

ISS Safety Requirements Document

International Space Station Program

Baseline

September 2019

This publication does not contain information which falls under the purview of the U.S. Munitions List (USML), as defined in the International Traffic in Arms Regulations (ITAR), 22 CFR 120-130, and is not export controlled via the ITAR. This publication also does not contain information within the purview of the Export Administration Regulation (EAR), 15 CFR 730-744, and is not export controlled via the EAR. Additional release to the general public requires approval through the appropriate NASA release process.



National Aeronautics and Space Administration
International Space Station Program
Johnson Space Center
Houston, Texas Contract No.: NNJ12GA46C



REVISION AND HISTORY

REV.	DESCRIPTION	PUB. DATE
-	Initial Release (Reference per SSCD 015733, EFF. 10-18-19) Early Release Program Release	10-21-19 XX-XX-XX

PREFACE

ISS SAFETY REQUIREMENTS DOCUMENT

The contents of this document are intended to be consistent with the tasks and products to be prepared by the International Space Station Program participants. SSP 51721 shall be implemented on all new International Space Station (ISS) contractual and internal activities and shall be included in any existing contracts through contract changes. This document is under the control of the Space Station Control Board (SSCB). The SSCB delegates control and approval authority for future updates and/or revisions to the Multilateral Safety and Mission Assurance Control Board (MSMACB).

See Directive Approval _____

Kirk Shireman
National Aeronautics and Space Administration
International Space Station Program
Program Manager

_____ Date

ISS SAFETY REQUIREMENTS DOCUMENT
CONCURRENCE
SEPTEMBER 2019

Concurred by: Willie Lyles OE
SAFETY & MISSION ASSURANCE/PROGRAM RISK ORG
MANAGER
Willie Lyles 10/8/19
SIGNATURE DATE

Concurred by: Kristi Duplichen OE
ISS SAFETY MANAGER ORG
Kristi Duplichen 10/8/19
SIGNATURE DATE

Prepared & Jenny Andrews OE
Supervised by: SAFETY REQUIREMENTS PROJECT LEAD ORG
Jenny Andrews 10/8/19
SIGNATURE DATE

Prepared by: Monica Garcia OP
MAPI BOOK MANAGER ORG
Monica Garcia 10/08/19
SIGNATURE DATE

Book Coordinator: Marilyn J Jordan OP
MAPI BOOK COORDINATOR/DQA REPRESENTATIVE ORG
Marilyn J Jordan 10/08/19
SIGNATURE DATE

ISS SAFETY REQUIREMENTS DOCUMENT
APPROVAL
SEPTEMBER 2019

Approved by:

ESA REPRESENTATIVE

ESA
ORG

SIGNATURE

DATE

Approved by:

JAXA REPRESENTATIVE

JAXA
ORG

SIGNATURE

DATE

Approved by:

ASI REPRESENTATIVE

ASI
ORG

SIGNATURE

DATE

Approved by:

RSCE REPRESENTATIVE

RSCE
ORG

SIGNATURE

DATE

PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

PARAGRAPH		PAGE
1.0	INTRODUCTION	1-1
1.1	PURPOSE	1-1
1.2	SCOPE	1-1
1.3	PRECEDENCE.....	1-2
1.4	VERB APPLICATION.....	1-2
2.0	DOCUMENTS	2-1
2.1	APPLICABLE DOCUMENTS.....	2-1
2.2	REFERENCE DOCUMENTS	2-4
3.0	GENERAL	3-1
3.1	RESPONSIBILITY	3-1
3.1.1	ISS PROGRAM	3-1
3.1.2	INTERNATIONAL SPACE STATION SAFETY REVIEW PANEL (ISRP).....	3-1
3.1.3	END ITEM PROVIDER.....	3-1
3.1.4	INTERNATIONAL PARTNER.....	3-1
3.2	SAFETY ANALYSIS	3-1
3.3	HAZARD CONTROL SCHEME	3-2
3.3.1	DESIGN TO TOLERATE FAILURES (FAILURE TOLERANCE)	3-2
3.3.2	DESIGN FOR MINIMUM RISK.....	3-2
3.4	HAZARD REDUCTION PRECEDENCE SEQUENCE.....	3-3
3.4.1	DESIGN.....	3-3
3.4.2	SAFETY DEVICES.....	3-3
3.4.3	WARNING DEVICES	3-3
3.4.4	OPERATIONAL CONTROLS	3-3
3.5	GROUND SUPPORT EQUIPMENT AND GROUND PROCESSING HAZARDS.....	3-4
3.5.1	KENNEDY SPACE CENTER LAUNCH FACILITY	3-4
3.5.2	NORTHROP GRUMMAN LAUNCH FACILITY	3-4
3.5.3	SPACE LAUNCH FACILITY	3-4
3.5.4	SOYUZ/PROGRESS LAUNCH FACILITY	3-4
3.5.5	HTV LAUNCH FACILITY	3-4
3.6	VISITING VEHICLES	3-5
3.7	RUSSIAN SEGMENT OPERATIONS	3-6
3.8	MAINTENANCE/ACCESS.....	3-6
3.9	DEPLOYABLE/FREE FLYING END ITEMS	3-6
3.10	REFLIGHT, SERIES, AND MODIFIED END ITEMS	3-7
3.11	CREW HABITABLE MODULES	3-7
3.12	VERIFICATION	3-8
3.12.1	VERIFICATION METHODS.....	3-8
3.13	LIMITED LIFE ITEM VERIFICATION	3-9
3.14	SAFETY NON-COMPLIANCE REPORTS	3-9
3.15	SAFETY CRITICAL	3-9
3.16	FAIL SAFE.....	3-10

SSP 51721
Baseline

4.0	SAFETY REQUIREMENTS.....	4-1
4.1	CORE REQUIREMENTS	4-1
4.1.1	GENERAL HAZARD SEVERITIES, CONTROLS, & VERIFICATION REQUIREMENTS.....	4-1
4.1.1.1	MARGINAL HAZARD CONTROLS	4-1
4.1.1.1.1	VERIFICATION – MARGINAL HAZARD CONTROLS	4-1
4.1.1.2	CRITICAL HAZARD CONTROLS.....	4-1
4.1.1.2.1	VERIFICATION – CRITICAL HAZARD CONTROLS.....	4-2
4.1.1.3	CATASTROPHIC HAZARD CONTROLS	4-2
4.1.1.3.1	VERIFICATION – CATASTROPHIC HAZARD CONTROLS	4-2
4.1.2	ENVIRONMENTAL COMPATIBILITY	4-3
4.1.2.1	VERIFICATION – ENVIRONMENTAL COMPATIBILITY	4-3
4.1.3	SAFE WITHOUT SERVICES	4-3
4.1.3.1	VERIFICATION - SAFE WITHOUT SERVICES	4-4
4.1.4	CRITICAL SERVICES.....	4-4
4.1.4.1	VERIFICATION – CRITICAL SERVICES	4-4
4.2	STRUCTURES.....	4-4
4.2.1	SAFETY CRITICAL STRUCTURES AND FRACTURE CONTROL	4-4
4.2.1.1	PAYLOAD STRUCTURES AND FRACTURE CONTROL.....	4-5
4.2.1.1.1	VERIFICATION – PAYLOAD STRUCTURES AND FRACTURE CONTROL.....	4-5
4.2.1.2	NON-PAYLOAD STRUCTURES	4-5
4.2.1.2.1	VERIFICATION - NON-PAYLOAD STRUCTURES.....	4-6
4.2.1.3	NON-PAYLOAD FRACTURE CONTROL	4-6
4.2.1.3.1	VERIFICATION – NON-PAYLOAD FRACTURE CONTROL.....	4-6
4.2.2	SAFETY CRITICAL MECHANISMS	4-6
4.2.2.1	MECHANISMS CLEARANCE	4-7
4.2.2.1.1	VERIFICATION – MECHANISMS CLEARANCE	4-8
4.2.2.2	MECHANISMS TOLERANCES	4-8
4.2.2.2.1	VERIFICATION – MECHANISMS TOLERANCES.....	4-9
4.2.2.3	MECHANISMS LUBRICATION	4-9
4.2.2.3.1	VERIFICATION - MECHANISMS LUBRICATION.....	4-9
4.2.2.4	MECHANISMS SPRINGS	4-10
4.2.2.4.1	VERIFICATION – FAILURE TOLERANT MECHANISM SPRINGS	4-10
4.2.2.5	MECHANISM ACTUATION FORCE/TORQUE STALL	4-10
4.2.2.5.1	VERIFICATION-MECHANISM ACTUATION FORCE/TORQUE STALL	4-10
4.2.2.6	MECHANISM MECHANICAL STOPS.....	4-10
4.2.2.6.1	VERIFICATION - MECHANISM MECHANICAL STOPS.....	4-11
4.2.2.7	MECHANISM INADVERTENT IMPACT LOADS.....	4-11
4.2.2.7.1	VERIFICATION - MECHANISM INADVERTENT IMPACT LOADS.....	4-11
4.2.2.8	MECHANISM POSITIVE INDICATION OF STATUS	4-11
4.2.2.8.1	VERIFICATION - MECHANISM POSITIVE INDICATION OF STATUS	4-11
4.2.2.9	MECHANISM STARTING TORQUE/FORCE MARGINS	4-11
4.2.2.9.1	VERIFICATION - MECHANISM STARTING TORQUE/FORCE MARGINS.....	4-12
4.2.2.10	MECHANISM DYNAMIC TORQUE/FORCE MARGINS.....	4-12
4.2.2.10.1	VERIFICATION - MECHANISM DYNAMIC TORQUE/FORCE MARGINS	4-12

