

SSP 50021

Safety Requirements Document

International Space Station Program

December 12, 1995

Incorporates DCN 001

**National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas 77058**



REVISION AND HISTORY PAGE

REV.	DESCRIPTION	PUB. DATE
-	Initial Release per SSCD 000353, EFF, 08-16-96 DCN 001 per SSCD 001778, EFF, 11-17-98	09-03-96 05-07-99

TABLE OF CONTENTS

1.0 INTRODUCTION	1-1
1.1 PURPOSE	1-2
1.2 SCOPE	1-2
1.2.1 GSE DESIGN AND GROUND OPERATIONS	1-2
1.2.2 MISSION RULES	1-2
1.3 PRECEDENCE	1-2
1.4 DELEGATION OF AUTHORITY	1-3
1.4.1 ISS	1-3
1.5 WAIVERS AND DEVIATIONS	1-3
2.0 APPLICABLE AND REFERENCE DOCUMENTS	2-4
2.1 APPLICABLE DOCUMENTS	2-4
2.2 REFERENCE DOCUMENTS	2-4
3.0 TECHNICAL REQUIREMENTS	3-9
3.1 SEGMENT SPECIFICATION AND PIDS SECTION 3.3.6 REQUIREMENTS	3-9
3.3.6 Safety	3-9
3.3.6.1 General	3-9
3.3.6.1.1 Catastrophic Hazards	3-9
3.3.6.1.2 Critical Hazards	3-9
3.3.6.1.3 Design for minimum risk	3-9
3.3.6.1.4 Control of functions resulting in critical hazards	3-10
3.3.6.1.5 Control of functions resulting in catastrophic hazards	3-10
3.3.6.1.6 Subsequent induced loads	3-11
3.3.6.1.7 Safety interlocks	3-11
3.3.6.1.8 Environmental compatibility	3-11
3.3.6.2 Hazard Detection and Safing	3-11
3.3.6.2.1 Reserved	3-11
3.3.6.2.2 Monitors	3-11
3.3.6.2.3 Near-real time monitoring	3-12
3.3.6.2.4 Real Time Monitoring	3-12
3.3.6.3 Command and computer control of hazardous functions	3-13
3.3.6.3.1 Computer control of hazardous functions	3-13
3.3.6.4 Hazardous Materials	3-13
3.3.6.4.1 Hazardous fluid containment failure tolerance	3-13
3.3.6.4.2 Storage of Hazardous Chemicals.	3-13
3.3.6.5 Pyrotechnics	3-13
3.3.6.5.1 Pyrotechnics for USOS application	3-13
3.3.6.6 Non-Ionizing Radiation	3-14
3.3.6.7 Optics and Lasers	3-14

3.3.6.7.1 Lasers	3-14	
3.3.6.7.2 Optical Requirements	3-14	
3.3.6.8 Electrical Safety	3-14	
3.3.6.8.1 Electrical power circuit overloads	3-14	
3.3.6.8.2 Crew protection for electrical shock	3-15	
3.3.6.8.3 Reapplication of power	3-15	
3.3.6.8.4 Batteries	3-15	
3.3.6.9 Liquid propellant propulsion system	3-15	
3.3.6.9.1 Inadvertent engine firings during ISS operations	3-15A	
3.3.6.9.2 Propellant overheating	3-15B	
3.3.6.9.3 Propellant leakage	3-15B	
3.3.6.9.4 Reserved	3-15B	
3.3.6.9.5 Plume impingement	3-15B	
3.3.6.9.6 Hazardous venting	3-15B	
3.3.6.9.7 Monitoring propulsion system status	3-15B	
3.3.6.9.8 <End Item> induced loads	3-16	DCN 001
3.3.6.10 Fire Protection	3-16	
3.3.6.11 Constraints	3-17	
3.3.6.11.1 Reserved	3-17	
3.3.6.11.2 Pressurized/Volume depressurization and repressurization tolerance	3-17	
3.3.6.11.3 Emergency egress	3-17	
3.3.6.11.4. Reserved	3-17	
3.3.6.11.5 Reserved	3-17	
3.3.6.11.6 Component hazardous energy provision	3-17	
3.3.6.11.7 Hatch opening	3-18	
3.3.6.11.8 Reserved	3-18	
3.3.6.11.9 Reserved	3-18	
3.3.6.11.10 Reserved	3-18	
3.3.6.11.11 Cryogenics	3-18	DCN 001
3.3.6.11.12 Hazardous Gas Accumulation	3-18	
3.3.6.11.13 Equipment clearance for entrapment hazard	3-19	
3.3.6.11.14 Frangible materials	3-19	
3.3.6.12 Human engineering safety	3-19	DCN 001
3.3.6.12.1 Internal volume touch temperature	3-19	
3.3.6.12.2 External touch temperature	3-20	DCN 001
3.3.6.12.3 External corner and edge protection	3-21	
3.3.6.12.4 Internal corner and edge protection	3-21	
3.3.6.12.5 Contingency repressurization	3-22	
3.3.6.12.6 Latches	3-22	
3.3.6.12.7 Screws and bolts	3-22	
3.3.6.12.8 Safety Critical Fasteners	3-22	
3.3.6.12.9 Levers, cranks, hooks and controls	3-22	
3.3.6.12.10 Burrs	3-22	
3.3.6.12.11 Holes	3-23	
3.3.6.12.12 Protrusions	3-23	
3.3.6.12.13 Pinch points	3-23	
3.3.6.12.14 Emergency Ingress	3-23	
3.3.6.12.15 Reserved	3-23	
3.3.6.12.17 Translation routes and established worksites	3-24	
3.3.6.12.18 Moving or rotating equipment	3-26	
3.3.6.13 Launch vehicle interfaces and services	3-26	
3.3.6.13.1 Safe Without Space Shuttle Program Services	3-26	
3.3.6.13.2 Critical Orbiter Services	3-26	
3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions	3-26	
3.3.6.13.4 Planned Deployment/Extension Functions	3-27	

