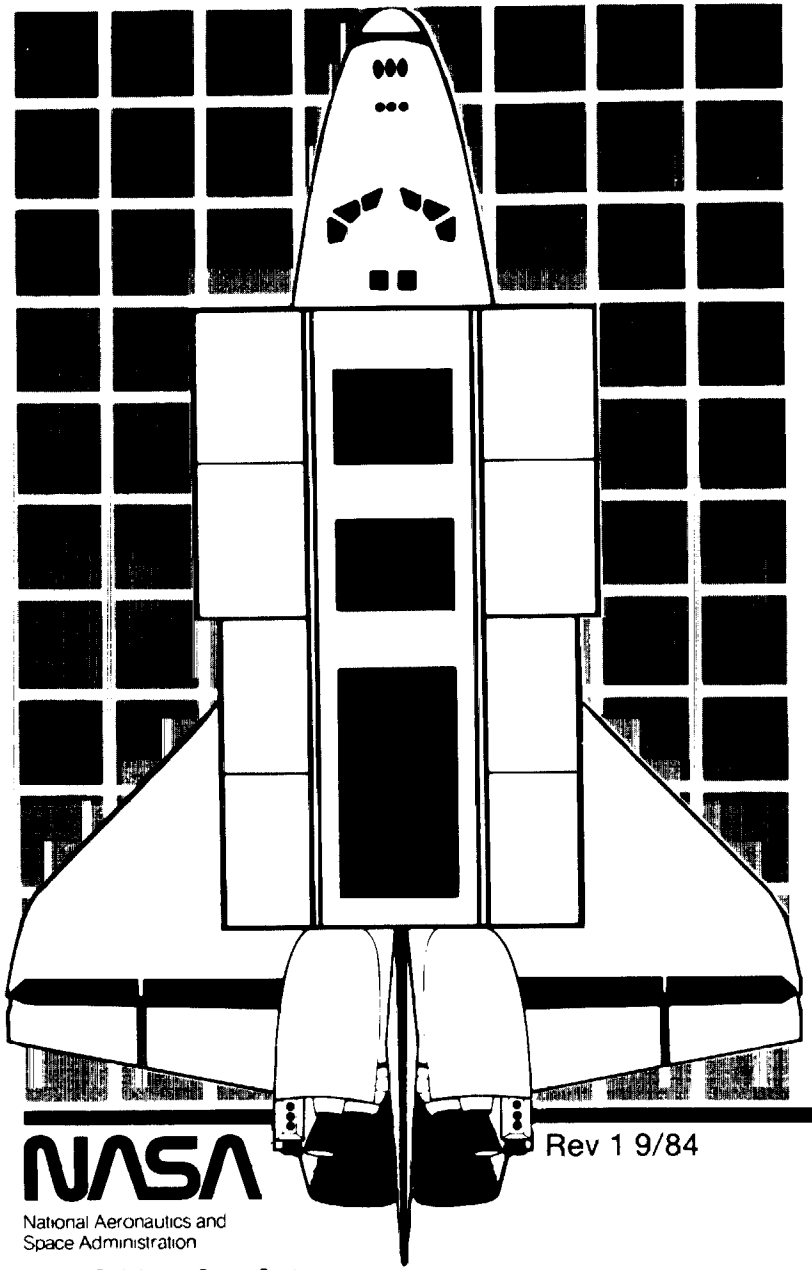
NASA-TM-108231



SPACE SHUTTLE PAYLOAD

DESIGN AND DEVELOPMENT

JSC-20052
VOLUME 7

NASA
7N-16-TM
167303
D_56

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

N94-70371

Unclas

Z9/16 0167303

SAFETY GUIDELINES AND REQUIREMENTS

Rev 1 9/84

NASA
National Aeronautics and Space Administration
Lyndon B. Johnson Space Center

CONTENTS

S-84-04485

SECTION PAGE

SAFETY PROCESS OVERVIEW 4
STS REQUIREMENTS AND RESPONSIBILITIES 5
SAFETY REVIEW PANELS 9
SAFETY PROCESS 10
TECHNICAL REQUIREMENTS SUMMARY 20
CUSTOMER-ORIENTED FEATURES 24
NHB 1700.7A 26
DETAILED TECHNICAL REQUIREMENTS 27

PRECEDING PAGE BLANK NOT FILMED

SECTION I

STS PAYLOAD SAFETY REVIEW PROCESS

STS REQUIREMENTS

S-84-01862

- NHB 1700.7A, *"SAFETY POLICY AND REQUIREMENTS FOR PAYLOADS USING THE SPACE TRANSPORTATION SYSTEM (STS)"*
  - TECHNICAL REQUIREMENTS
  - SYSTEM SAFETY REQUIREMENTS
  - REFERENCE DOCUMENTATION
    - — JSC 13830A, *"IMPLEMENTATION PROCEDURE FOR STS PAYLOADS SYSTEM SAFETY REQUIREMENTS"*
    - — JSC 11123, *"STS PAYLOAD SAFETY GUIDELINES HANDBOOK"*
    - — JSC 18798, *"INTERPRETATIONS OF STS PAYLOAD SAFETY REQUIREMENTS"*
    - — SAMTO HB S-100/KHB 1700.7, *"SPACE TRANSPORTATION SYSTEM PAYLOAD GROUND SAFETY HANDBOOK"*