SSP 51721
Baseline

4.2.2.11	MECHANISM HOLDING FORCE MARGINS	4-12
4.2.2.11.1	VERIFICATION – MECHANISM HOLDING FORCE MARGINS	4-13
4.2.2.12	MECHANISM CONTAMINATION.....	4-13
4.2.2.12.1	VERIFICATION – MECHANISM CONTAMINATION.....	4-13
4.2.2.13	MECHANISM FUNCTION	4-13
4.2.2.13.1	VERIFICATION - MECHANISM FUNCTION	4-13
4.2.2.14	MECHANISM LIFE	4-14
4.2.2.14.1	VERIFICATION - MECHANISM LIFE.....	4-14
4.2.2.15	MECHANISM LOAD REDISTRIBUTION.....	4-14
4.2.2.15.1	VERIFICATION - MECHANISM LOAD REDISTRIBUTION.....	4-14
4.2.3	PRESSURE SYSTEMS.....	4-14
4.2.3.1	PRESSURE SYSTEMS – SEALED CONTAINER.....	4-15
4.2.3.1.1	VERIFICATION – SEALED CONTAINER	4-16
4.2.3.2	PRESSURE SYSTEMS - PRESSURE VESSELS.....	4-16
4.2.3.2.1	PRESSURE SYSTEMS – PAYLOAD PRESSURE VESSELS.....	4-16
4.2.3.2.1.1	VERIFICATION - PRESSURE SYSTEMS – PAYLOAD PRESSURE VESSELS.....	4-16
4.2.3.2.2	PRESSURE SYSTEMS – SYSTEM PRESSURE VESSELS	4-16
4.2.3.2.2.1	VERIFICATION - PRESSURE SYSTEMS – SYSTEM PRESSURE VESSELS.....	4-16
4.2.3.3	PRESSURE SYSTEMS PRESSURIZED LINES, FITTINGS AND COMPONENTS RESTRAINT	4-16
4.2.3.3.1	VERIFICATION PRESSURIZED LINES, FITTINGS AND COMPONENTS RESTRAINT	4-17
4.3	ELECTRICAL	4-17
4.3.1	ELECTRICAL SYSTEMS	4-17
4.3.1.1	RESERVED.....	4-18
4.3.1.2	WIRE DERATING.....	4-18
4.3.1.2.1	VERIFICATION - WIRE DERATING	4-19
4.3.1.3	CIRCUIT PROTECTION	4-19
4.3.1.3.1	VERIFICATION – CIRCUIT PROTECTION.....	4-19
4.3.1.4	DC CIRCUIT ELECTRICAL INHIBITS USED TO PREVENT CATASTROPHIC HAZARDS	4-20
4.3.1.4.1	VERIFICATION – DIRECT CURRENT (DC) CIRCUIT ELECTRICAL INHIBITS USED TO PREVENT CATASTROPHIC HAZARDS	4-20
4.3.1.5	SEPARATION OF REDUNDANT SAFETY CRITICAL CIRCUITS	4-20
4.3.1.5.1	VERIFICATION – SEPARATION OF REDUNDANT SAFETY CRITICAL CIRCUITS	4-20
4.3.2	ELECTRIC SHOCK	4-21
4.3.2.1	GENERAL EPCE WITH NO DIRECT INTERFACE TO MEDICAL EQUIPMENT.....	4-21
4.3.2.1.1	VERIFICATION – GENERAL EPCE WITH NO DIRECT INTERFACE TO MEDICAL EQUIPMENT	4-22
4.3.2.2	GENERAL EPCE WITH DIRECT INTERFACES TO MEDICAL EQUIPMENT.....	4-22
4.3.2.2.1	VERIFICATION – GENERAL EPCE WITH DIRECT INTERFACES TO MEDICAL EQUIPMENT	4-23
4.3.2.3	PROTECTIVE COVERS – ELECTRICAL POWER CONDUCTORS AND TERMINATIONS	4-23
4.3.2.3.1	VERIFICATIONS – PROTECTIVE COVERS – ELECTRICAL POWER CONDUCTORS AND TERMINATIONS	4-24
4.3.2.4	BONDING AND ISOLATION	4-24

**SSP 51721
Baseline**

4.3.2.4.1	VERIFICATIONS – BONDING AND ISOLATION.....	4-25
4.3.3	ELECTRICAL SHOCK AND MOLTEN METAL – CREW MATING/DEMATING OF ELECTRICAL CONNECTORS.....	4-25
4.3.3.1	SCOOP-PROOF POWER CONNECTORS.....	4-26
4.3.3.1.1	VERIFICATIONS – SCOOP-PROOF POWER CONNECTORS.....	4-26
4.3.3.2	POWER CONNECTOR SOCKETS.....	4-26
4.3.3.2.1	VERIFICATION – POWER CONNECTOR SOCKETS.....	4-27
4.3.3.3	UPSTREAM VERIFIABLE INHIBIT FOR POWER CONNECTORS.....	4-27
4.3.3.3.1	VERIFICATION – UPSTREAM VERIFIABLE INHIBIT FOR POWER CONNECTORS.....	4-27
4.3.3.4	EVA 2 ND UPSTREAM INHIBIT FOR MATING/DEMATING ELECTRICAL POWER CONNECTORS <200VDC/RMS, <65A, <8.2KW, OR A BATTERY OCV <40VDC.....	4-27
4.3.3.4.1	VERIFICATION - EVA 2 ND UPSTREAM INHIBIT FOR MATING/DEMATING ELECTRICAL POWER CONNECTORS <200V DC/RMS, <65A, <8.2KW, OR A BATTERY OCV <40VDC.....	4-28
4.3.3.5	BATTERY CONNECTORS WITH OCV <40VDC.....	4-29
4.3.3.5.1	VERIFICATION - BATTERY CONNECTORS WITH OCV <40VDC.....	4-29
4.3.3.6	BLIND MATE OR REMOTE CONNECTORS >32V DC/RMS.....	4-29
4.3.3.6.1	VERIFICATION – BLIND MATE OR REMOTE CONNECTORS >32V DC/RMS.....	4-30
4.3.3.7	SECOND VERIFIABLE UPSTREAM INHIBIT FOR POWER CONNECTORS >200V DC/RMS, >65A, >8.2KW, AND/OR >40VDC BATTERIES.....	4-30
4.3.3.7.1	VERIFICATION - SECOND VERIFIABLE UPSTREAM INHIBIT FOR POWER CONNECTORS >200V DC/RMS, >65A AND/OR >40VDC BATTERIES.....	4-30
4.3.4	BIOMEDICAL INSTRUMENTATION.....	4-30
4.3.4.1	BIOINSTRUMENTATION CERTIFICATION.....	4-33
4.3.4.1.1	VERIFICATION - BIOINSTRUMENTATION CERTIFICATION.....	4-33
4.3.4.2	BIOINSTRUMENTATION TOUCH/LEAKAGE CURRENT.....	4-33
4.3.4.2.1	VERIFICATION – BIOINSTRUMENTATION TOUCH/LEAKAGE CURRENT.....	4-34
4.3.4.3	BIOINSTRUMENTATION INTENTIONAL CREW APPLIED CURRENT.....	4-35
4.3.4.3.1	VERIFICATION – BIOINSTRUMENTATION INTENTIONAL CREW APPLIED CURRENT..	4-35
4.3.4.4	AMBULATORY CREW BIOINSTRUMENTATION.....	4-35
4.3.4.4.1	BATTERY POWERED.....	4-35
4.3.4.4.1.1	VERIFICATION –AMBULATORY CREW BIOINSTRUMENTATION - BATTERY POWERED.....	4-35
4.3.4.4.2	ELECTRICALLY INSULATED.....	4-36
4.3.4.4.2.1	VERIFICATION – AMBULATORY CREW BIOINSTRUMENTATION – ELECTRICALLY INSULATED.....	4-36
4.3.4.4.3	ELECTRICALLY ISOLATED.....	4-36
4.3.4.4.3.1	VERIFICATION – AMBULATORY CREW BIOINSTRUMENTATION – ELECTRICALLY ISOLATED.....	4-37
4.3.5	BATTERIES.....	4-37
4.3.5.1	LOW BRC BATTERIES.....	4-40
4.3.5.1.1	VERIFICATION – LOW BRC BATTERIES.....	4-40
4.3.5.2	MEDIUM/HIGH BRC BATTERIES.....	4-41
4.3.5.2.1	VERIFICATION – FUNCTIONAL BASELINE TEST.....	4-41
4.3.5.2.2	VERIFICATION – QUALIFICATION TEST.....	4-41
4.3.5.2.3	VERIFICATION – MEDIUM AND HIGH BRC CUSTOM FLIGHT BATTERIES.....	4-43

SSP 51721
Baseline

4.3.5.2.4	VERIFICATION – MEDIUM AND HIGH BRC BATTERIES FLIGHT ACCEPTANCE	4-43
4.3.5.2.5	VERIFICATION – PRIMARY MEDIUM AND HIGH BRC CELLS/OR BATTERIES	4-43
4.3.5.2.6	VERIFICATION – HIGH BRC END ITEM THERMAL RUNAWAY.....	4-43
4.3.6	CAPACITORS	4-44
4.3.6.1	ELECTROLYTIC CAPACITORS	4-45
4.3.6.1.1	VERIFICATION – ELECTROLYTIC CAPACITORS	4-46
4.3.6.2	ELECTROCHEMICAL CAPACITORS	4-47
4.3.6.2.1	LOW RISK ELECTROCHEMICAL CAPACITORS	4-49
4.3.6.2.1.1	VERIFICATION – LOW RISK ELECTROCHEMICAL CAPACITORS	4-49
4.3.6.2.2	MEDIUM/HIGH RISK ELECTROCHEMICAL CAPACITORS	4-49
4.3.6.2.2.1	VERIFICATION – MEDIUM/HIGH RISK ELECTROCHEMICAL CAPACITORS	4-49
4.3.7	ELECTROMAGNETIC COMPATIBILITY	4-52
4.3.7.1	ELECTROMAGNETIC EFFECTS	4-52
4.3.7.2	PROTECTING AGAINST HAZARDOUS RF IRRADIATION	4-52
4.3.7.2.1	VERIFICATION - PROTECTING AGAINST HAZARDOUS RF IRRADIATION.....	4-52
4.3.7.3	DEPLOYABLE END ITEM RADIO FREQUENCY TRANSMITTERS	4-54
4.3.7.3.1	VERIFICATION - DEPLOYABLE END ITEM RADIO FREQUENCY TRANSMITTERS	4-54
4.3.8	RADIO FREQUENCY-TRANSMITTER COMPATIBILITY	4-55
4.3.8.1	PROTECTING AGAINST HAZARDOUS RF IRRADIATION	4-55
4.3.8.1.1	VERIFICATION - PROTECTING AGAINST HAZARDOUS RF IRRADIATION.....	4-57
4.4	COMMAND AND DATA HANDLING	4-59
4.4.1	COMPUTERS BASED CONTROL SYSTEMS.....	4-59
4.4.2	HAZARDOUS COMMANDING.....	4-59
4.4.2.1	ON-BOARD COMPUTER SYSTEMS.....	4-60
4.4.2.1.1	VERIFICATION ON BOARD COMPUTER SYSTEMS HAZARDOUS COMMANDING	4-60
4.4.2.2	BI-DIRECTIONAL KU-BAND (KU) ACCESS FOR LOCAL AREA NETWORK (LAN) (KU/LAN)	4-61
4.4.2.2.1	KU/LAN SAFETY ASSESSMENT	4-61
4.4.2.2.1.1	VERIFICATION – KU/LAN SAFETY ASSESSMENT	4-61
4.4.2.2.2	KU/LAN INFORMATION TECHNOLOGY (IT) SECURITY ASSESSMENT	4-62
4.4.2.2.2.1	VERIFICATION: KU/LAN (IT) SECURITY ASSESSMENT	4-62
4.4.2.2.3	ON BOARD SOFTWARE PROTECTIONS WITH KU/LAN INTERFACES.....	4-63
4.4.2.2.3.1	VERIFICATION - ON BOARD SOFTWARE PROTECTIONS WITH KU/LAN INTERFACES.....	4-63
4.4.2.2.4	KU/LAN AND HAZARDOUS COMMANDING - MUST WORK FUNCTIONS	4-63
4.4.2.2.4.1	VERIFICATION – KU/LAN AND HAZARDOUS COMMANDING – MUST WORK FUNCTIONS.....	4-63
4.4.2.2.5	KU/LAN AND HAZARDOUS COMMANDING – COMMAND AND DATA INTEGRITY	4-64
4.4.2.2.5.1	VERIFICATION KU/LAN AND HAZARDOUS COMMANDING – COMMAND AND DATA INTEGRITY	4-64
4.4.2.3	GROUND INITIATED HAZARDOUS COMMANDING.....	4-64
4.4.2.3.1	VERIFICATION – GROUND INITIATED HAZARDOUS COMMANDING.....	4-65
4.5	MONITORING	4-67
4.5.1	MONITORING – MONITOR CAPABILITIES	4-69
4.5.1.1	VERIFICATION – MONITORING – MONITOR CAPABILITIES	4-69