3.3.6.13.5 Contingency Return and Rapid Safing	3-27
3.3.6.13.6 Flammable Atmosphere	3-27
3.3.6.13.7 Allowable RF radiation levels	3-28
3.3.6.13.8 Lightning protection	3-28
3.3.6.13.9 Orbiter vent/dump provisions	3-28
3.3.6.13.10 Sealed Compartments	3-29
3.3.6.14 Ground interfaces and services - Space Shuttle launch	3-29
3.2 ALL OTHER SECTIONS SAFETY REQUIREMENTS	3-30
3.2.1 Redundancy	3-30
3.2.1.1 Failure propagation	3-30
3.2.1.2 Separation of redundant paths	3-30
3.2.1.3 Failure tolerance	3-30
3.2.2 Characteristics	3-30
3.2.2.1 Performance Characteristics	3-30
3.2.2.2 Monitor total pressure	3-30
3.2.2.3 Introduce nitrogen	3-31
3.2.2.3.1	3-31
3.2.2.3.2	3-31
3.2.2.3.3	3-31
3.2.2.3.4	3-31
3.2.2.3.5	3-31
3.2.2.4 Introduce oxygen	3-32
3.2.2.4.1	3-32
3.2.2.4.2	3-32
3.2.2.4.3	3-32
3.2.2.5 Relieve overpressure	3-32
3.2.2.5.1	3-32
3.2.2.6 Equalize pressure	3-33
3.2.2.6.1	3-33
3.2.2.7 Verifiable seal leakage paths	3-33
3.2.2.8 Non-verifiable seal leakage paths	3-34
3.2.2.9 Capability: Support station ingress	3-34
3.2.2.10 Depressurization and Repressurization for EVA	3-35
3.2.2.10.1 Provide repressurization for ingress	3-35
3.2.2.10.2 Support station ingress	3-35
3.2.2.10.3 Support station egress	3-35
3.2.2.10.4 Provide depressurization for egress	3-35
3.2.2.11 Monitor Oxygen partial pressure	3-35
3.2.2.12 Monitor atmosphere temperature	3-36
3.2.2.13 Detect hazardous atmosphere	3-36
3.2.2.14 Recover from hazardous atmosphere	3-36
3.2.2.15	3-36
3.2.2.16 Monitor carbon dioxide	3-36
3.2.2.17 Remove gaseous contaminants	3-37
3.2.2.18 Remove airborne microbes	3-43
3.2.2.19 Monitor airborne microbes	3-43
3.2.2.20 Mode: Assured safe crew return	3-43
3.2.3 Caution and Warning	3-43
3.2.3.1 Annunciate alarms	3-43
3.2.4 Fault Detection Isolation and Recovery	3-44
3.2.4.1 Reserved	3-44
3.2.4.2 Isolate to the recovery level	3-44
3.2.4.3 Isolate hazard	3-44
3.2.4.4 Assess functional data	3-44