RESPONSIBILITY*

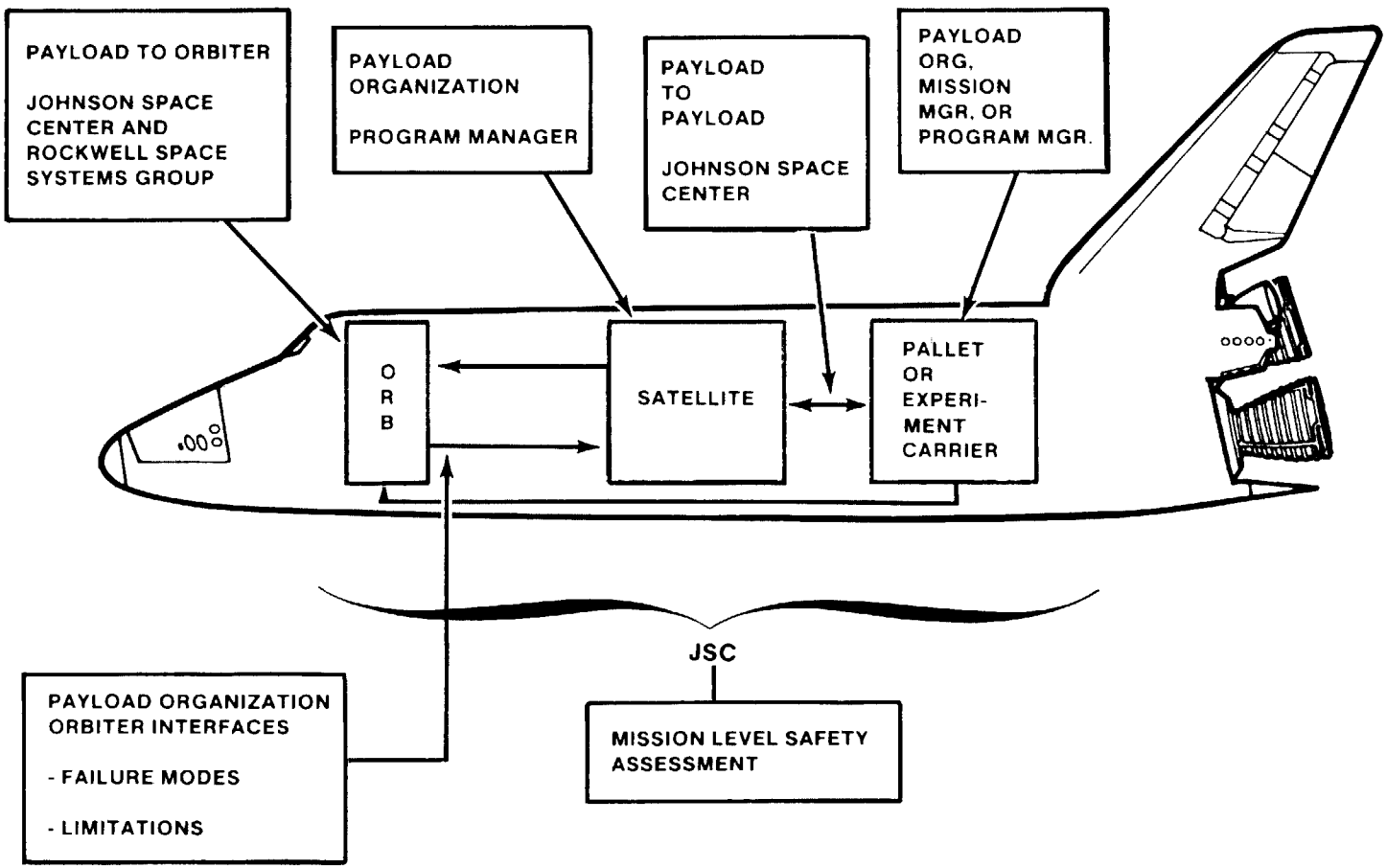
S-84-01859

- 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)

INTEGRATED SAFETY PROGRAM RESPONSIBILITY

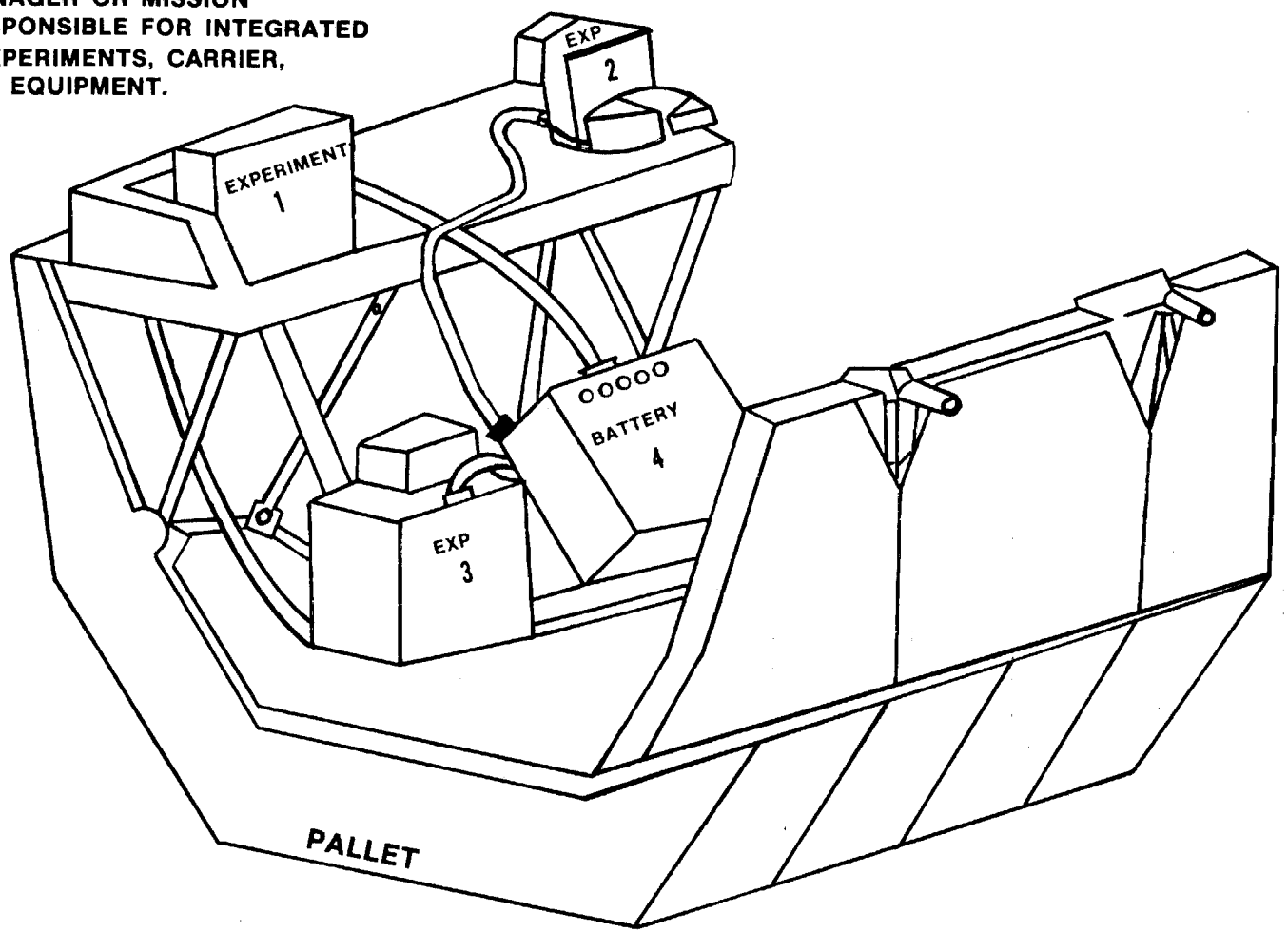
NASA-S-84-01046



NASA-S-84-01032

SAFETY RESPONSIBILITY
SEVERAL EXPERIMENTS ON THE SAME PALLET

PROGRAM MANAGER OR MISSION MANAGER RESPONSIBLE FOR INTEGRATED PAYLOAD — EXPERIMENTS, CARRIER, AND SUPPORT EQUIPMENT.