**SSP 51721
Baseline**

4.5.2	MONITORING FREQUENCY.....	4-70
4.5.2.1	MONITORING FREQUENCY – RTM.....	4-71
4.5.2.1.1	VERIFICATION – MONITORING FREQUENCY – RTM.....	4-71
4.5.2.2	MONITORING FREQUENCY – NEAR REAL TIME MONITORING (NRTM).....	4-71
4.5.2.2.1	VERIFICATION– MONITORING FREQUENCY – NRTM.....	4-72
4.5.2.3	MONITORING FREQUENCY - WHEN INHIBIT MONITORING IS NOT REQUIRED.....	4-72
4.5.2.3.1	VERIFICATION – MONITORING FREQUENCY – WHEN INHIBIT MONITORING IS NOT REQUIRED.....	4-72
4.5.3	MONITORING OF DEPLOYABLE END ITEMS FROM ISS.....	4-73
4.5.3.1	VERIFICATION – MONITORING OF DEPLOYABLE END ITEMS FROM ISS.....	4-74
4.5.4	USE OF TIMERS.....	4-74
4.5.4.1.1	VERIFICATION – USE OF TIMERS.....	4-74
4.6	EXTERNAL ENVIRONMENTS.....	4-75
4.6.1	PLASMA.....	4-75
4.6.2	IONIZING RADIATION ENVIRONMENT.....	4-76
4.6.2.1	IONIZING RADIATION.....	4-76
4.6.2.1.1	VERIFICATION – IONIZING RADIATION.....	4-76
4.7	MATERIALS.....	4-77
4.7.1	MATERIALS SELECTION.....	4-77
4.7.1.1	FLAMMABLE MATERIALS.....	4-78
4.7.1.1.1	VERIFICATION – FLAMMABLE MATERIALS.....	4-79
4.7.1.2	MATERIAL OFFGASSING IN HABITABLE AREAS.....	4-79
4.7.1.2.1	VERIFICATION – MATERIAL OFFGASSING IN HABITABLE AREAS.....	4-80
4.7.1.3	MATERIALS COMPATIBILITY.....	4-80
4.7.1.3.1	VERIFICATION - MATERIALS COMPATIBILITY.....	4-81
4.7.2	HAZARDOUS MATERIALS.....	4-81
4.7.2.1	HAZARDOUS MATERIALS EXTERNAL RELEASE NEAR OR THROUGH THE ISS.....	4-90
4.7.2.1.1	VERIFICATION – EXTERNAL RELEASE OF HAZARDOUS MATERIALS NEAR OR THROUGH THE ISS.....	4-90
4.7.2.2	CHEMICALS.....	4-91
4.7.2.2.1	CHEMICAL RELEASE.....	4-91
4.7.2.2.1.1	VERIFICATION - RELEASE OF CHEMICALS.....	4-92
4.7.2.2.2	REDUCTION IN FAILURE TOLERANCE FOR CHEMICALS (LIQUIDS) DURING OPERATIONS.....	4-93
4.7.2.2.2.1	VERIFICATION - FAILURE TOLERANCE REDUCTION FOR CHEMICALS (LIQUIDS) DURING OPERATIONS.....	4-94
4.7.2.3	RADIOACTIVE MATERIAL RELEASE.....	4-95
4.7.2.3.1	VERIFICATION– RADIOACTIVE MATERIALS RELEASE.....	4-95
4.7.2.4	BIOLOGICAL MATERIAL RELEASE.....	4-96
4.7.2.4.1	VERIFICATION - RELEASE OF BIOLOGICALS.....	4-97
4.7.2.5	PHYSICAL AGENTS.....	4-98
4.7.2.5.1	PHYSICAL AGENTS RELEASE.....	4-98
4.7.2.5.1.1	VERIFICATION– RELEASE OF PHYSICAL AGENTS.....	4-98
4.7.2.5.2	SHATTERABLE MATERIALS.....	4-99
4.7.2.5.2.1	SHATTERABLE MATERIALS RELEASE.....	4-100

**SSP 51721
Baseline**

4.7.2.5.2.1.1	VERIFICATION– SHATTERABLE MATERIALS RELEASE	4-100
4.7.2.5.2.2	OPTICAL GLASS PROTECTION.....	4-100
4.7.2.5.2.2.1	VERIFICATION– OPTICAL GLASS PROTECTION.....	4-101
4.8	FIRE PROTECTION.....	4-101
4.9	HUMAN FACTORS SAFETY	4-102
4.9.1	ACOUSTICS.....	4-102
4.9.1.1	IMPULSE NOISE HAZARD LIMIT.....	4-103
4.9.1.1.1	VERIFICATION– IMPULSE NOISE HAZARD LIMIT.....	4-103
4.9.1.2	CLASS 1 AND CLASS 2 ALARM AUDIBILITY.....	4-103
4.9.1.2.1	VERIFICATION- CLASS 1 AND CLASS 2 ALARM AUDIBILITY.....	4-104
4.9.1.3	ALARM HAZARD LIMIT	4-104
4.9.1.3.1	VERIFICATION - ALARM HAZARD LIMIT	4-104
4.9.1.4	REVERBERATION TIME	4-104
4.9.1.4.1	VERIFICATION - REVERBERATION TIME	4-104
4.9.1.5	COMPOSITE CONTINUOUS ACOUSTIC EMISSIONS – ISS LEVEL REQUIREMENT (USOS).....	4-105
4.9.1.5.1	VERIFICATION – COMPOSITE CONTINUOUS ACOUSTIC EMISSIONS.....	4-105
4.9.2	IVA TOUCH TEMPERATURE	4-105
4.9.2.1	TOUCH TEMPERATURE LIMITS	4-106
4.9.2.1.1	VERIFICATION - TOUCH TEMPERATURE LIMITS	4-106
4.9.2.2	TOUCH TEMPERATURE BASED ON END ITEM FUNCTIONALITY	4-107
4.9.2.2.1	VERIFICATION - TOUCH TEMPERATURE BASED ON END ITEM FUNCTIONALITY.....	4-108
4.9.3	IVA CREW CONTACT HAZARDS	4-108
4.9.3.1	USE OF SAFETY WIRE	4-109
4.9.3.1.1	VERIFICATION - USE OF SAFETY WIRE.....	4-109
4.9.4	LASERS AND BROADBAND LIGHT.....	4-109
4.9.4.1	LASERS - GENERAL	4-110
4.9.4.1.1	VERIFICATION- –LASERS - GENERAL.....	4-110
4.9.4.2	MAGNIFICATION OF LASERS	4-111
4.9.4.2.1	VERIFICATION- MAGNIFICATION OF LASERS.....	4-111
4.9.4.3	CLASS 3R, 3B, AND 4 LASERS	4-111
4.9.4.3.1	VERIFICATION - CLASS 3R, 3B, AND 4 LASERS	4-112
4.9.4.4	VISIBLE LIGHT EXPOSURE FROM ARTIFICIAL SOURCES	4-112
4.9.4.4.1	VERIFICATION- VISIBLE LIGHT EXPOSURE FROM ARTIFICIAL SOURCES.....	4-112
4.9.4.5	INFRARED RADIATION (IR) LIGHT EXPOSURE FROM ARTIFICIAL SOURCES.....	4-112
4.9.4.5.1	VERIFICATION – INFRARED RADIATION (IR) LIGHT EXPOSURE FROM ARTIFICIAL SOURCES.....	4-113
4.9.4.6	ULTRAVIOLET (UV) RADIATION LIGHT EXPOSURE FROM ARTIFICIAL SOURCES	4-113
4.9.4.6.1	VERIFICATION – ULTRAVIOLET (UV) RADIATION LIGHT EXPOSURE FROM ARTIFICIAL SOURCES.....	4-113
4.9.5	LIGHTING.....	4-113
4.9.5.1	EMERGENCY EGRESS PATH INDICATION	4-113
4.9.5.1.1	VERIFICATION - EMERGENCY EGRESS PATH INDICATION	4-114
4.9.6	EMERGENCY RESPONSE.....	4-114
4.9.6.1	EGRESS FROM END ITEM APPARATUS	4-114

SSP 51721
Baseline

4.9.6.1.1	VERIFICATION – EGRESS FROM END ITEM APPARATUS	4-114
4.9.6.2	INTRAMODULE EMERGENCY EGRESS	4-114
4.9.6.2.1	VERIFICATION – INTRAMODULE EMERGENCY EGRESS	4-115
4.9.6.3	VOLUME ISOLATION	4-115
4.9.6.3.1	VERIFICATION – VOLUME ISOLATION	4-115
4.9.6.4	HATCH DRAG-THROUGHS	4-116
4.9.6.4.1	VERIFICATION – HATCH DRAG-THROUGHS	4-116
4.10	EXTRAVEHICULAR ACTIVITY	4-116
4.10.1	EVA TEMPERATURE EXTREMES.....	4-117
4.10.1.1	INCIDENTAL CONTACT.....	4-117
4.10.1.1.1	VERIFICATION- INCIDENTAL CONTACT.....	4-118
4.10.1.2	UNLIMITED CONTACT.....	4-118
4.10.1.2.1	VERIFICATION- UNLIMITED CONTACT.....	4-119
4.10.2	EXTERNAL CORNER AND EDGE	4-119
4.10.2.1	SHARP EDGES AND PROTRUSIONS.....	4-119
4.10.2.1.1	VERIFICATION – SHARP EDGES AND PROTRUSIONS.....	4-122
4.10.2.2	EVA BURRS.....	4-122
4.10.2.2.1	VERIFICATION – EVA BURRS.....	4-123
4.10.3	EQUIPMENT CLEARANCE FOR ENTRAPMENT HAZARD.....	4-123
4.10.3.1	EVA HOLES	4-123
4.10.3.1.1	VERIFICATION – EVA HOLES	4-123
4.10.3.2	GLOVED OPERATION	4-123
4.10.3.2.1	VERIFICATION – GLOVED OPERATION	4-124
4.10.3.3	TRANSLATION PATHS	4-124
4.10.3.3.1	VERIFICATION – TRANSLATION PATHS	4-124
4.10.4	PINCH POINTS.....	4-125
4.10.4.1	VERIFICATION - PINCH POINTS.....	4-125
4.10.5	CREW IMPACT FROM MOVING OR ROTATING EQUIPMENT	4-125
4.10.5.1	VERIFICATION - CREW IMPACT FROM MOVING OR ROTATING EQUIPMENT.....	4-125
4.10.6	UNCONTROLLED MOTION OF FLEX HOSES	4-126
4.10.6.1	VERIFICATION – UNCONTROLLED MOTION OF FLEX HOSES	4-126
4.10.7	ENTANGLEMENT	4-126
4.10.7.1	VERIFICATION – ENTANGLEMENT	4-126
4.10.8	COMPONENT HAZARDOUS ENERGY – STORED ENERGY.....	4-126
4.10.8.1	VERIFICATION – COMPONENT HAZARDOUS ENERGY – STORED ENERGY.....	4-126
4.10.9	TOXIC/CORROSIVE MATERIALS.....	4-127
4.10.9.1	VERIFICATION – TOXIC/CORROSIVE MATERIALS.....	4-127
4.11	MICROMETEOROID AND ORBITAL DEBRIS.....	4-128
4.11.1	MICROMETEOROID AND ORBITAL DEBRIS.....	4-128
4.11.1.1	VERIFICATION – MICROMETEOROID AND ORBITAL DEBRIS.....	4-128
4.12	PROPULSION SYSTEMS.....	4-129
4.12.1	SOLID PROPELLANT ROCKET MOTORS	4-130
4.12.1.1	VERIFICATION – SOLID PROPELLANT ROCKET MOTORS.....	4-130
4.12.2	LIQUID PROPELLANT PROPULSION SYSTEMS	4-131