3.2.4.5	Manual FDIR	3-44
3.2.4.6	Manual control of FDIR	3-45
3.2.4.7	Collect function status data	3-45
3.2.4.8		3-45
3.2.4.9	Condition function status data	3-45
3.2.5	Lighting	3-45
3.2.5.1	Illuminate general area	3-45
3.2.5.2	Illuminate emergency egress area	3-46
3.2.5.3	Control emergency egress lighting	3-46
3.2.6	Noise	3-46
3.2.6.1	Acoustic emission limits	3-46
3.2.7	Radiation	3-46
3.2.7.1	Ionizing radiation crew limits	3-46
3.2.7.2	Ionizing radiation emission limits	3-46
3.2.7.3	Support radiation exposure monitoring	3-47
3.2.7.4	Reserved	3-47
3.2.7.5	Meteoroids and orbital debris (M/OD)	3-47
3.2.7.6	Probability of no penetration	3-47
3.2.7.7		3-47
3.2.7.8	Environmental conditions	3-48
3.2.7.9	Electromagnetic Radiation	3-48
3.2.7.10	EMC	3-48
3.2.7.11	EMI	3-48
3.2.7.12	Electrical Grounding	3-48
3.2.7.13	Electrical Bonding	3-48
3.2.7.14	Plasma	3-48
3.2.7.15	Ionizing radiation	3-48
3.2.7.16	Electrostatic Discharge (ESD)	3-48
3.2.7.17	Corona	3-49
3.2.7.18	Cable and wire design	3-49
3.2.8	Respond to Fire	3-49
3.2.9	Materials	3-53
3.2.9.1	Materials and processes	3-53
3.2.9.2	Fluid leakage	3-53
3.2.9.3	Used for hazardous fluids	3-53
3.2.10	Structures	3-53
3.2.10.1	Structural design requirements	3-53
3.2.10.2	EVA on-orbit induced loads	3-53
3.2.10.3	Margin(s) of Safety	3-56
3.2.10.4	End-of-life decommissioning and disposal	3-56
3.2.10.5	Negative Differential Pressure	3-56
3.2.10.6	IVA crew load requirements	3-56
3.2.10.7	External limit loads	3-56
3.2.10.8	IVA Induced Loads	3-58
3.2.10.9	Fracture Control	3-58
3.2.10.10	Glass, window, and ceramic design criteria	3-58
3.2.10.11	Pressure systems and pressure vessels	3-58
3.2.10.12	Bolts	3-58
3.2.10.13	Materials selection	3-58
3.2.10.14	Nonstandard fasteners	3-58
3.2.10.15	Fail-Safe or Safe-Life	3-58
3.2.10.16	Thermal Effects	3-59
3.2.10.17	Shuttle Payload Configuration Design Loads	3-60
3.2.10.17.1	Re-distributed Loads	3-60
3.2.10.17.2	Factors of Safety - Test verified structure	3-60

3.2.10.17.3. Shuttle Transport To/From Orbit	3-60
3.2.10.17.4 Emergency Landing	3-61
3.3 SSP 30559 AND SSP 30558 REQUIREMENTS	4-62
3.3.1 SSP 30559, Structural Design and Verification Requirements:	4-62
3.1.3 Strength and Stiffness	4-62
3.1.9 Design Requirements for Pressure System	4-62
3.1.9.1 Fracture Control	4-62
3.1.9.2 Pressure Control	4-62
3.1.9.3 Dewars	4-62
3.1.9.4 Secondary Volumes	4-63
3.1.9.5 Flow Induced Vibration	4-63
3.1.9.6 Pressure Stabilized Vessels	4-63
3.1.9.7 Burst Discs	4-64
3.1.9.8 Mechanical properties	4-64
3.3.2 SSP 30558, Fracture Control Requirements for International Space Station:	4-65
4.4.1 Pressure Vessels	4-65
4.4.1.1	4-65
4.4.2 Pressure System Components	4-66
4.4.2.1	4-66
5.0 OPERATIONAL SAFETY REQUIREMENTS	5-1
5.1 EVA Activity Safety	5-1
5.1.3.1 For Shuttle Loads	5-1
5.1.3.6 Verification Of Beryllium Structures	5-1
APPENDIX A - ACRONYM LISTING	A-1
APPENDIX B - GLOSSARY OF TERMS	B-1
APPENDIX C - TRACEABILITY OF NSTS 1700.7B TO SSP 50021	C-1
APPENDIX D - ATTACHED PRESSURIZED MODULE SEGMENT SPECIFICATION	D-1
APPENDIX E - JEM SEGMENT SPECIFICATION	E-1
APPENDIX F - ITALIAN MINI-PRESSURIZED LOGISTICS SEGMENT SPECIFICATION	F-1
APPENDIX G - MOBILE SERVICING SYSTEM SEGMENT SPECIFICATION	G-1
APPENDIX H - RUSSIAN SEGMENT SPECIFICATION	H-1

1.0 INTRODUCTION

The ISS Program establishes the technical safety requirements for the design, development, test and operation of the International Space Station (ISS) End Items, Launch Packages (LPs), government furnished equipment (GFE), and their ground support equipment (GSE) through the ISS System Specification, SSP 41000, and the subsidiary segment and end item specifications. These specifications will continue to provide the safety requirements for ISS system developers, however, the ISS Prime contractor will be required to show traceability of the requirements herein to the appropriate ISS specifications for implementation and also assess compliance to the requirements herein using the results of the hazard analyses and ISS verification program. Joint documentation has been established to define the International Partner requirements. These documents are applicable to all ISS equipment provided by NASA, it's contractors, and the International Partners including support equipment. NSTS 1700.7B, Safety Policy and Requirements For Payloads Using the International Space Station, requirements applicable to ISS hardware and missions have been incorporated into this document. Appendix C provides tracibility between SSP 50021 and NSTS 1700.7 B.