STS PAYLOAD SAFETY REVIEW PANELS

S-84-01868

- JSC — PAYLOAD DESIGN AND FLIGHT OPERATIONS
  - CHAIRMAN — FROM JSC PAYLOAD INTEGRATION OFFICE
  - MEMBERS FROM THE FOLLOWING TECHNICAL AND OPERATIONAL DISCIPLINES
    - — ORBITER INTEGRATION
    - — OPERATIONS
    - — SAFETY
    - — ENGINEERING
    - — GROUND OPERATIONS
    - — LIFE SCIENCES
- KSC — GROUND SUPPORT EQUIPMENT DESIGN AND GROUND PROCESSING
  - CHAIRMAN — FROM KSC SYSTEMS ENGINEERING OFFICE
  - MEMBERS FROM THE FOLLOWING TECHNICAL AND OPERATIONAL DISCIPLINES
    - — GROUND PROCESSING
    - — FUEL/CRYO HANDLING
    - — BIOMEDICAL
    - — RANGE SAFETY
    - — CARGO INSTALLATION
    - — GROUND SUPPORT EQUIPMENT

SAFETY PROCESS

S-84-01857

- INITIAL CONTACT
- PHASED SAFETY REVIEWS
  - PHASE O, I, II, III
  - KEYED TO PAYLOAD DEVELOPMENT
    — CONCEPT, PRELIMINARY DESIGN REVIEW (PDR), CRITICAL DESIGN REVIEW (CDR), COMPLETION
- PAYLOAD SAFETY CERTIFICATION
  - SAFETY COMPLIANCE DATA
  - APPROVAL FOR LOADING INTO THE STS
  - APPROVAL FOR FLIGHT

INITIAL CONTACT MEETING WITH PAYLOAD ORGANIZATION

S-84-01823

- CONCURRENT WITH INITIAL PAYLOAD INTEGRATION PLAN (PIP) MEETING
- PROVIDE SAFETY DOCUMENTS
- BRIEFING ON IMPLEMENTATION PROCEDURE AND SAFETY REVIEWS
- SCHEDULE PHASE O SAFETY REVIEW

SAFETY REVIEWS

S-84-04471
Rev 1

- 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

HAZARD CONTROL PROCEDURE

S-84-02039

DESIGN CONCEPT	PDR	CDR	DELIVERY
PHASE O REVIEW	PHASE I REVIEW	PHASE II REVIEW	PHASE III REVIEW
IDENTIFY HAZARDS	DEFINE CONTROLS	VERIFY DESIGN IMPLEMENTS CONTROLS	VERIFY HARDWARE IMPLEMENTS CONTROLS

PHASE O SAFETY REVIEW
(JSC 13830A PARAGRAPH 5.2)

S-84-01815

- 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 O HAZARD REPORTS
- PHASE O SAFETY REVIEW MEETING
  - DESCRIPTION OF SAFETY CRITICAL SUBSYSTEMS
  - APPLICABLE SAFETY REQUIREMENTS
  - PHASE O HAZARD REPORTS
  - DATA REQUIREMENTS FOR THE PHASE I SAFETY REVIEW
  - BRIEFING ON LAUNCH AND LANDING SITE SAFETY

PHASE I SAFETY REVIEW
(JSC 13830A PARAGRAPH 5.3)

S-84-01814

- DATA REQUIREMENTS
  - UPDATE AS REQUIRED
    - PAYLOAD DESCRIPTION AND MISSION SCENARIO
    - DESCRIPTION OF SAFETY-CRITICAL SUBSYSTEMS INCLUDING OPERATIONS
    - HAZARD REPORTS
  - NEW DATA REQUIRED
    - IONIZING RADIATION SOURCE DATA SHEETS (JSC FORM 44)
    - DESCRIPTION OF GSE AND GROUND OPERATIONS
- PHASE I SAFETY REVIEW MEETING
  - OVERVIEW OF PAYLOAD INCLUDING MISSION SCENARIO AND GSE/GROUND OPERATIONS
  - ASSESSMENT OF APPLICABLE REQUIREMENTS
  - REVIEW AND DISPOSITION OF PHASE I HAZARD REPORTS

PHASE II SAFETY REVIEW

S-84-01816

(JSC 13830A PARAGRAPH 5.4)

- 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

PHASE III SAFETY REVIEW
(JSC 13830A PARAGRAPH 5.5)

S-84-01817

- DATA REQUIREMENTS (SAFETY COMPLIANCE DATA PACKAGE)
  - UPDATE AS REQUIRED
    - PAYLOAD DESCRIPTION AND MISSION SCENARIO
    - DESCRIPTIONS OF SAFETY-CRITICAL SUBSYSTEMS AND OPERATIONS INCLUDING GSE AND GROUND OPERATIONS
    - HAZARD REPORTS TO REFLECT VERIFICATION ACTIVITIES
  - NEW DATA REQUIREMENTS
    - SUMMARY OF SAFETY-RELATED FAILURES OR ACCIDENTS
    - LISTING OF OPEN SAFETY ITEMS
    - APPROVED WAIVERS/DEVIATIONS*
    - PRESSURE VESSEL LOGBOOK
    - LISTING OF PYROTECHNICS
- PHASE III SAFETY REVIEW MEETING
  - STATUS OF OPEN ACTION ITEMS
  - REVIEW AND DISPOSITION OF SAFETY COMPLIANCE DATA

*SEE JSC 13830A PARA. 6.0, PAYLOAD SAFETY NONCOMPLIANCE REPORT

SPACE TRANSPORTATION SYSTEM
CERTIFICATE OF PAYLOAD SAFETY COMPLIANCE

FOR

_____

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 PAYLOAD MANAGER — DATE

SAFETY REVIEWS

S-84-02033

- NUMBER AND DEPTH OF REVIEWS MAY BE TAILORED
  - COMBINED PHASES
    - — DESIGN MATURITY
    - — COMPLEXITY
    - — STS PAYLOAD EXPERIENCE
  - TELECON REVIEW
    - — LOW HAZARD POTENTIAL
    - — SIMPLE DESIGN
    - — MINIMUM INTERFACES
  - NO FORMAL REVIEW
    - — STANDARD ELEMENTS (SERIES AND REFLOWN PAYLOADS)
      - ZERO OR MINIMAL CHANGES
    - — CERTIFICATION OF BASELINE

TECHNICAL REQUIREMENTS SUMMARY

S-84-02034

- 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

TECHNICAL REQUIREMENTS SUMMARY (CONT)

S-84-02032

- CATASTROPHIC HAZARDS (CONT)
  - THE FOLLOWING ARE CLASSIFIED AS CATASTROPHIC HAZARDS
    - PREMATURE FIRING OF SOLID ROCKET MOTOR
      - SAFE AND ARM IN SAFE FOR BOOST AND ENTRY
      - 45-MINUTE COAST PRIOR TO IGNITION
    - PREMATURE FIRING OR ADIABATIC DETONATION OF LIQUID PROPELLANT PROPULSION SYSTEM
      - THREE INDEPENDENT FLOW CONTROL DEVICES
      - 200 FEET SEPARATION FOR $<$ 10 LB THRUST
    - PREMATURE SEPARATION OR DEPLOYMENT SO THAT PAYLOAD CANNOT WITHSTAND LANDING ENVIRONMENT
    - DEPLOYMENT/EXTENSION PREVENTING PAYLOAD BAY DOOR CLOSURE
    - RF ENERGY RADIATION ABOVE ICD LEVELS AT ORBITER ENVELOPE