SSP 51721
Baseline

4.12.2.1	VERIFICATION- LIQUID PROPELLANT PROPULSION SYSTEMS	4-131
4.12.3	ADIABATIC/RAPID COMPRESSION DETONATION	4-132
4.12.3.1	VERIFICATION - ADIABATIC/RAPID COMPRESSION DETONATION	4-132
4.12.4	PROPELLANT OVERHEATING.....	4-132
4.12.4.1	VERIFICATION- PROPELLANT OVERHEATING.....	4-133
4.12.5	PROPELLANT LEAKAGE	4-133
4.12.5.1	VERIFICATION - PROPELLANT LEAKAGE	4-133
4.12.6	MONITORING PROPULSION SYSTEM STATUS.....	4-133
4.12.6.1	VERIFICATION- MONITORING PROPULSION SYSTEM STATUS.....	4-133
4.13	PYROTECHNIC SYSTEMS	4-133
4.13.1	PYROTECHNIC LOSS OF FUNCTION (MUST WORK).....	4-134
4.13.1.1	VERIFICATION - PYROTECHNIC LOSS OF FUNCTION (MUST WORK).....	4-134
4.13.2	ELECTRICAL EXPLOSIVE DEVICES.....	4-135
4.13.2.1	VERIFICATION- ELECTRICAL EXPLOSIVE DEVICES	4-135
4.13.3	PYROTECHNIC ELECTRICAL CIRCUITS.....	4-136
4.13.3.1	VERIFICATION – PYROTECHNIC CONNECTORS AND PINS	4-136
4.13.3.2	VERIFICATION – FIRING CIRCUITS	4-137
4.13.3.3	VERIFICATION – PYROTECHNIC MONITOR CIRCUITS.....	4-137
4.13.3.4	VERIFICATION – SEPARATE FIRING SOURCE POWER DISTRIBUTION POINTS	4-138
4.13.3.5	VERIFICATION – FIRING SOURCE CIRCUIT RETURN SIDE ISOLATION	4-138
4.13.3.6	VERIFICATION – PYROTECHNIC CIRCUIT GROUNDING.....	4-138
4.13.3.7	VERIFICATION – PYROTECHNIC WIRING	4-138
4.13.3.8	VERIFICATION – CABLE AND HARNESS DETAILS	4-139
4.13.3.9	VERIFICATION – CABLE SHIELDING	4-139
4.13.3.10	VERIFICATION – INSULATION RESISTANCE	4-139
4.13.3.11	VERIFICATION – TWO FAULT TOLERANT CONDITION.....	4-140
4.13.3.12	VERIFICATION – PYROTECHNIC ELECTROMAGNETIC COMPATIBILITY.....	4-140
4.13.3.13	VERIFICATION – FIRING CIRCUIT SHIELDING.....	4-140
4.13.3.14	VERIFICATION – PROTECTION OF FIRING CIRCUIT SWITCHING DEVICES	4-141
4.13.3.15	VERIFICATION – PROTECTION OF DEVICES THAT CAN COMPLETE FIRING CIRCUIT	4-141
4.13.3.16	VERIFICATION – PYROTECHNIC ELECTRICAL BONDING.....	4-141
4.13.3.17	VERIFICATION – MINIMUM DEVICE WITHSTAND CAPABILITY	4-141
4.13.3.18	VERIFICATION – USE OF BLEED RESISTORS.....	4-141
4.13.3.19	VERIFICATION – ELECTROSTATIC DISCHARGE WITHSTAND	4-142
4.13.4	PYROTECHNIC MECHANICAL CONTAINMENT.....	4-142
4.13.4.1	VERIFICATION – TENSILE TESTING OF METALLIC PARTS.....	4-142
4.13.4.2	VERIFICATION – RETENTION OF THREADED PARTS	4-142
4.13.4.3	VERIFICATION – BLAST CONTAINMENT	4-143
4.13.4.4	VERIFICATION – LOCKED-SHUT TEST.....	4-143
4.13.4.5	VERIFICATION – DESIGN YIELD FACTOR OF SAFETY.....	4-143
4.13.4.6	VERIFICATION – DESIGN ULTIMATE FACTOR OF SAFETY.....	4-143
4.13.4.7	VERIFICATION – CARTRIDGE TORQUE	4-143
4.13.4.8	VERIFICATION - PROOF PRESSURE OF PRESSURE CARTRIDGES AND PROPELLANT ACTUATED DEVICES	4-143

**SSP 51721
Baseline**

4.13.5	AUTO-IGNITION	4-144
4.13.5.1	VERIFICATION - AUTO-IGNITION	4-144
4.13.6	MAXIMUM ENERGY TEST	4-144
4.13.6.1	VERIFICATION - MAXIMUM ENERGY TEST.....	4-144
4.14	DEPLOYMENT, SEPARATION AND JETTISON FUNCTIONS	4-144
4.14.1	RE-ENTRY HUMAN RISK.....	4-147
4.14.1.1	VERIFICATION – RE-ENTRY HUMAN RISK.....	4-147
4.14.2	TRACKABILITY	4-147
4.14.2.1	VERIFICATION – TRACKABILITY	4-148
4.14.3	FRAGMENTATION	4-148
4.14.3.1	VERIFICATION- FRAGMENTATION	4-148
4.14.4	EVA DEPLOY CLEARANCE	4-148
4.14.4.1	VERIFICATION- EVA DEPLOY CLEARANCE.....	4-148
4.14.5	ROBOTIC DEPLOY CLEARANCE	4-148
4.14.5.1	VERIFICATION – ROBOTIC DEPLOY CLEARANCE.....	4-149
4.14.6	CONTROLLABILITY.....	4-149
4.14.6.1	VERIFICATION- CONTROLLABILITY	4-149
4.14.7	RECONTACT AVOIDANCE	4-150
4.14.7.1	KEEP-OUT SPHERE	4-150
4.14.7.1.1	VERIFICATION– KEEP-OUT SPHERE	4-150
4.14.7.2	RESERVED.....	4-150
4.14.7.2.1	RESERVED.....	4-150
4.14.7.3	R-BAR CROSSING	4-150
4.14.7.3.1	VERIFICATION– R-BAR CROSSING	4-150
4.14.7.4	SUBCOMPONENT DEPLOY	4-151
4.14.7.4.1	VERIFICATION– SUBCOMPONENT DEPLOY INITIATION.....	4-151
4.14.7.4.2	SUBCOMPONENT REQUIREMENTS	4-151
4.14.7.5	LOWER ORBIT NON-ISS DEPLOY	4-151
4.14.7.5.1	VERIFICATION– LOWER ORBIT NON-ISS DEPLOY	4-152
4.14.7.6	HIGHER ORBIT NON-ISS DEPLOY	4-152
4.14.7.6.1	VERIFICATION – HIGHER ORBIT NON-ISS DEPLOY	4-152
4.15	HATCHES	4-152
4.15.1	VISUAL INSPECTION OF ADJACENT VOLUME	4-152
4.15.1.1	VERIFICATION – VISUAL INSPECTION OF ADJACENT VOLUME	4-153
4.15.2	INDICATION OF PRESSURE AND TEMPERATURE PRIOR TO HATCH OPENING.....	4-153
4.15.2.1	VERIFICATION – INDICATION OF PRESSURE AND TEMPERATURE PRIOR TO HATCH OPENING.....	4-153
4.15.3	CAPABILITY TO OPERATE FROM BOTH SIDES.....	4-153
4.15.3.1	VERIFICATION – CAPABILITY TO OPERATE FROM BOTH SIDES.....	4-153
4.15.4	PREVENTION OF OPENING PRIOR TO COMPLETE PRESSURE EQUALIZATION.....	4-153
4.15.4.1	VERIFICATION – CAPABILITY TO OPERATE FROM BOTH SIDES.....	4-153
4.15.5	OPERATION BY ONE CREWMEMBER	4-154
4.15.5.1	VERIFICATION – OPERATION BY ONE CREWMEMBER	4-154

**SSP 51721
Baseline**

4.15.6	CO-LOCATION OF TOOLS OR DEVICES NECESSARY FOR HATCH OPERATION.....	4-154
4.15.6.1	VERIFICATION – CO-LOCATION OF TOOLS OR DEVICES NECESSARY FOR HATCH OPERATION	4-154