DCN 001

The following documents were used as a basis to derive SSP 50021.

DOCUMENT NO.	TITLE
SSP 50005	International Space Station Flight Crew Integration Standard (NASA-STD-3000/T)
NSTS 1700.7B	Safety Policy and Requirements for Payloads Using the Space Transportation System
KHB 1700.7B	Space Shuttle Payload Ground Safety Handbook
SSP 30000 Section 3	Space Station Freedom Program Requirements Document, Safety, Reliability, Maintainability, and Quality Assurance Section
SSP 41000	ISS System Specification
SSP 41162	U.S. On-Orbit Segment Specification
SSP 41163	Russian Segment Specification
SSP 41165	Japanese Experiment Module Segment Specification
SSP 41167	Mobile Service System Segment Spcification
SSP 41160	Attached Pressurized Module Segment Specification
SSP 41164	Min-Pressurized Logistics Module Segment Specification
Various	U.S. Prime Item Development Specifications

2.0 APPLICABLE AND REFERENCE DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The documents identified below are applicable to the extent specified herein. The references show where each applicable document is cited in this document.

No applicable documents have been identified.

2.2 REFERENCE DOCUMENTS

The documents identified below are referenced in this document and form a part of this document to the extent specified herein. The locations of each reference are identified.

DOCUMENT NO.

TITLE

ANSI-Z-136.1	American National Standard for Safe Use of Lasers	
Reference 3.3.6.7.1		
KHB 1700.7B	Space Transportation System Payload Ground Safety Handbook	
Reference 1.2.1, 3.3.6.14		
MIL-STD-1522	Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems	
Reference 3.2.10.11, 4.4.11		
MIL-STD-1576	Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems	
Reference 3.3.6.5.1.2	All paragraphs except 5.12.3.1.e.	DCN 001
MSFC-DWG-20M02540	Assessment of Flexible Line for Flow Induced Vibration	
Reference Appendix C		
NSTS 07700, Vol. XIV	System Description and Design Data - Extravehicular Activities	
Reference		
3.3.6.6	Attachment 1 (ICD 2-19001)	
3.3.6.13.6.4		
3.3.6.13.7		
3.3.6.13.8		
3.3.6.12.3.1	Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb	DCN 001
NSTS 08060	Space Shuttle System Pyrotechnic Specification	
Reference 3.3.6.5.1.3		
NSTS 08307	Criteria for Preloaded Bolts	
Reference 3.2.10.12		
NSTS 20793	Manned Space Vehicle, Battery Safety Handbook	
Reference 3.3.6.8.4		

factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of "Design for Minimum Risk" areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards

3.3.6.1.4.1 Inadvertent operation resulting in critical hazards

A function whose inadvertent operation could result in a critical hazard (See Appendix B) shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.4.2 Loss of function resulting in critical hazards

Where loss of a function could result in a critical hazard, no single credible failure (See Appendix B) shall cause loss of that function and the function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function". Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.5 Control of functions resulting in catastrophic hazards

3.3.6.1.5.1 Inadvertent operation resulting in catastrophic hazards

Compliance with requirements a, b, and c may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

- a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See Appendix B), whenever the hazard potential exists.
- b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.
- c. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 Loss of function resulting in catastrophic hazards

Compliance with requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

- a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.
- b. The function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function". .

3.3.6.1.6 Subsequent induced loads

If a component of the <END ITEM> is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the component to eliminate the hazard.

3.3.6.1.7 Safety interlocks

Safety interlocks (See Appendix B) shall be provided to prevent unsafe operations when access to <END ITEM> equipment is required for maintenance.

3.3.6.1.8 Environmental compatibility

<End Item> functions shall be safe (See Appendix B) in the applicable worst case natural and induced environments defined in SSP 41000, paragraph 3.2.6, "Environmental Conditions," or as defined in a payload integration plan, mission integration plan, and/or Interface Control Document (ICD).