TECHNICAL REQUIREMENTS SUMMARY (CONT)

S-84-02036

- 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

TECHNICAL REQUIREMENTS SUMMARY (CONT)

S-84-02031

- STRUCTURAL (CONT)
  - MATERIAL SELECTION TO PREVENT STRESS CORROSION IN ACCORDANCE WITH MSFC-SPEC-522
  - PRESSURE VESSELS
    - ASME BOILER CODE
    - MIL-STD-1522
    - NSS/HP 1740.1 WITH FACTOR OF SAFETY (F.O.S.) 1.5
    - QUAL TEST TO DESIGN BURST
    - SEALED CONTAINER PROOF TESTED TO F.O.S. OF 1.5 IF HAZARDOUS
- MATERIALS
  - DESIGN TO CONTAIN EFFLUENTS
  - SINGLE BARRIER FAILURE SHOULD NOT CAUSE HAZARDOUS REACTION FOR SYSTEMS CONTAINING HAZARDOUS MATERIALS
  - MINIMIZE USE OF MERCURY
  - ORBITER CABIN USAGE MUST MEET NHB 8060.1B
  - GOOD DESIGN PRACTICE IN PAYLOAD BAY FOR FLAMMABILITY CONTROL
  - OFFGASSING TESTS FOR COMPONENTS IN ORBITER CABIN

FEATURES OF SAFETY PROCESS

S-84-01804

- 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)

HELP AVAILABLE TO CUSTOMER

S-84-01841

- SAFETY ENGINEER SUPPORT
  - SINGLE POINT OF CONTACT FOR SAFETY
  - PRE-REVIEW CONSULTATION
  - ISSUE/QUESTION DISCUSSION
  - COORDINATE DETAILED TECHNICAL ASSISTANCE ON SPECIFIC ISSUES
- SAFETY PANEL INTERPRETATIONS OF POLICY/ REQUIREMENTS
  - JSC 18798, "INTERPRETATIONS OF STS PAYLOAD SAFETY REQUIREMENTS"
  - SPECIAL ISSUE/QUESTION DISPOSITION AS REQUIRED

SECTION 2

NHB 1700.7A

TECHNICAL REQUIREMENTS

S-84-01874

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS (NHB 1700.7A)

- GENERAL (200)
  - THESE REQUIREMENTS APPLY TO ALL PAYLOADS THAT ARE FLOWN ON THE STS
  - THESE REQUIREMENTS APPLY UNDER WORST CASE NATURAL AND INDUCED ENVIRONMENTS OF THE STS MISSION INCLUDING ABORT AND EMERGENCY LANDING
  - PAYLOADS PLANNED TO BE DEPLOYED MUST BE COMPATIBLE WITH CONTINGENCY ABORT AND EMERGENCY LANDING CONDITIONS
  - NONCOMPLIANCE TO THESE REQUIREMENTS REQUIRES APPROVAL, BY THE STS, OF A DEVIATION OR WAIVER

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

S-84-01864

- **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

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

S-84-01876

- CONTROL OF HAZARDOUS FUNCTIONS (202)
  - FUNCTIONS RESULTING IN CRITICAL HAZARDS
    - — *TWO INDEPENDENT* INHIBITS
    - — MONITOR AND RETURN TO SAFE CONDITION ON A CASE-BY-CASE BASIS
    - — FLIGHT OR GROUND CREW MONITOR IN NEAR-REAL TIME, WHEN REQUIRED
    - — NO MONITORING IF POWER AND CONTROL CIRCUITS ARE CONNECTED TO *UNPOWERED* BUS