APPENDIX

A	ACRONYMS AND ABBREVIATIONS	A-1
B	GLOSSARY	B-1
C	OPEN WORK	C-1
D	RATIONALE	D-1

TABLE

3.6-1	VEHICLE LAUNCH/RETURN REQUIREMENTS DOCUMENTS.....	3-6
4.2.2.14	SERVICE LIFE OF A MECHANISM	4-14
4.2.3-1	PRESSURE SYSTEMS CLASSIFICATIONS.....	4-15
4.3.1.2-1	WIRE SIZE DERATING AND CIRCUIT PROTECTION	4-18
4.3.3.4-1	INPUT EMI FILTER ENERGY STORAGE CAPABILITY CALCULATION.....	4-28
4.3.4-1	MEDICAL ELECTRICAL EQUIPMENT TYPES.....	4-32
4.3.4.2-1	MAXIMUM PERMISSIBLE FAULT TOLERANT TOUCH/LEAKAGE CURRENT FOR BIOINSTRUMENTATION.....	4-34
4.3.6-1	CAPACITOR RISK CLASSIFICATION (CRC).....	4-45
4.3.7.3-1	CHARACTERISTICS OF DEPLOYABLE END ITEMS RF TRANSMITTERS	4-54
4.3.7.3-2	CHARACTERISTICS OF DEPLOYABLE END ITEMS RF TRANSMITTERS	4-54
4.3.8.1-1	CHARACTERISTICS OF DEPLOYABLE END ITEMS RF TRANSMITTERS	4-56
4.3.8.1-3	SAFETY VERIFICATION ACTIVITY FOR RF TRANSMITTER HAZARDS.....	4-57
4.5.2-1	HAZARDOUS FUNCTION MONITORING CATEGORIES	4-71
4.7.2-1	LEVELS OF CONTAINMENT/CONTROL AND HAZARD RATINGS	4-89
4.9.1.5-1	NC~52	4-105
4.10.1.1-1	HEAT TRANSFER RATES.....	4-117
4.10.1.2-1	HEAT TRANSFER RATES.....	4-118
4.10.1.2-2	DESIGNATED EVA INTERFACES	4-118
4.10.2.1-1	EDGE, CORNER, AND PROTRUSION CRITERIA – EDGE AND IN-PLANE CORNER RADII*	4-120
4.10.2.1-2	EDGE, CORNER, AND PROTRUSION CRITERIA – PROTRUSIONS AND OUTSIDE CORNERS.....	4-121
4.14-1	BALLISTIC NUMBER FOR DEPLOY DELTA VELOCITY.....	4-145
4.14-2	AVERAGE FRONTAL AREA.....	4-146
4.14-3	BALLISTIC NUMBER CALCULATIONS.....	4-146
C-1	TO BE DETERMINED ITEMS	C-1
C-2	TO BE RESOLVED ISSUES	C-1
D.4.2.3.3-1	MINIMUM FOS FOR PRESSURE SYSTEMS.....	D-8
D.4.3.2.4-1	MEASURES TO PREVENT CREW ELECTRICAL SHOCK HAZARDS.....	D-23
D.4.3.6.1-1	SUCCESS CRITERIA FOR POST CAPACITOR-SCREENING FUNCTIONAL TEST	D-35
D.4.7.2.2.1-1	TOXICITY HAZARD LEVEL (THL) AND HAZARD SEVERITY	D-59
D.4.7.2.2.1-2	FLAMMABILITY HAZARD LEVEL (FHL) AND HAZARD SEVERITY	D-61
D.4.7.2.2.1-3	ECLSS CABIN ENVIRONMENTAL IMPACT RATING	D-62

SSP 51721
Baseline

D.4.7.2.2.1-4	ECLSS HARDWARE IMPACT RATING (E RATING) AND HAZARD SEVERITY.....	D-63
D.4.7.2.4-1	NASA IN-FLIGHT BIOSAFETY LEVEL RATING AND HAZARD SEVERITY.....	D-68
D.4.7.2.5.1-1	PHYSICAL AGENTS AND HAZARD SEVERITY	D-72
D.4.9.2.1-1	INVERSE THERMAL INERTIA FOR COMMONLY USED MATERIALS.....	D-79
D.4.9.2.1-2	CONSTANTS FOR INCIDENTAL (UNPLANNED) ($T \leq 1$ S) CONTACT	D-79
D.4.9.2.1-3	CONSTANTS FOR INTENTIONAL (PLANNED) CONTACT.....	D-80

FIGURE

4.3.2.1-1	TOUCH CURRENT VERIFICATION NETWORK.....	4-22
4.4.1-1	CBCS REQUIREMENTS APPLICABILITY.....	4-59
4.5-1	MUST NOT WORK SYSTEM (INHIBITS).....	4-68
4.5-2	MUST WORK SYSTEM (REDUNDANCY).....	4-68
4.5-3	ACTIVELY SAFED SYSTEM (SHUTDOWN WHEN OUT OF LIMITS)	4-69
4.10.2.1-1	EXPOSED CORNER AND EDGE REQUIREMENTS	4-122
4.10.3.2-1	WORK ENVELOPE FOR GLOVED HAND	4-124
4.12-1	SAFE DISTANCE FOR FIRING THRUSTERS.....	4-130
4.13-1	PYROTECHNIC DEVICE ELECTRICAL AND CONTAINMENT SAFETY REQUIREMENTS.....	4-134
D.4.3.2.4-1	POWER CABLE CONNECTED TO EQUIPMENT	D-24
D.4.3.2.4-2	POWER CABLE CONNECTED TO PORTABLE EQUIPMENT	D-24
D.4.3.2.4-3	POWER CABLE AS AN EXTENSION OR JUMPER.....	D-25
D.4.3.2.4-4	POWER CABLE FLOATING CONNECTOR INTERFACE – BACKSHELL TO GROUND WIRE.....	D-25
D.4.3.2.4-5	POWER CABLE FLOATING CONNECTOR INTERFACE – BACKSHELL TO BACKSHELL	D-26
D.4.9.2.1-1	HOT T_{PM} TOUCH TEMPERATURE LIMITS.....	D-80
D.4.9.2.1-2	COLD T_{PM} TOUCH TEMPERATURE LIMITS.....	D-81

SSP 51721
Baseline

1.0 INTRODUCTION

The International Space Station (ISS) Program (ISSP) establishes the technical requirements for the safe design, development, test and operation of end items. End items include, but are not limited to: ISS hardware/elements (inclusive of Contractor Furnished Equipment (CFE) and Government Furnished Equipment (GFE)), payload/science hardware, Visiting Vehicles (VV), logistics, crew psychological support items, tools, spare instruments and assemblies, including waste. SSP 41000, System Specification for the International Space Station, provides performance and design requirements for ISS and contains many ISS level safety and design requirements that must be considered when developing end item specification documents for ISS end items. SSP 51721, ISS Safety Requirements, exists to further define the safety requirements to be applied to end items developed for ISS.

1.1 PURPOSE

This document is the principal source for technical safety requirements intended to protect the general public, public/private property, flight crews, the ISS, VVs, and other end items from hazards. Although it is not the intent to impede or preclude the use of ISS for the development of science and commercial objectives, it is the responsibility of the end item developer to design and verify in accordance with these requirements.

1.2 SCOPE

Safety requirements applicable to ISS end items are established in this document. These requirements are applicable to pressurized and unpressurized end items transported, transferred, stowed, operated on and/or removed from the ISS, (via return or disposal), as well as for end items with any on-orbit reconfigurations or modifications which could create potentially hazardous conditions.

SSP 51721 supersedes SSP 51700, Payload Safety Policy and Requirements for the International Space Station, and SSP 50021, Safety Requirements Document for the International Space Station Program. The content of interpretation letters from SSP 51700, Appendix E (previously NSTS/ISS 18798) and internal policy letters used by the ISRP have been incorporated as appropriate. Unincorporated requirements from NSTS 1700.7B, which were listed in Appendix D of SSP 51700, were also considered. These letters and unincorporated requirements are a significant lessons learned archival resource for space safety, and are retained for reference to safety requirements not explicitly addressed herein.

The process by which the ISRP assesses compliance with these ISS technical safety requirements is defined in SSP 30599, Safety Review Process. ISS safety reviews are conducted to assess the safety hazards related to the design, operations, and functional capabilities of ISS end items and associated Ground Support Equipment (GSE). SSP 30599 defines the requirements for hazard analysis data submittal content as well as appropriate timing for each of the phased safety review meetings.

To reduce duplication of verification reporting for requirements previously levied via both the safety review and interface/integration processes, the determination of some

SSP 51721

Baseline

requirements applicability (and the associated verification review/closure activities) are now managed through the end item's associated Interface Requirements Document (IRD) or other system specification verification processes (e.g., SSP 57000, Pressurized Payloads IRD, SSP 57003, External Payload Interface Requirements Document, or SSP 50835, ISS Pressurized Volume Hardware Common Interface Requirements Document). These verification transfers are nominally associated with hazards rated as a "marginal" severity. If the IRD requirement is successfully verified, it is considered closed for safety as well. If an IRD exception (with additional safety requirements applicability) is identified, the ISRP must be informed and a decision will be made as to whether there are additional Hazard Report (HR) impacts. In some cases, exceptions may require a Non-Compliance Report (NCR). The IRDs will include a notation as to which requirements are considered safety and would need ISRP acceptance of an exception. The applicable technical disciplines verified via the IRD are identified in Section 4.0 in this document.

The organization in this document is as follows. Section 2.0 contains applicable and reference documents. Section 3.0, in this document, contains general information necessary to understand the philosophy and terminology of the ISRP. It also explains in more detail the applicability of the requirements. Section 4.0 contains the safety requirements. Section 4.1 includes requirements that apply to all end items and the remaining sections address detailed requirements that must be applied and verified as appropriate.

Each requirement includes rationale statements and verification success criteria. The rationale statement explains the purpose of the requirement, provides background as to why the requirement is important to the safety of the ISS and its crew. It also provides information to help determine the applicability of the requirement. The rationale statement may also include definitions or explanations relevant to the terminology used in the requirement and explanation of verification work. The verification information defines what will be necessary to substantiate successful implementation of the requirement.

1.3 PRECEDENCE

Unless explicitly noted otherwise, the safety requirements contained within this document take precedence over any previous/conflicting requirements (including previous versions of SSP 51700 and SSP 50021), other documents, requirements verifications, or verification processes.

1.4 VERB APPLICATION

The verb "shall" is used to indicate a binding requirement that must be implemented and its implementation verified. Use of the verb "will" indicates a statement of fact and is not verified. The verbs "should" and "may" are used for stating non-mandatory goals. "Must" is used in this document to denote items that are required but are verified elsewhere or are included in verification deliverables for a given requirement. "Must" is also used to denote a process that is to be followed.

SSP 51721
Baseline

2.0 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents include specifications, models, standards, guidelines, handbooks, and other special publications. The documents listed in this paragraph are applicable to the extent specified herein.