DCN 001

3.3.6.2 Hazard Detection and Safing

3.3.6.2.1 Reserved

3.3.6.2.2 Monitors

3.3.6.2.2.1 Status information

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention

3.3.6.6 Non-Ionizing Radiation

- a. The <End Item> shall limit the levels of non-ionizing radiation in accordance with SSP 50005, paragraph 5.7.3.2 or provide personnel protection.
- b. Transmitters shall not irradiate the Orbiter at levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001). A two-fault tolerant combination of pointing controls or independent inhibits to transmission may be used to prevent hazardous irradiation of the Orbiter. The inhibits to prevent radiation do not require monitoring unless the predicted radiation levels exceed Orbiter limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

DCN 001

3.3.6.7 Optics and Lasers

3.3.6.7.1 Lasers

Lasers used on <End Item>s shall be in accordance with American National Standard for Safe Use of Lasers, ANSI-Z-136.1.

3.3.6.7.2 Optical Requirements

3.3.6.7.2.1 Optical instruments

Optical instruments shall prevent harmful light intensities and wavelengths from being viewed by operating personnel.

3.3.6.7.2.2 Personnel protection

Quartz windows, apertures, or beam stops and enclosures shall be used for hazardous wavelengths and intensities unless suitable protective measures are taken to protect personnel from Ultraviolet or Infrared burns or X-Ray radiation.

3.3.6.7.2.3 Direct viewing optical systems

Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems shall be limited to levels below the maximum permissible exposure (MPE).

3.3.6.8 Electrical Safety

3.3.6.8.1 Electrical power circuit overloads

3.3.6.8.1.1 Circuit overload protection

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective device sizing

Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded.

3.3.6.8.1.3 Bent pin or conductive contamination

- a. <End Item> electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.
- b. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 Crew protection for electrical shock

The crew shall be protected from electrical hazards in accordance with SSP 50005, Section 6.4.3.

3.3.6.8.3 Reapplication of power

The <End Item> shall provide local control (See Appendix B) of interruption and reapplication of power to each IVA maintenance area.

3.3.6.8.4 Batteries

Batteries shall be designed to control application hazards caused by buildup or venting of flammable, corrosive or toxic gasses and reaction products; the expulsion of electrolyte; and by failure modes of over temperature, shorts, reverse current, cell reversal, leakage, cell grounds, and over pressure. Safety guidelines for batteries are contained in NSTS 20793.

3.3.6.9 Liquid propellant propulsion system

The <End Item> propulsion system shall be constrained by ISS safety requirements and NSTS safety requirements depending upon the phase of flight.

During <End Item> operations with the Orbiter (including all ground and flight phases until the <End Item> has been initially deployed from the Orbiter payload bay and is at a safe distance from the Orbiter), NSTS requirements related to premature firing of a liquid propellant propulsion system engine apply and are identified in NSTS 1700.7B, all paragraphs under section 202.2.

3.3.6.9.1 Inadvertent engine firings during ISS operations

The design and operations of <End Item> propellant systems during ISS operations shall be constrained by the hazardous consequences of inadvertent engine firings. The consequences of engine firings are dependent upon many factors such as the propellant, plume impingement effects (i.e., contamination, heat flux, loads and moments imparted on the ISS or other space vehicles while docked or in approach corridors), operations being conducted in proximity to the thrusters, collision potential, etc. As a minimum the requirements of paragraphs 3.3.6.1.4.1 and 3.3.6.1.5.1 apply to the control of inadvertent engine firings.

3.3.6.9.1.1 Propellant flow control devices

During on-orbit operations of the ISS with the <End Item>, the propellant delivery system in <End Item> liquid propellant thruster systems shall contain a minimum of two mechanically independent flow control devices in series to prevent engine firing, or expulsion of propellant through the thrust chambers (i.e., at least one isolation valve that separates the propellant tanks from the remainder of the distribution system, and a thruster valve). Since the <End Item> is a bi-propellant system, the minimum number of devices apply to both the oxidizer and fuel sides.

3.3.6.9.1.1.1 Thruster valves

The thruster valves in <End Item> liquid propellant thruster system shall be designed to return to the closed position in the absence of an opening signal.

3.3.6.9.1.1.2 Operations

A minimum of two mechanical flow control devices between the propellant tank and a thruster shall be in the closed position, whenever firing of the thruster could result in catastrophic consequences. If the design of the propellant system is such that the effects of firing some thrusters are non-hazardous and others are hazardous, the non-hazardous thrusters may be fired provided the applicable mechanical flow control devices are closed and the appropriate number of electrical inhibits (see paragraph 3.3.6.9.1.2) are in place for the hazardous thrusters.

3.3.6.9.1.2 Electrical inhibits

The minimum number of independent electrical inhibits to prevent inadvertent firing of a thruster shall be consistent with the hazardous consequences as defined under paragraphs 3.3.6.1.4.1 and

3.3.6.1.5.1. One of the electrical inhibits must control the opening of the isolation valve whenever inadvertent firing would result in catastrophic consequences.