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

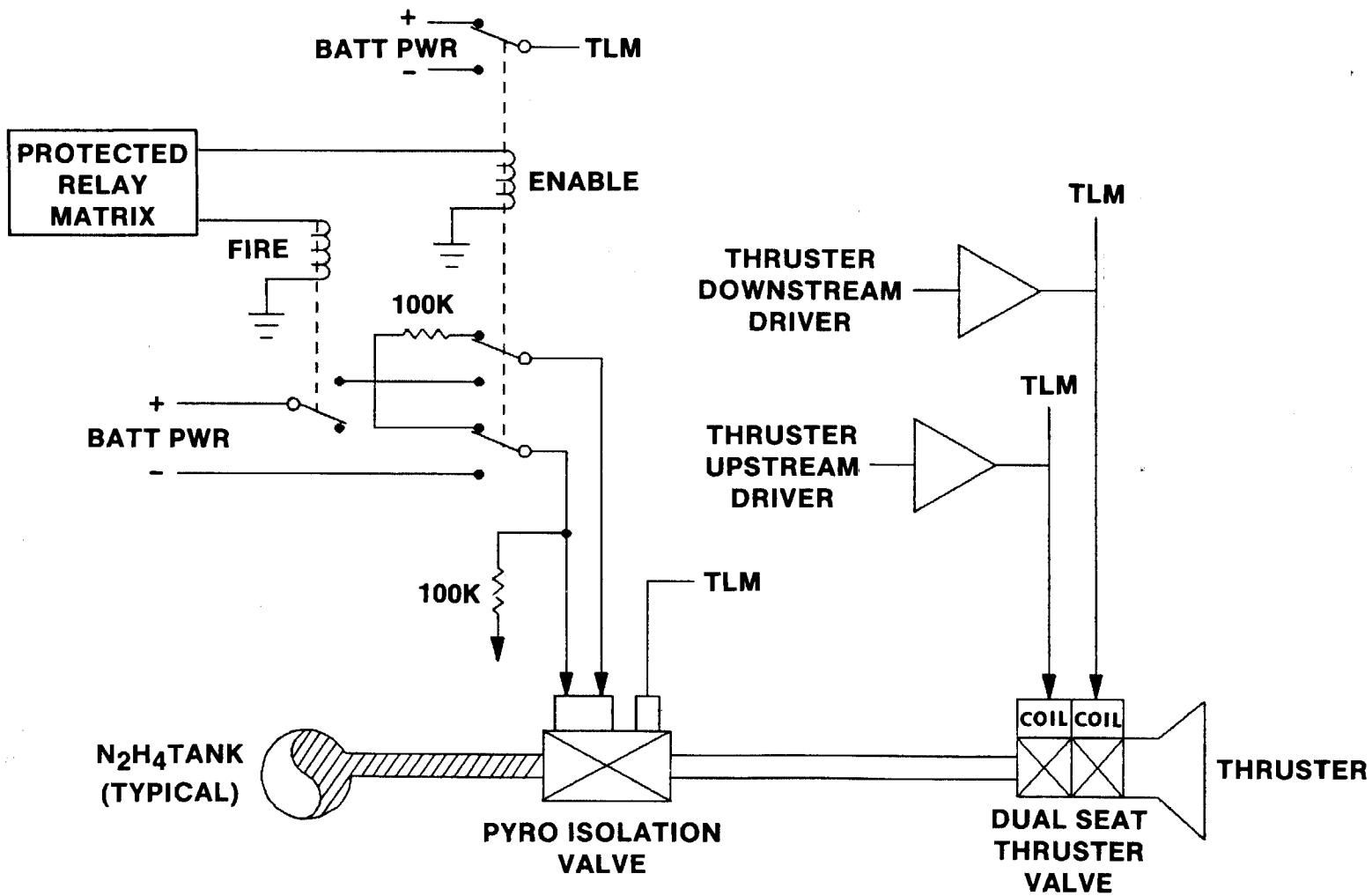
S-84-01877

- 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)