No Number	Falcon 9 Launch Vehicle Payload User's Guide
6354-GD7100	Cygnus Pressurized Cargo Module to Internally-Carried Payload Interface Definition Document
6472-GD7100	Cygnus Vehicle Interface Definition Document
ANSI Z-136.1	American National Standard for Safe Use of Lasers
ANSI/AIAA S-080	Space Systems – Metallic Pressure Vessels, Pressurized Structures, and Pressure Components
ANSI/AIAA S-081	Space Systems – Composite Overwrapped Pressure Vessels (COPVs)
ASTM E8	Standard Test Methods of Tension Testing of Metallic Materials
IEC 60601	Medical Electrical Equipment
JMR-002	Launch Vehicle Payload Safety Standard
JPR 1800.5	Biosafety Review Board Operations and Requirements
JSC 20793	Crewed Space Vehicle Battery Safety Requirements
JSC 27472	Requirements for Submission of Data Needed for Toxicological Assessment of Chemicals to be Flown on Manned Spacecraft
JSC 28322	International Space Station Acoustic Requirements and Testing for Non-Integrated Equipment
JSC 29353	Flammability Configuration Analysis for Spacecraft Applications
JSC 62809	Human Rated Spacecraft Pyrotechnic Specification

SSP 51721
Baseline

JSC 66202	ISS Power Inverter to 120VAC 60Hz Loads IDD
KNPR 8715.3, Vol. II	KSC Safety Practices Procedural Requirements
MIL-STD-1576	Electro Explosive Subsystem Safety Requirements and Test Methods for Space Systems
MSFC-DWG-20M02540	Assessment of Flexible Bellows and 32L2 Flexible Hose
MSFC-SPEC-626	Test Control Document for Assessment of Flexible Lines for Flow Induced Vibration
NASA/TP-2014-217370	NASA Orbital Debris Engineering Model (ORDEM) 3.0 – User’s Guide
NASA-STD-5020	Requirements for Threaded Fastening Systems in Spaceflight Hardware
NASA-STD-6001	Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures
NASA-STD-8719.14A	Process for Limiting Orbital Debris
NSTS-08123	Certification of Flex Hoses and Bellows for Flow Induced Vibrations
SPX-00036031	Dragon FRAM Payloads Interface Requirements Document
SPX-00036832	CRS Dragon 1 Pressurized Cargo Interface Requirements Document
SSP 30233	Space Station Requirements for Materials and Processes
SSP 30237	Space Station Electromagnetic Emission and Susceptibility Requirements
SSP 30245	Space Station Electrical Bonding Requirements
SSP 30426	Space Station External Contamination Control Requirements
SSP 30558	Fracture Control Requirements for Space Station
SSP 30559	Structural Design and Verification Requirements

SSP 51721
Baseline

SSP 30560	Glass, Window, and Ceramic Structural Design and Verification Requirements
SSP 30599	Safety Review Process
SSP 41000	System Specification for the International Space Station
SSP 41170	Configuration Management Requirements
SSP 41172	Qualification and Acceptance Environmental Test Requirements
SSP 50004	Ground Support Equipment Design Requirement
SSP 50005	International Space Station Flight Crew Integration Standard
SSP 50038	Computer-Based Control System Safety Requirements
SSP 50808	ISS to Commercial Orbital Transportation Services (COTS) Interface Requirements Document
SSP 50833	ISS Cargo Transportation Requirements Document
SSP 50835	ISS Pressurized Volume Hardware Common Interface Requirements Document
SSP 50974	International Space Station System Security Assessment Process
SSP 50989	International Space Station Onboard IT Security Policy
SSP 52000	Payload Interface Definition Documents (IDD)
SSP 52005	Payload Flight Equipment Requirements and Guidelines for Safety-Critical Structures
SSP 57000	Pressurized Payloads IRD
SSP 57003	External Payload Interface Requirements Document
SSP 57011	Payload Verification Program Plan

2.2 REFERENCE DOCUMENTS

The following documents contain supplemental information to guide the user in the application of this document. These reference documents may or may not be specifically cited within the text of this document.

Department of Energy PNNL-18696	Pressure Systems Stored-Energy Threshold Risk Analysis
ANSI Z-136.2 (2012)	Safe Use of Optical Fiber Communication Systems Utilizing Laser Diode and Light Emitting Diode (LED) Sources
ANSI Z-136.6 (2015)	Safe Use of Lasers Outdoors
ISO 16069	Graphical Symbols -- Safety Signs -- Safety Way Guidance Systems (SWGS)
JMR-002	Launch Vehicle Payload Safety Standard
JSC 26626A	EVA Hardware Generic Design Requirement Document (GDRD)
JSC 26895	Guidelines for Assessing the Toxic Hazard of Spacecraft Chemicals and Test Materials
MIL-STD-1553	Digital Time Division Command/Response Multiplex Data Bus
MIL-STD-461	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
MSFC-HDBK-3697	Electrical Bonding Design Guide Handbook
NASA/SP-2010-3407	Human Integration Design Handbook (HIDH)
NASA-HDBK-5010	Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware
NASA-STD-3001	NASA Space Flight Human-System Standard
NASA-STD-5019	Fracture Control Requirements for Spaceflight Hardware
NASDA-ESPC-2857	HTV Cargo Standard Interface Requirements Document

SSP 51721
Baseline

SSP 30256-001	EVA Standard Interface Control Document
SSP 30309	Safety Analysis and Risk Assessment Requirements Document
SSP 30512	Space Station Ionizing Radiation Design Environment
SSP 30560	Glass, Window and Ceramic Structural Design and Verification Requirements
SSP 41162	Segment Specification for the USOS
SSP 50021	Safety Requirements Document for the International Space Station Program
SSP 50094	NASA/RSA Joint Specifications/Standards Document for the ISS Russian Segment
SSP 50621	Generic On-Orbit Stowage Capabilities and Requirements: Pressurized Volume
SSP 50809	ISS To Commercial Orbital Transportation Services (COTS) Interface Control Document for Dragon
SSP 50885	ISS to Commercial Orbital Transportation Services (COTS) Interface Control Document for Cygnus
SSP 51700	Payload Safety Policy and Requirements for the International Space Station
Π32928-103	Requirements for International Partner Cargos Transported on Russian Progress and Soyuz Vehicles
Π32958-106	Requirements for Hardware to be Stored or Operated on the ISS Russian Segment

3.0 GENERAL

3.1 RESPONSIBILITY

3.1.1 ISS PROGRAM

NASA/ISSP is responsible for the overall integrated safety of the ISS and is required to provide assurance that all end items are safe have complied with applicable safety requirements. It is the responsibility of the ISSP to ensure that interaction between end items and the ISS systems does not create a hazard. It is also the responsibility of NASA/ISSP to establish the overall safety requirements of the ISSP.

3.1.2 INTERNATIONAL SPACE STATION SAFETY REVIEW PANEL (ISRP)

Applicability, acceptance, and approval of verifications associated with these safety requirements is the responsibility of the ISRP and will be determined on a case-by-case basis consistent with the hazard potential. The ISRP will review end items for compliance to these requirements for all phases of flight and operations, as well as, assess end item safety verification data.

The ISRP assessment may also include additional end item hazard control/verification audits and safety inspections, as necessary.

3.1.3 END ITEM PROVIDER

The end item provider is responsible for ensuring the safety of hardware, software and operations, by implementing the requirements in this document. The findings must be reported in the applicable flight and/or ground safety assessment, including provision of a certification of flight readiness.

3.1.4 INTERNATIONAL PARTNER

As human spaceflight has expanded to multinational activities through the cooperation in the ISSP, the ISSP recognizes the responsibility and experience of the International Partner (IP) Safety Organizations. It is the responsibility of the IPs to support the ISS safety review process and to certify that all applicable safety requirements have been met with respect to their respective end items. In some cases, the ISSP has developed agreements of internal IP safety organization methodologies and processes that meet or exceed the standards of the NASA ISRP and ensure the safe implementation of the requirements dictated within this document. Such agreements are documented in appropriate ISSP Charters, Memorandums of Understanding or Agreement and/or other documented agreements, as applicable.

3.2 SAFETY ANALYSIS

A safety analysis is performed to identify potential hazards, applicable technical safety requirements, hazard controls/verification methods, and to document safety risk assessment of an end item. This technique is used to anticipate and prevent hazardous circumstances that may potentially result in mishaps.

SSP 51721
Baseline

In providing a method to analyze hazards, the safety analysis accomplishes the following:

- Identifies hazardous conditions and hazardous elements in end item designs,
- Assesses the significance of the identified hazardous condition's effects,
- Provides a basis for establishing system safety preventive measures,
- Provides verification of end item design compliance to specified safety requirements,
- Examines the safety impact of failures,
- Examines the hazard interface,
- Identifies areas for ancillary analysis.

The safety analysis (to be conducted by the end item provider) should be initiated in the design concept phase and be kept current throughout the development phases. The results of this analysis is typically documented in the form of a Safety Data Package (SDP) and should include hazard identification, classification, and resolution, and a record of all safety-related failures. Detailed instructions for conducting a safety analysis are provided in SSP 30599, Safety Review Process. SSP 30309, Safety Analysis and Risk Assessment Requirements Document, additionally provides methodologies and examples to document traditional safety analysis techniques.

3.3 HAZARD CONTROL SCHEME

Hazards are controlled using one of the following methodologies.

3.3.1 DESIGN TO TOLERATE FAILURES (FAILURE TOLERANCE)

Failure tolerance is the safety philosophy that is used to control most hazards and is the preferred approach whenever feasible. The end item must tolerate a minimum number of credible failures and/or operator errors determined by the hazard severity level as listed in Section 4.1.1 without creating a hazard. Vulnerability of common cause failures must be identified and assessed when determining the failure tolerance of an end item. Common cause failures are failures of multiple items or systems due to a single event or common failure mode. Two or more controls to a hazard are independent if no single credible failure, event, or environment can eliminate more than one control.

3.3.2 DESIGN FOR MINIMUM RISK

Design for Minimum Risk (DFMR) is an alternate approach to failure tolerance using the safety related properties and characteristics of the design to reduce the associated risk to an acceptable level. Hazards related to DFMR are controlled by the safety-related properties and characteristics of the design, such as margin or Factors of Safety (FOS) that have been baselined by ISSP requirements.

In some design areas, failure tolerance cannot be achieved in a logical manner without making the design so complex or expensive that it cannot perform its function. In these cases, creating a design that meets a certain FOS, for example, provides a comparable

SSP 51721
Baseline

control to failure tolerance. DFMR can provide the equivalency of either one or two failure tolerance, provided specific design features (as defined by the appropriate engineering technical authority and concurred by the ISRP), are fully implemented and verified. Examples of areas where DFMR is acceptable include structures, glass, pressure vessels, pressurized lines and fittings, pyrotechnic devices, mechanisms in critical applications, material compatibility, and flammability. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the end item provider. Specific details for hazard areas utilizing DFMR are provided in the technical requirements in Section 4.0.

3.4 HAZARD REDUCTION PRECEDENCE SEQUENCE

Action for reducing hazards should be conducted in the following order of precedence.

3.4.1 DESIGN

Hazards should be eliminated from end items when possible. The major goal throughout the design phase is to ensure inherent safety through the selection of appropriate design features, materials and parts selection, and FOS. When elimination is not possible, control and isolation of potential hazards and failure tolerance considerations are to be included in design considerations.

3.4.2 SAFETY DEVICES

Known hazards which cannot be solely controlled by design should be reduced to an acceptable level by incorporating automatic safety devices (for example, pressure relief valves, thermostats that autonomously relieve pressure or inhibit power if over pressurization, overheating, or overcooling of a device results in a potential hazard, etc.).