3.3.6.9.1.3 Monitoring of electrical inhibits to prevent catastrophic thruster firing

At least two of the three electrical inhibits to prevent a catastrophic thruster firing shall be monitored with one of those monitors being related to the status of the isolation valve.

3.3.6.9.2 Propellant overheating

The <End Item> propulsion system components (e.g., heaters, valve coils, etc.) that are capable of heating the propellant above the material/fluid compatibility limits of the system shall be two failure tolerant to overheating.

3.3.6.9.3 Propellant leakage

Mechanical fittings in <End Item> propulsion systems shall contain at least two seals to prevent leakage of propellant into the on-orbit environment.

3.3.6.9.4 Reserved

3.3.6.9.5 Plume impingement

The <End Item> shall be able to maintain attitude control of the ISS and prevent hazardous thruster impingement on the Orbiter or the servicing spacecraft.

3.3.6.9.6 Hazardous venting

<End Item> propulsion system vents (i.e., relief valves, turbo pump assemblies, etc.) shall perform the venting function without causing an additional hazard to the ISS, Orbiter, or a servicing vehicle.

3.3.6.9.7 Monitoring propulsion system status

The <End Item> shall provide data related to pressure, temperature, and quantity gauging of <End Item> propulsion system tanks, components, and lines to ISS to monitor system health and safety.

3.3.6.9.8 <End Item> induced loads

The <End Item> shall perform attitude control and reboost functions without inducing loads which exceed the design limit loads specified in the ICD governing the interfaces between the <End Item> and the ISS element(s) to which it is attached.

DCN 001

3.3.6.10 Fire Protection

- a. The Space Station shall have the capability for crew initiated notification of a fire event within 1 minute after crew detection.
- b. The Space Station shall assure that isolation of a fire event does not cause loss of functionality which may create a catastrophic hazard.
- c. The Space Station shall accommodate the application of a fire suppressant at each enclosed location containing a potential fire source.
- d. Fire suppressant shall be compatible with Space Station life support hardware, not reach toxic concentrations, and be noncorrosive.
- e. Fire suppressant by-products shall be compatible with the Space Station life support contamination control capability.
- f. Fixed fire suppression, where installed, shall incorporate a disabling feature to prevent inadvertent activation during maintenance.
- g. One Portable Breathing Apparatus (PBA) and one Portable Fire Extinguisher (PFE) shall be located in elements less than or equal to 24 feet in accessible interior length. Where the element exceeds 24 feet in accessible interior length, a set of PBAs and PFEs shall be located within 12 feet of each end of the element. At least one PBA shall be located within three feet of each PFE.
- h. Fixed fire suppression, where installed, shall be restorable after discharge.
- i. Fixed fire suppression, where installed, shall remain functional after the removal of power to a location after detection of a fire event.

j. The Space Station shall confirm a fire event condition prior to any automated isolation, or suppression. Confirmation consists of at least two validated indications of fire/smoke from a detector.

k. On-board verification of suppressant availability shall be provided.

3.3.6.11 Constraints

3.3.6.11.1 Reserved

3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance

3.3.6.11.2.1 Pressure differential tolerance

<END ITEM> equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard .

3.3.6.11.2.2 Operation during pressure changes

Equipment expected to function during depressurization or repressurization shall be designed to operate without producing hazards.

3.3.6.11.3. Emergency egress

The <End Item> shall provide for safe emergency IVA egress to the remaining contiguous pressurized volumes and have the capability to isolate from other flight pressurized volumes within three minutes, including closing hatches.

3.3.6.11.4. Reserved

3.3.6.11.5 Reserved

3.3.6.11.6 Component hazardous energy provision

Components which retain hazardous energy potential shall either be designed to prevent a crewmember conducting maintenance from releasing the stored energy potential or be designed with provisions to allow safing of the potential energy including provisions to confirm that the safing was successful.

3.3.6.11.7 Hatch opening

The <End Item> shall provide the capability to control pressure differential and verify that the environment is within the oxygen, nitrogen and carbon dioxide levels as well as within the SMAC levels of selected compounds from Table 1 (See paragraph 3.2.2.7, Table VII) provide visual inspection of the interior of the pressurized volume prior to crew ingress.

3.3.6.11.8 Reserved**3.3.6.11.9 Reserved****3.3.6.11.10 Reserved****3.3.6.11.11 Cryogenics****3.3.6.11.11.1 Thermal characteristics**

Cryogenic systems shall allow for component thermal expansion and contraction without imposing excessive loads on the system. Bellows, reactive thrust bellows, or other suitable load relieving flexible joints may be used.