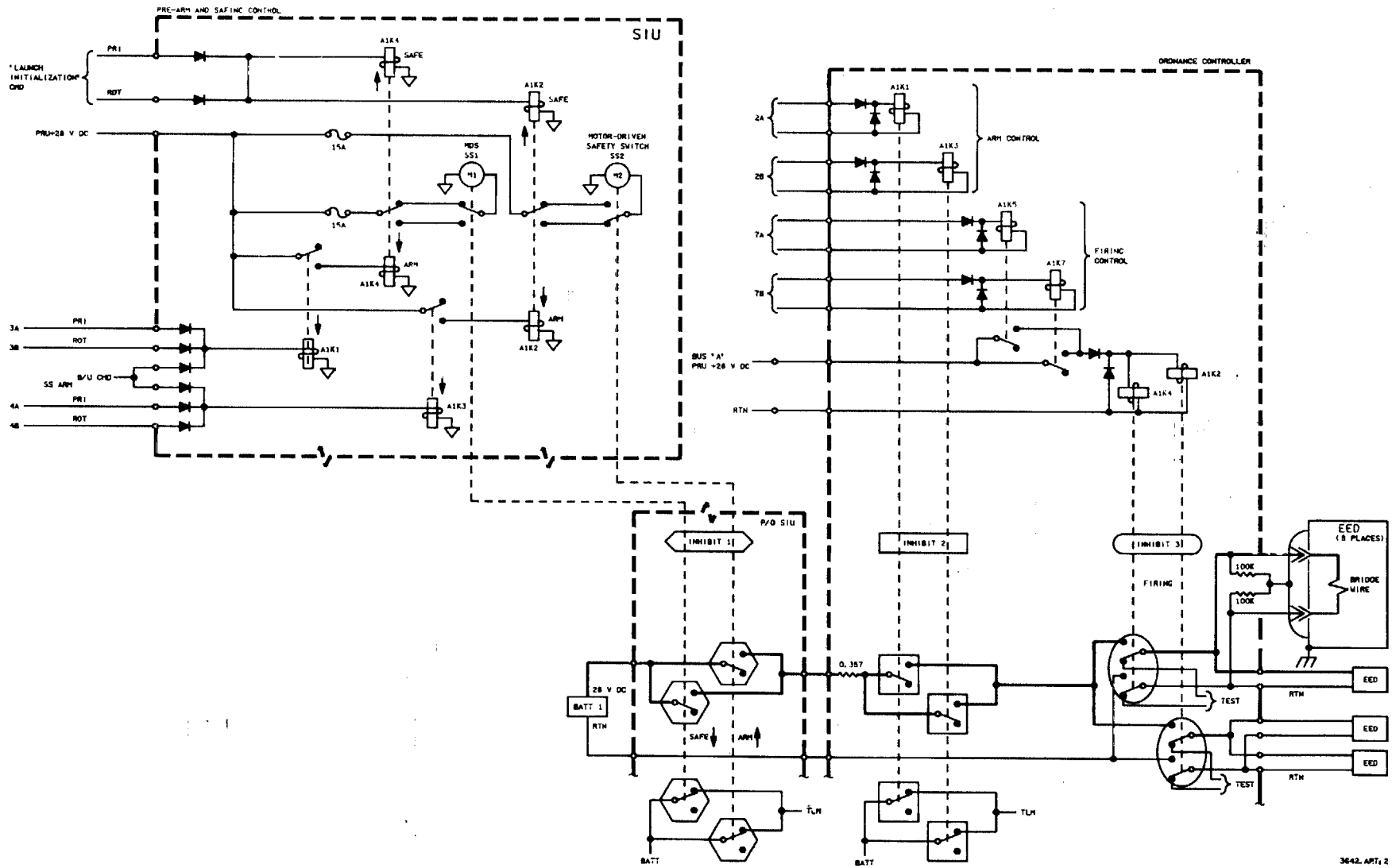
REACTION CONTROL SYSTEM INHIBITS-CONTROLS-MONITORS

S-84-01867



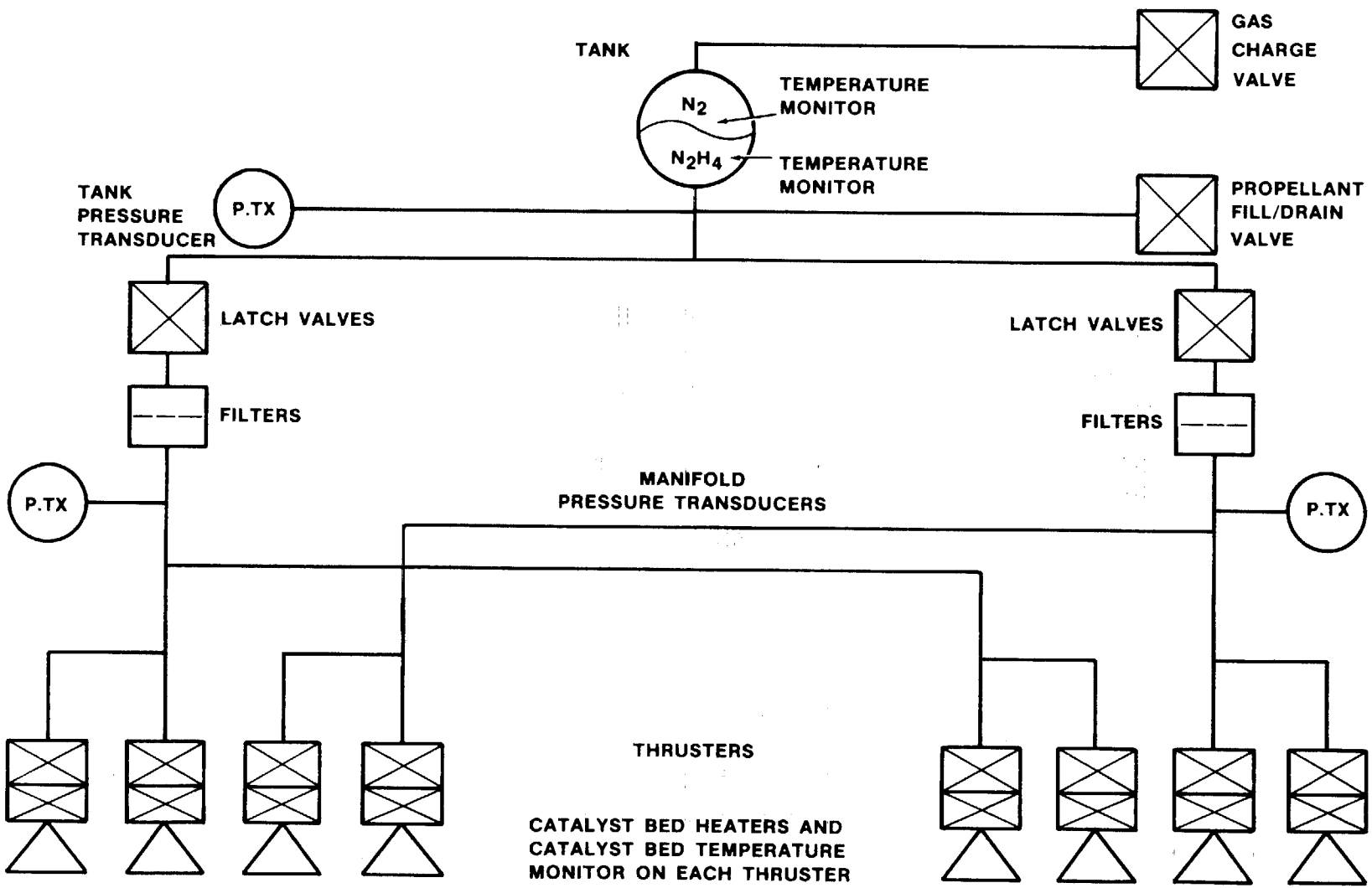
INHIBITS—CONTROLS—MONITORS ELECTRICAL SYSTEM

S-84-01656



LIQUID THRUSTER SYSTEMS

S-84-01400



S-84-01878

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

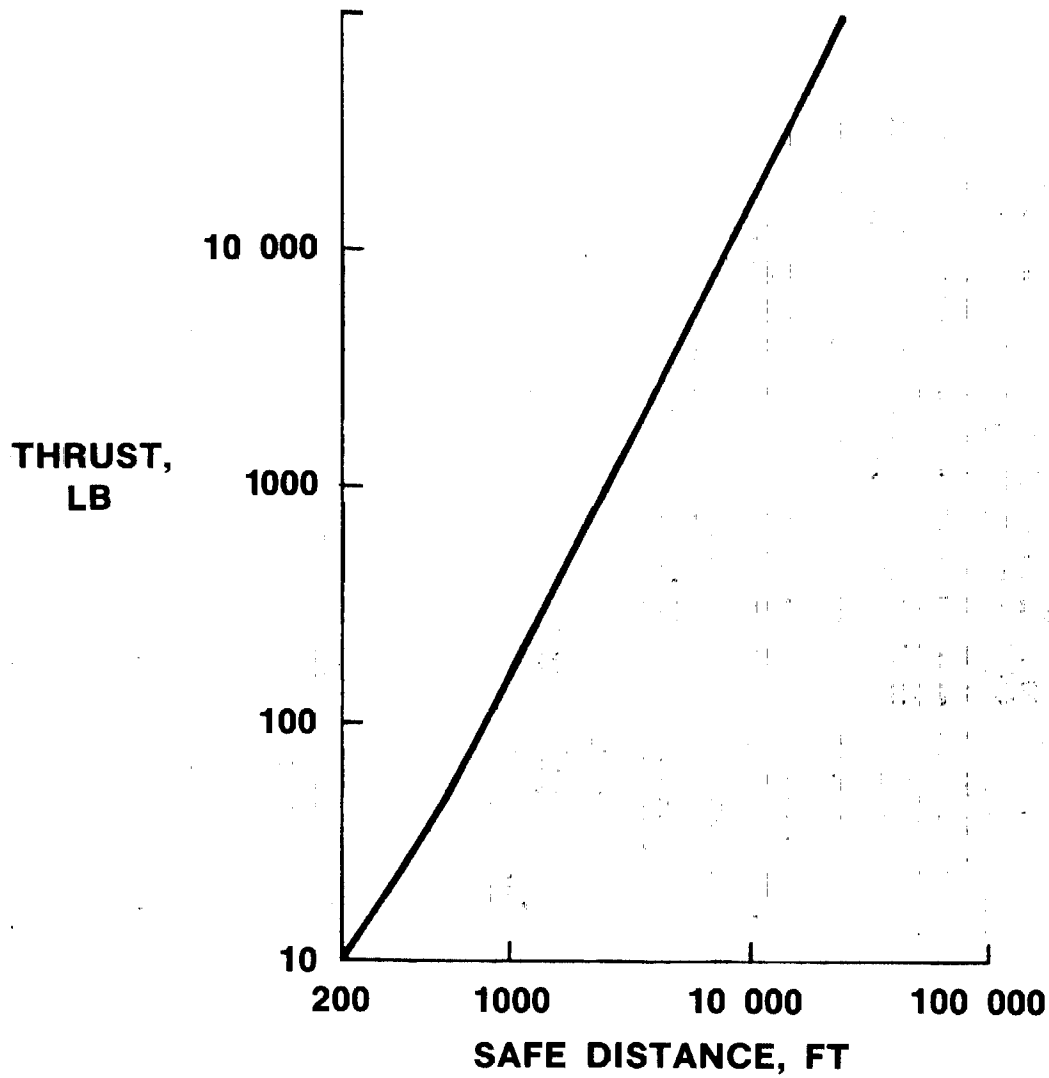
S-84-01879

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- LIQUID PROPELLANT PROPULSION SYSTEMS
  - PREMATURE FIRING OR ADIABATIC DETONATION IS A CATASTROPHIC HAZARD
  - MINIMUM OF THREE MECHANICALLY INDEPENDENT FLOW CONTROL DEVICES (INHIBITS) IN SERIES, WHICH REMAIN CLOSED UNTIL PAYLOAD REACHES SAFE DISTANCE
  - FLOW CONTROL DEVICE TO ISOLATE TANK(S) FROM DISTRIBUTION SYSTEM — MAY BE OPENED UNDER CERTAIN PROVISIONS
  - MINIMUM OF ONE FLOW CONTROL DEVICE "FAIL SAFE"
  - OPENING OF ANY FLOW CONTROL DEVICE SHALL NOT RESULT IN ADIABATIC DETONATION
  - SAFE DISTANCE IS 200 FT FOR THRUST LESS THAN OR EQUAL TO 10 POUNDS
  - SAFE DISTANCE FOR GREATER THAN 10 POUNDS THRUST DEFINED IN NASA LETTER NS 2/83-L167 DATED JUNE 10, 1983 (SEE FOLLOWING PAGE)
  - FOR BIPROPELLANT SYSTEM DEVICES MUST PREVENT PROPELLANT MIXING OR EXPULSION THROUGH THRUST CHAMBERS