3.4.3 WARNING DEVICES

When it is not practical to preclude the existence or occurrence of known hazards or to use automatic safing devices, detection capabilities coupled with warning devices, such as alarms, should be employed for the timely detection and annunciation of the hazardous condition and the generation of an adequate warning signal. The use of emergency controls of corrective action for operating personnel to safe or shut down the affected subsystem may also need to be assessed.

3.4.4 OPERATIONAL CONTROLS

Where it is not possible to reduce the magnitude of an existing or potential hazard by design or the use of safety and warning devices, operational controls may be employed to counter hazardous conditions. The primary method used for operational controls is procedures. The next method, flight rules, is normally for aspects that are not contained in a nominal procedure (e.g., thermal requirements, contingency situations, lighting). The last method is crew training. The last method is crew training. It is difficult to reliably verify that the crew understands the intent of the control and it requires proficiency/currency training to maintain the crewmember's ability to perform the operation within the time to effect for the hazard.

3.5 GROUND SUPPORT EQUIPMENT AND GROUND PROCESSING HAZARDS

End items, and their GSE, must be designed to accommodate the expected ground transportation and/or use environments for delivery and handling preflight at the associated launch vehicle ground processing facility.

GSE and ground facility requirements are dependent on the vehicle and/or processing facility. Therefore, the hardware must meet the requirements dictated by the applicable governing documentation in this section. Ground processing of controls to hazards are not considered operational controls (as defined in paragraph 3.4.4), even though there may be a ground operator performing those functions.

NOTE: If the end item is processed at Kennedy Space Center (KSC) prior to shipment to another launch facility, the requirements for KSC and the launch facility apply.

3.5.1 KENNEDY SPACE CENTER LAUNCH FACILITY

The requirements for GSE design and operational safety, including end items processing at KSC facilities (ISS Processing Facility or associated buildings), are contained in KNPR 8715.3, Volume II, KSC Safety Practices Procedural Requirements, and SSP 50004, Ground Support Equipment Design Requirement.

3.5.2 NORTHROP GRUMMAN LAUNCH FACILITY

End items being transported by the Cygnus vehicle must meet the requirements of 6354-GD7100, Cygnus Pressurized Cargo Module (PCM) to Internally-Carried Payload Interface Definition Document (IDD) and/or 6472-GD7100, Cygnus Vehicle Interface Definition Document.

3.5.3 SPACE LAUNCH FACILITY

End items being transported by the Space-X Dragon vehicle must meet the requirements of the Falcon 9 Launch Vehicle Payload User's Guide, as well as SPX-00036832, CRS Dragon 1 Pressurized Cargo Interface Requirements Document, and SPX-00036031, Dragon FRAM Payloads Interface Requirements Document for operations occurring at the Space-X facility.

3.5.4 SOYUZ/PROGRESS LAUNCH FACILITY

End items being transported by the Russian Progress or Soyuz vehicles must meet the requirements of П32928-103, Requirements for International Partner Cargos Transported on Russian Progress and Soyuz Vehicles.

3.5.5 HTV LAUNCH FACILITY

End items being transported by the H-II Transfer Vehicle (HTV) must meet the requirements of JMR-002, Launch Vehicle Payload Safety Standard.

SSP 51721
Baseline

3.6 VISITING VEHICLES

Hardware that is planned for launch and transfer to ISS must meet the requirements in this document. For requirements specific to each launch vehicle, the end item provider must also refer to the appropriate launch/return vehicle requirements documents as listed below.

SSP 50835 and SSP 57000 envelope transport load and environment requirements but other interface definitions are included in the documents in Table 3.6-1.

TABLE 3.6-1 VEHICLE LAUNCH/RETURN REQUIREMENTS DOCUMENTS

Vehicle	Requirements
JAXA HTV	JMR-002, Launch Vehicle Payload Safety Standard NASDA-ESPC-2857, HTV Cargo Standard Interface Requirements Document
RSC-E Soyuz and Progress	П32928-103, Requirements for International Partner Cargos Transported on Russian Progress and Soyuz Vehicles
Cygnus	6354-GD7100, Cygnus Pressurized Cargo Module (PCM) to Internally-Carried Payload Interface Definition Document SSP 50885, ISS to Commercial Orbital Transportation Services (COTS) Interface Control Document for Cygnus SSP 50808, ISS to Commercial Orbital Transportation Services (COTS) Interface Requirements Document SSP 50833, ISS Cargo Transportation Requirements Document (CTRD)
SpaceX Dragon	SPX-00036832, CRS Dragon 1 Pressurized Cargo Interface Requirements Document SPX-00036031, Dragon FRAM Payloads Interface Requirements Document Falcon 9 Launch Vehicle Payload User's Guide SSP 50809, ISS To Commercial Orbital Transportation Services (COTS) Interface Control Document for Dragon SSP 50808, ISS to Commercial Orbital Transportation Services (COTS) Interface Requirements Document
Sierra Nevada Dreamchaser	SSP 50808, ISS to Commercial Orbital Transportation Services (COTS) Interface Requirements Document
Boeing CST-100	SSP 50808, ISS to Commercial Orbital Transportation Services (COTS) Interface Requirements Document

3.7 RUSSIAN SEGMENT OPERATIONS

Additionally, end items that intend to operate in the Russian Segment of ISS must refer to П32958-106, Requirements for Hardware to be Stored or Operated on the ISS Russian Segment and SSP 50094, NASA/RSA Joint Specifications/Standards Document for the ISS Russian Segment, for additional requirements.

3.8 MAINTENANCE/ACCESS

Hazards during maintenance and the on-orbit configuration change of the end item must be considered during the end item design phase and controls must be provided consistent with the hazard severity. Some items to be considered are sharp edges, touch temperatures, stored energy devices, electrical shock, and contamination. A maintenance hazard assessment must consider safe access to maintenance area(s), changes to existing safety features during maintenance, and re-verification of hazard controls following maintenance. Any constraints on the maintenance activity, such as special handling, cool down time of internal components, or required inhibits must be identified.

3.9 DEPLOYABLE/FREE FLYING END ITEMS

For deployable or free flying end items with the potential for retrieval or visitation (examples: failure to deploy with intent to then retrieve or planned intentional return/re-capture of an external free-flyer), they must have the capability to re-verify a safe

SSP 51721
Baseline

configuration, returning any hazardous systems to a safe condition (example, re-establishing required fault tolerance and re-establishment of all required levels of hazard control and verification of safe state.

3.10 REFLIGHT, SERIES, AND MODIFIED END ITEMS

Reflight, series, and modified end items must be reassessed to the requirements in this document prior to flight per SSP 30599.

Reflight end items are defined as those (using the same part number and serial number) that have previously flown on a transportation vehicle or ISS, are unmodified, and are being manifested for reflight.

Series end items are defined as those of the same design and operation as previously flown. Series end items must be built to the same drawings, have the same part number, and use the same processes as the initial end item(s).

Modified end items are defined as those that are of a similar design and operation of other previously flown end items, but with modifications. Dependent upon the degree of these modifications and impacts to the associated baselined/approved safety products (hazard reports, etc.), the “Series and Reflown Equipment” safety review process (as detailed within SSP 30599) may be applicable.

In the event of significant modification to either, the end item or previously approved safety products (including changes from original design or operations, substitution of experiment chemicals/biological samples, or updates to previously approved hazard causes, controls, or verification methods), the ISRP may choose to implement the nominal, phased safety review process per SSP 30599. Coordination with the ISRP is necessary to first confirm agreement to utilize the “Series and Reflown Equipment” process for modified end items.

3.11 CREW HABITABLE MODULES

All requirements in this document are applicable to post-assembly complete ISS modules that are intended to share environment and atmospheric support with the ISS. In addition, when creating a requirement set for volumes that are meant to be attached to ISS and occupied by the crew, requirements should be gathered from the design and capability requirements in SSP 41000 and any related IRD. Items to be considered include communication with ISS, proper ventilation, Caution and Warning (C&W), hatch and window design, etc.

Design features related to habitability must be compatible with and equivalent to those provided by the ISS. This includes items such as radiation protection, toxic offgassing, emergency egress, module isolation, chemical releases and lighting. Monitoring of essential habitability factors must be incorporated in the design as well. These factors include total pressure, smoke detection, and oxygen and carbon dioxide partial pressure.

3.12 VERIFICATION

Test, analysis, demonstration, and inspection are common techniques for verification of features used to control potential hazards. The successful completion of the safety process requires positive feedback of completion results for all verifications associated with a given hazard. In some cases, a design verification is completed via the interface requirement process or equivalent specification document. Verification methods for individual requirements are provided along with each requirement starting in Section 4.2. All verifications listed for each requirement are mandatory unless specified otherwise within the verification section. Final verification methodology/approach will be determined during the phased safety reviews when HRs are approved by the ISRP.

When an operational control is used to control a hazard, the verification is the acceptance of the documentation into the Operational Control Agreement Database (OCAD), NASA Payload Hazard Control Matrix (PHCM), or equivalent IP operational control database, which ensures the agreed to operational control is in place.

Additional flight rules may be established that are not considered hazard controls. These flight rules outline preplanned decisions designed to minimize the amount of real-time rationalization required when anomalous situations occur. These flight rules are not additional safety requirements, but define actions for completion of the ISS objectives consistent with crew safety. End items that choose to meet only the minimum safety requirements potentially limit operational flexibility. Flight rules could be imposed to define actions for crew safety that may impact continued end item operations.

For items with hazard potential during operation, the verification method must be selected such that it verifies the correct operation (example, an end-to-end system assessment as well as component-level verification), as well as verifying the design. Verification planning must take into consideration the possibility that the design could be incorrect; therefore, the intended operation of the end item must be confirmed. It is recommended that verification methods be developed by personnel independent from those designing the system. Test requirements, procedures and apparatus should be derived to confirm intended system performance rather than design. Testing supplemented by analysis can be used to verify a function; however, when this approach is used, separate analysis effort by independent parties are recommended, or conservative safety margins should be applied to single party results.

3.12.1 VERIFICATION METHODS

ANALYSIS (A) - Analysis is the technical evaluation process of using techniques and tools such as mathematical models and computer simulation, historical/design/test data, and other quantitative assessments to calculate characteristics and verify specification compliance. Analysis is used to verify requirements compliance where established techniques are adequate to yield confidence or where testing is impractical. (e.g., testing would cause damage to the end item or the on-orbit environment cannot be adequately duplicated).

DEMONSTRATION (D) - Demonstration is the qualitative determination of compliance with requirements by observation during actual operation or simulation under

SSP 51721

Baseline

preplanned conditions and guidelines. (i.e., observing proper operation or response of the end item during expected flight-like usage).

INSPECTION (I) - Inspection is a physical measurement or visual evaluation of the end item and associated documentation. Inspection is used to verify construction features, drawing compliance, workmanship, and physical condition. The verification of some types of operational controls may also be considered an inspection (example: inspection of documentation) based on a review that the proper procedure, procedure input, flight rule, or crew training has been put in place.