3.3.6.11.11.2 Cryogenic entrapment

Anywhere a cryogenic can be trapped between any valves in the system, automatic relief shall be incorporated to preclude excess pressure from conversion from liquid to gaseous state causing a rupture.

3.3.6.11.11.3 Air compatibility

Cryogenic systems shall be insulated with an oxygen compatible material or be vacuum-jacketed to preclude liquefaction of air.

3.3.6.11.12 Hazardous Gas Accumulation**3.3.6.11.12.1 Accumulation prevention**

The <End Item> shall provide the capability to prevent uncontrolled hazardous accumulations of gases.

3.3.6.11.12.2 Detection, monitoring, and control

Detection, monitoring, and control of hazardous gases or vapors shall be required.

3.3.6.11.13 Equipment clearance for entrapment hazard

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.14 Frangible materials

Equipment inside habitable volumes containing frangible materials shall incorporate features to contain all fragments in the case of breakage.

DCN 001

3.3.6.12 Human engineering safety**3.3.6.12.1 Internal volume touch temperature****3.3.6.12.1.1 Continuous contact - high temperature**

Surfaces which are subject to continuous contact with crewmember bare skin and whose temperature exceeds 113 degrees Fahrenheit, shall be provided with guards or insulation to prevent crewmember contact.

3.3.6.12.1.2 Incidental or momentary contact - high temperature

For incidental or momentary contact (30 seconds or less), the following apply:

Crewmember warning - Surfaces which are subject to incidental or momentary contact with crewmember bare skin and whose temperatures are between 113 and 122 degrees Fahrenheit shall have warning labels that will alert crewmembers to the temperature levels.

Crewmember protection - Surface temperatures which exceed 122 degrees Fahrenheit shall be provided with guards or insulation that prevent crewmember contact.

3.3.6.12.1.3 Internal volume low touch temperature

When surfaces below 39 degrees Fahrenheit which are subject to continuous or incidental contact, are exposed to crewmember bare skin contact, protective equipment shall be provided to the crew and warning labels shall be provided at the surface site.

3.3.6.12.2 External touch temperature

The suit shall be protected from high or low touch temperature extremes as follows:

3.3.6.12.2.1 Incidental contact

For incidental contact, temperatures shall be maintained within -180 to +235 degrees F, or limit heat transfer rates as specified in TableVII, “ Heat Transfer Rates”.

TABLE VII. <u>Heat transfer rates</u>				
Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (5F)	Linear Conductor (BTU/hr 5F)	Maximum Average Heat Rate ⁽¹⁾ (Btu/hr)
Hot Object	Unlimited	113	1.149	42.52 ⁽²⁾
	Incidental (0.5 max)	113	1.444	176.2 ⁽³⁾
Cold Object	Unlimited	40	1.062	-132.7 ⁽²⁾
	Incidental (0.5 max)	40	1.478	-325.2 ⁽³⁾

Notes:

1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 30 minutes of simulated contact (excursions up to 1.5 times this rate for
3. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for

3.3.6.12.2 Unlimited contact

For unlimited contact, temperatures shall be maintained within -45 degrees F to +145, or for designated EVA crew interfaces specified in Table VIII, limit heat transfer rates as specified in Table VII.

TABLE VIII. <u>Designated EVA interfaces</u>
EVA Tools and Support Equipment
EVA Translation Aids (e.g., CETA Cart, handrails, handholds, etc.)
EVA Restraints (foot restraints, tethers, tether points, etc.)
All EVA translation paths (handrails or structure identified for use as a translation path)
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA worksite accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

3.3.6.12.3 External corner and edge protection

3.3.6.12.3.1 Sharp edges

<END ITEM> equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with NSTS 07700, Vol. XIV, Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb.

3.3.6.12.3.2 Thin materials

Materials less than 0.08 inches thick, with exposed edges that are uniformly spaced, not to exceed 0.5 inch gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.003 inches.

3.3.6.12.3.3 Planned maintenance or storage

Equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4.1

3.3.6.12.4 Internal corner and edge protection

3.3.6.12.4.1 Equipment exposed to crew activity

3.3.6.12.17.3 EVA crewmember contact isolation

<END ITEM> hardware which cannot be controlled by design features to comply with "Primary translation routes and established worksites" or "Secondary translation routes and established worksites" shall be isolated to preclude EVA crewmember contact.

3.3.6.12.18 Moving or rotating equipment

The EVA crewmember shall be protected from moving or rotating equipment.

3.3.6.13 Launch vehicle interfaces and services

3.3.6.13.1 Safe Without Space Shuttle Program Services

3.3.6.13.1.1 Fault tolerance/safety margins

The <END ITEM> shall maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight Space Shuttle Program services.