SAFE DISTANCE FOR FIRING LIQUID PROPULSION ENGINES

S-84-02043



S-84-01880

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS

- LIQUID PROPELLANT PROPULSION SYSTEMS (CONT)
  - ELECTRICAL CONTROLS, MONITORING, AND SAFING REQUIREMENTS ARE A FUNCTION OF PLANNED OPERATIONS
    - — ISOLATION VALVE NOT OPENED UNTIL PAYLOAD REACHES SAFE DISTANCE
      - MINIMUM THREE INDEPENDENT ELECTRICAL CONTROLS TO FIRING ENGINE
      - FLIGHT OR GROUND CREW MONITORING OF MINIMUM OF TWO OF THREE ELECTRICAL CONTROLS IN NEAR REAL TIME
      - ONE MONITOR MUST BE ISOLATION VALVE CONTROL
    - — ISOLATION VALVE OPENED PRIOR TO PAYLOAD REACHING SAFE DISTANCE
      - MINIMUM THREE INDEPENDENT ELECTRICAL CONTROLS TO FIRING ENGINE UNTIL PAYLOAD REACHES SAFE DISTANCE
      - ISOLATION VALVE CLOSED DURING BOOST AND ENTRY, OPENED ONLY BY FLIGHT CREW COMMAND FOR DEPLOYMENT
      - TWO OF THREE REMAINING ELECTRICAL CONTROLS VERIFIED SAFE PRIOR TO ISOLATION VALVE OPENING
      - CONTINUOUS REAL-TIME MONITORING OF TWO ELECTRICAL CONTROLS BY FLIGHT OR GROUND CREW
      - SINGLE FAILURE-TOLERANT DEPLOYMENT CAPABILITY REQUIRED IF SYSTEM CANNOT BE SAFED BY CREW COMMAND

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS

- DEPLOYMENT AND/OR SEPARATION
  - PREMATURE DEPLOYMENT OR SEPARATION TO CONDITION IN WHICH PAYLOADS CANNOT WITHSTAND STS-INDUCED 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

S-84-01882

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- DEPLOYMENT/EXTENSION PREVENTING PAYLOAD BAY DOOR CLOSURE
  - HAZARD CONTROLLED BY INDEPENDENT PRIMARY AND BACKUP METHOD
  - COMBINATION MUST BE TWO-FAILURE TOLERANT
- RF ENERGY RADIATION
  - CARGO RADIATION IN EXCESS OF "DOORS OPEN" LEVELS IN VOLUME XIV, ATTACHMENT 1, IS CATASTROPHIC
  - THREE INDEPENDENT INHIBITS TO RADIATION
  - NO COMMAND AND MONITORING REQUIREMENTS FOR THESE INHIBITS

S-84-01883

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- 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"

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- **FAILURE PROPAGATION (206)**
  - DESIGN SHALL PRECLUDE PROPAGATION OF FAILURES FROM THE PAYLOAD TO THE ENVIRONMENT OUTSIDE THE PAYLOAD
- **REDUNDANCY SEPARATION (207)**
  - SAFETY-CRITICAL REDUNDANT SUBSYSTEMS SHOULD BE ARRANGED SO THAT PROPAGATION OF FAILURE FROM ONE TO THE OTHER IS MINIMIZED

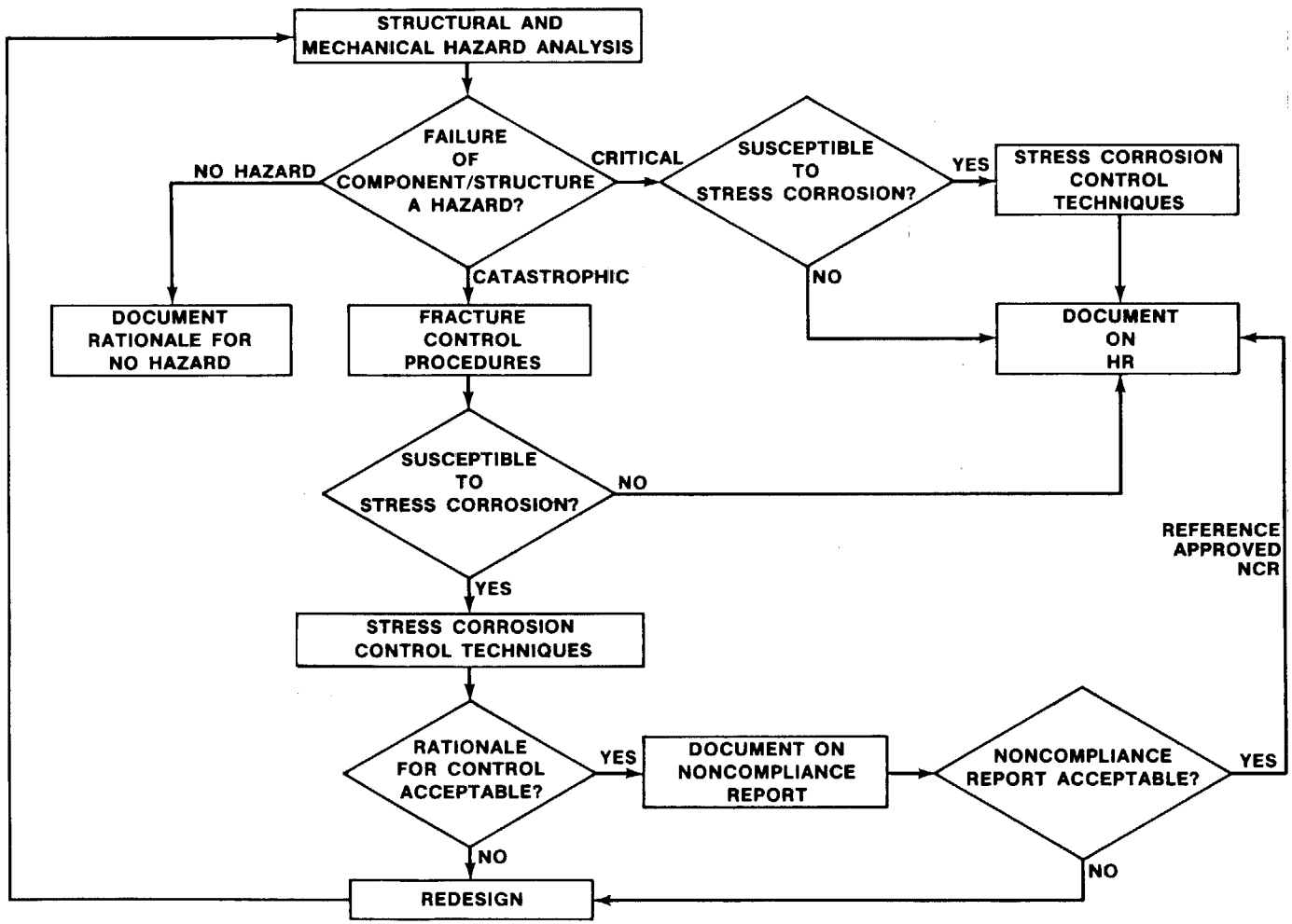
S-84-01885

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- 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

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

S-84-02040



SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

S-84-04470
Rev 1

- 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 $\geq$ 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

S-84-04045

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS (CONT)

- STRUCTURAL (208) (CONT)
  - PRESSURIZED LINES AND FITTINGS
    - FITTINGS AND LINES LESS THAN 1.5 INCHES INSIDE DIAMETER SHALL HAVE FACTOR OF SAFETY GREATER THAN OR EQUAL TO 4.0
    - FITTINGS AND LINES GREATER THAN 1.5 INCHES INSIDE DIAMETER SHALL HAVE FACTOR OF SAFETY GREATER THAN OR EQUAL TO 1.5
    - OTHER COMPONENTS SHALL HAVE FACTOR OF SAFETY GREATER THAN OR EQUAL TO 2.5

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- 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

S-84-02035

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- HAZARDOUS MATERIALS — GENERAL
  - SHALL NOT BE RELEASED OR EJECTED IN OR NEAR ORBITER
  - SYSTEMS MUST CONTAIN FLUIDS THROUGH ALL MISSION ENVIRONMENTS
    - — VENTING MAY BE NEGOTIATED WITH STS OPERATOR
  - MATERIALS USED IN HAZARDOUS FLUID SYSTEMS
    - — OXYGEN SYSTEMS
      - MATERIALS MUST MEET COMPATABILITY REQUIREMENTS OF NHB 8060.1B FOR TYPE D MATERIALS AT MAXIMUM PRESSURE AND TEMPERATURE
    - — OTHER HAZARDOUS FLUIDS SYSTEMS
      - MATERIALS MUST MEET COMPATABILITY REQUIREMENTS OF NHB 8060.1B FOR TYPE J MATERIALS AT MAXIMUM PRESSURE AND TEMPERATURE
    - — COMPATIBILITY IS REQUIRED FOR DIRECT OR SINGLE BARRIER FAILURE CONTACT OF FLUIDS
  - COMPATABILITY DATA BY PAYLOAD MAY BE USED IF APPROVED BY NASA
- HAZARDOUS MATERIALS — MERCURY
  - USE OF MERCURY SHALL BE MINIMIZED; WHEN USED, SPECIFIC DATA DOCUMENTED PRIOR TO NASA APPROVAL

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS

S-84-01865

- MATERIALS (209) (CONT)
  - ORBITER CABIN MATERIALS
    - — MUST MEET REQUIREMENTS FOR FLAMMABILITY, 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
        - MATERILAS 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

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

S-84-01866

- MATERIALS (209) (CONT)
  - MATERIAL OFFGASSING (CABIN MATERIALS ONLY)
    - — AVOID MATERIALS WITH TOXIC OFFGASSING IN HABITABLE AREAS
    - — OFFGASSING TESTS FOR SAFETY VALIDATION PRIOR TO STS INTEGRATION
    - — RIGOROUS MATERIAL SELECTION NEGOTIABLE ALTERNATIVE
    - — NHB 8060.1 OR STS OPERATOR-APPROVED EQUIVALENT TESTS

S-84-01889

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

S-84-01890

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS

- PYROTECHNICS (210) (CONT)
  - NEW PAYLOADS
    - — USE NSI INITIATORS OR STS-APPROVED ALTERNATIVE
  - ELECTRICAL CONNECTION OF PYRO DEVICES FOR GROUND PROCESSING
    - — IF PREMATURE FIRING IS HAZARDOUS TO PERSONNEL OR PROPERTY, DESIGN TO BE ELECTRICALLY CONNECTED AFTER INSTALLATION IN ORBITER AND ELECTRICAL INTERFACE VERIFICATION COMPLETED
    - — EXCEPTIONS REQUIRE SPECIFIC LAUNCH SITE SAFETY OFFICE APPROVAL
- DESTRUCT SYSTEMS (211)
  - USE ONLY WHEN APPROVED BY STS OPERATOR
  - MUST COMPLY WITH HAZARD CONTROL AND HAZARD DETECTION AND SAFING REQUIREMENTS

S-84-01860

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- 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

S-84-01806

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- **ELECTRICAL SYSTEMS (213)**
  - ELECTRICAL POWER DISTRIBUTION DESIGNED SO THAT FAULTS INTERNAL TO PAYLOAD DO NOT DAMAGE STS CIRCUITS
  - DESIGN SO THAT FAULTS DO NOT CREATE IGNITION SOURCES FOR PAYLOAD OR ORBITER MATERIAL
  - WHEN LIGHTNING PROTECTION REQUIRED FOR CATASTROPHIC HAZARD, USE JSC 07636 AS DESIGN GUIDE
- **VERIFICATION REQUIREMENTS (214)**
  - SAFETY ASPECTS OF HAZARDOUS PAYLOAD EQUIPMENT SHALL BE SATISFACTORILY VERIFIED
  - TEST, ANALYSES, AND INSPECTION ARE TECHNIQUES
  - METHODS DOCUMENTED IN SAFETY REVIEWS

S-84-01832

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

S-84-01891

SAFETY POLICY AND REQUIREMENTS
TECHNICAL REQUIREMENTS

- SERIES PAYLOADS (218)
  - SERIES PAYLOADS SHALL BE REVIEWED FOR
    - — SAFETY IMPACT OF ALL CHANGES INCLUDING MODIFICATION OF HARDWARE OR PROCEDURES
    - — CORRECTION OF ANY SAFETY DEFICIENCIES ON PREVIOUS MISSIONS
    - — ANY LIMITED-LIFE ITEMS THAT AFFECT SAFETY
- FLAMMABLE ATMOSPHERES (219)
  - DURING ENTRY, LANDING, OR POSTLANDING (PLANNED OR CONTINGENCY) NORMAL PAYLOAD FUNCTIONS SHALL NOT CAUSE IGNITION OF A FLAMMABLE PAYLOAD BAY ATMOSPHERE, WHICH MAY RESULT FROM LEAKAGE OR INGESTION OF FLUIDS

S-84-01892

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS SUMMARY

- 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

SAFETY POLICY AND REQUIREMENTS TECHNICAL REQUIREMENTS

S-84-01805

SUMMARY (CONT)

- **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**

* U.S. GOVERNMENT PRINTING OFFICE: 1984—789-013/7578