3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions

During Orbiter emergency conditions, <END ITEM> shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

3.3.6.13.2 Critical Orbiter Services

When Orbiter services are to be utilized to control <END ITEM> hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of functions resulting in critical hazards and 3.3.6.1.5, Control of functions resulting in catastrophic hazards.

3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions

Inadvertent deployment, separation or jettison of the <END ITEM> or appendages which could result in a collision or inability to sustain subsequent loads shall be one or two failure tolerance consistent with the hazard level. The general inhibit and monitoring requirements of 3.3.6.1.4, 3.3.6.1.5 and 3.3.6.2.2 apply.

3.3.6.13.4 Planned Deployment/Extension Functions

3.3.6.13.4.1 Violation of Orbiter payload door envelope

If a component of the <END ITEM> or any <END ITEM> orbital support equipment (OSE) violates the payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.

3.3.6.13.4.2 Method of fault tolerance

The combination of these primary and backup methods shall be two-fault tolerant. Two methods are considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

3.3.6.13.5 Contingency return and rapid safing

The <End Item> shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and deorbit when emergency conditions develop.

The <End item> cargo elements shall provide single failure tolerance to allow the Orbiter to start closing the payload bay doors within 1 hour and 45 minutes. Whenever the Shuttle Remote Manipulator System (SRMS) is in use, ten (10) minutes of this time shall be allotted to stowing the SRMS.

DCN 001

3.3.6.13.6 Flammable Atmosphere

3.3.6.13.6.1 Normal functions

- (j) For low cycle applications a proof test of each flight pressure vessel to a minimum of 1.5 times MDP and a fatigue analysis showing the greater of 500 pressure cycles or 10 lifetimes may be used in lieu of testing a certification vessel to qualify a vessel design that in all other respects meets the requirements of SSP 30559 and MIL-STD-1522A, Approach A.

4.4.2 Pressure System Components

4.4.2.1

Pressure system components (or equipment) not meeting the definition of pressure vessels given in Appendix B of SSP 30558, shall be considered fracture critical if they contain hazardous fluids or if loss of pressurization would result in a catastrophic hazard. All fusion weld joints on Fracture Critical components shall be inspected using a qualified NDE method. In instances where NDE is not feasible, or is incapable of being dealt with successfully, the manufacturer will employ a verification by sampling procedure for establishing the quality of uninspectable welds. This option requires NASA or International Partner approval. Cracks or any other type of flaw indication not meeting specification requirements shall be cause for rejection of these components. Safe-life analysis is not required for fracture critical pressurized lines, fittings and components which are proof tested to the factor of safety requirements of SSP 30559, Structural Design and Verification Requirements, section 3.3. In addition to proof testing of parts during individual acceptance, pressure integrity shall be verified at the system level.

5.0 OPERATIONAL SAFETY REQUIREMENTS

5.1 EVA Activity Safety

All ISS requirements for EVA shall be defined and documented in the MIP Operations Approval (from Space Shuttle Astronaut AIT, EVA System AIT, and Space Shuttle Missions AIT) and shall be required for any EVA task. (Ref. COU SSP 50011-01 Rev. B; Para. 4.2.2; Oct. 19, 1994)

5.1.3.1 For Shuttle Loads

The International Space Station structural design and verification requirements for the transport phases to and from orbit shall be consistent with the requirements for Shuttle payloads specified in NSTS 14046. ISS elements shall be verified by test and/or analysis to the ascent vibro-acoustic environment defined in ICD 2-19001.

5.1.3.6 Verification Of Beryllium Structures

Verification of Beryllium structures shall be in accordance with NSTS's 14046, section 5.1.1.1.

Appendix A - Acronym Listing

AC	Alternating Current
BFO	Blood Forming Organs
CETA	Crew and Equipment Translation Aids
CO2	Carbon Dioxide
dB	Decibel
DC	Direct Current
EVA	Extravehicular Activity
ICD	Interface Control Document
ISS	International Space Station
IVA	Intravehicular Activity
IMV	Intermodule Venitlation (System)
MDP	Maximum Design Pressure
MEQ	Milliequilivants
MPE	Maximum Permissible Exposure
MT	Mobile Transporter
NSI	NASA Standard Initiator
NSTS	National Space Transportation System
ORU	Orbital Replacement Unit
OSE	Orbital Support Equipment
PBA	Portable Breathing Apparatus
PFE	Portable Fire Extinguisher
PIP	Payload Integration Plan
RMS	Remote Manipulator Subsystem
RTM	Real-Time Monitor
SMAC	Spacecraft Maximum Allowable Concentration
SRMS	Shuttle Remote Manipulator System
STS	Space Transportation System

DCN 001

DCN 001