TEST (T) - Test is actual operation of the end item, normally instrumented, under simulated or flight equivalent conditions or the subjection of parts or end item to specified environments to measure and record responses in a quantitative manner. Testing can be at flight equivalent conditions (acceptance testing) or at levels above flight conditions to prove safety margins (qualification testing).

3.13 LIMITED LIFE ITEM VERIFICATION

The periodic re-verification or discontinuation from use of any limited life item used as a hazard control must be considered when documenting the verification process for the end item. The safe design life and safe operational life of an end item must be assessed, and are based on the certified life of safety-related component(s) (e.g., seals, relief valves, regulators, electronic components, batteries, structures). Where applicable, limited life is covered in more detail in the technical requirements.

3.14 SAFETY NON-COMPLIANCE REPORTS

If an end item fails to meet the safety requirements as contained within this document, a safety NCR may be required. Documentation and processing requirements for the non-compliance (including the acceptance of increased risk by the ISS Program) **shall** be in accordance with SSP 30599. **<TBR 3-1>**

3.15 SAFETY CRITICAL

Safety critical refers to a condition, event, operation, process, function or feature with potential to create a critical or catastrophic hazard. A safety critical feature of a design is a feature whose failure or malfunction has the potential to create a critical or catastrophic hazard. This terminology is most often used with structures, circuits, fasteners, software, and mechanisms. An end item with a safety critical feature does not classify the entire end item as safety critical. Safety critical may also be applicable to must-work and must-not-work designs when hazard potential is present. The term safety critical and its usage is further defined for each of the applicable technical categories in Section 4.0. Safety critical features of an end item should be identified early (by Phase I or Phase II Safety Reviews) so that they can be appropriately addressed in the hazard reports and analyses at Safety Reviews. The ISRP, with input from the appropriate engineering and technical disciplines, is the final authority to determine if an end item has safety critical aspects.

SSP 51721

Baseline

3.16 FAIL SAFE

Fail safe is the ability to sustain a failure and retain the capability to safely terminate or control the operation. End Items using fail safe designs typically parallel DFMR type design criteria that implements very specific and proven engineering requirements that ensure the risk or a hazardous event is reduced to a level acceptable to the ISSP. This terminology is used with the design of structure, pressure systems, and fasteners to ensure that after failure of any single structural component, the remaining structural components can withstand the resulting redistributed loads without failure. A fail-safe approach can also be implemented with computer systems, but this typically results in end item inoperability after the first failure.

4.0 SAFETY REQUIREMENTS

4.1 CORE REQUIREMENTS

The following requirements are applicable to all end items launching to, operating on (internal or external), or stowed on ISS. Core requirements are levied by the ISRP based on the unique hazards associated with an end item; therefore, specific verification for these requirements vary based on the specific hazard that is identified. End item hazards, related controls to prevent the hazards, and verification methods will be outlined in the HR and approved by the ISRP.

4.1.1 GENERAL HAZARD SEVERITIES, CONTROLS, & VERIFICATION REQUIREMENTS

4.1.1.1 MARGINAL HAZARD CONTROLS

The end item **shall** be designed to prevent damage to an ISS end item (the loss of which then itself does not constitute a critical or catastrophic hazard) and/or an injury that does not require medical intervention from a second crewmember nor consultation with a flight surgeon (including those injuries that might result in minor crew discomfort).

Rationale

Hazards in this category include the potential for loss of other ISS end items, which do not create additional critical or catastrophic hazardous conditions (e.g., Orbital Replacement Units (ORUs), payloads). For crewmember impacts, the intent of the marginal severity is to assist in understanding/clarification of the lower limit of the critical hazard severity by further defining ranges of a “non-disabling personnel injury” which would be more appropriately classified within the marginal definition. Examples of minor crew injuries nominally associated with the marginal severity could include (but are not limited to: crew discomfort, abrasions, bruises, or superficial burns. Marginal hazards are typically addressed via end item provider internal processes and practices, and in order to document a comprehensive hazard analysis, the end item provider should summarize/reference the results of their analysis within the associated Safety Data Package (SDP). Marginal hazards do not require submission of HRs for formal approval by the ISRP.

4.1.1.1.1 VERIFICATION – MARGINAL HAZARD CONTROLS

Verification is considered successful when an analysis of the end item design, failure/malfunction modes, and operational scenarios shows the end item is designed to not create a marginal hazard. (A)

4.1.1.2 CRITICAL HAZARD CONTROLS

The end item **shall** be designed such that no single failure or single operator error can result in a non-disabling personnel injury or illness, loss of a major ISS end item, loss of redundancy for on-orbit life sustaining function (i.e., with only a single hazard control remaining), and/or loss of use of systems needed for essential logistics (e.g. the Space Station Remote Manipulator System (SSRMS)).

SSP 51721

Baseline

Rationale

For failure tolerance considerations, critical hazards include loss of major ISS end items (e.g., ISS pressurized modules, ISS truss segments, ISS docking/berthing ports, unmanned cargo visiting vehicles) that are not in the critical path for ISS survival or which can be restored through contingency repair. Non-disabling personnel injury or illness includes an injury that requires medical intervention from a second crewmember, and/or consultation with a Flight Surgeon. Compliance with this requirement can be accomplished at the end item level or through a combination of hazard control at the Segment/System levels and end item level. Two verifiable controls must be provided to prevent the occurrence of the identified critical hazard for the end item to be considered single failure tolerant.

4.1.1.2.1 VERIFICATION – CRITICAL HAZARD CONTROLS

Verification is considered successful when an analysis of the end item design, failure/malfunction modes, and operational scenarios shows the end item has an acceptable DFMR approach or two controls against the specific identified hazard such that no single hardware failure or single operator error can result in a critical hazard. (A)

4.1.1.3 CATASTROPHIC HAZARD CONTROLS

The end item **shall** be designed such that no combination of two failures, or two operator errors, or one of each can result in a disabling or fatal personnel injury or illness, and/or one of the following: loss of ISS, loss of a crew-carrying vehicle, or loss of a major ground facility.

Rationale

For failure tolerance considerations, loss of the ISS is to be limited to those conditions resulting from failures or damage to end items for the ISS that render the ISS unusable for further operations, even with contingency repair within the time-to-effect of the hazard or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements. Disabling personnel injury includes the inability to self-rescue. Loss of a crew-carrying vehicle, even during the unmanned timeframe, is also considered catastrophic. End item hazards resulting in potential catastrophic impacts to visiting vehicles (example: interference resulting in ISS collision) are also considered catastrophic. Compliance with this requirement can be accomplished at the end item level or through a combination of hazard controls at the Segment/System levels and end item level. Three verifiable controls must be provided to prevent the occurrence of the identified catastrophic hazard for the end item to be considered two failure tolerant.

4.1.1.3.1 VERIFICATION – CATASTROPHIC HAZARD CONTROLS

Verification is considered successful when an analysis of the end item design, failure/malfunction modes, and operational scenarios shows the end item has an acceptable DFMR approach or three controls against the specific identified hazard such that no combination of two hardware failures, two operator errors, or one of each can result in a catastrophic hazard. (A)

4.1.2 ENVIRONMENTAL COMPATIBILITY

End item hazard controls **shall** be selected and implemented such that all hazards are controlled during and after exposure to all applicable worst-case natural and induced environments for the duration of the end item life.

Rationale

The safety assessment must take into consideration the worst-case environment in which the end item is intended to reside and operate, inclusive of launch and return/disposal. An end item is considered safe when it does not create a hazard and when the identified hazard controls are verified to function in the worst-case natural and induced environments. Worst-case environments consist of all the environments that the end item will be exposed to, including handling, exposure durations, appropriate combinations of thermal, vibration, pressure (including module depressurization), mechanical, cycle life, and others as appropriate. As an example, a pressure system Maximum Design Pressure (MDP) must be determined using the worst-case temperature. End items intending to be used in the United States On-orbit Segment (USOS) airlock during Extravehicular Activity (EVA) preparations would need to consider the worst-case oxygen environment per Section 4.7.1.1. Environments are defined in SSP 41000, SSP 57000, SSP 57003, and SSP 50835. Transport vehicle requirements from Section 3.5 must also be considered in determining the worst-case environment. Hazard controls, especially those of an electrical or electronic nature could be rendered inoperable when exposed to the natural and induced environments of ISS or visiting vehicles. In some cases, the suitability of those controls may require a test or demonstration above and beyond an analysis to show compatibility of the end item hazard controls with the environment. In these cases, the end item developer must inspect (and may be required to provide to the ISRP) these additional verification submittals, such as test and demonstration reports, to confirm the hazard is controlled throughout the life of the end item.

4.1.2.1 VERIFICATION – ENVIRONMENTAL COMPATIBILITY

Verification is considered successful when one or both (as applicable) are completed:

- A. Analysis of the end item design and operational scenarios shows hazards are controlled during and after exposure to the applicable worst-case natural and induced environments for the duration of the end item life. (A)
- B. Inspection, analysis, demonstration, or test results confirm those hazard controls that may be affected by the worst-case environments, as detailed in the hazard analysis, are suitable for the worst-case environment for the duration of the end item life. (I, A, D, T)

4.1.3 SAFE WITHOUT SERVICES

Unless provision of critical services have been negotiated with and agreed to by the ISSP and/or transport vehicles, end items **shall** be designed to maintain failure tolerance or safety margins consistent with the hazard potential without ground or flight

SSP 51721
Baseline

crew intervention in the event of sudden loss or temporary interruption of ISS or transport vehicle provided services.

Rationale

Unless negotiated with/agreed to by the ISSP as a “critical service” an end item must not rely on vehicle-provided services, such as power, to be or remain in a safe state. The end item must remain in a safe state until returned to operation by the ground or flight crew.

4.1.3.1 VERIFICATION - SAFE WITHOUT SERVICES

In cases where provision of critical services have not been negotiated with and agreed to by the ISSP and/or transport vehicles, verification is considered successful when an analysis of the end item design and operational scenarios shows that the end item maintains required failure tolerance or safety margin consistent with the hazard potential without ground or flight crew intervention in the event of sudden loss or temporary interruption of ISS or transport vehicle provided services. (A)

4.1.4 CRITICAL SERVICES

When ISS or transport vehicle services assist in controlling hazards, the integrated system **shall** meet the failure tolerance requirements based on the hazard severity.

Rationale

If a hazard control relies on vehicle services, the combination of controls provided by the vehicle and end item must be adequate to meet the failure tolerance requirements. The SDP and individual HRs must identify those vehicle interfaces used to control and/or monitor hazards.

4.1.4.1 VERIFICATION – CRITICAL SERVICES

Verification is considered successful when an analysis of the end item and integrated system shows that the combination of hazard controls provided by the vehicle and end item meet the failure tolerance requirements based on the hazard severity. (A)

4.2 STRUCTURES

Structural safety requirements are levied to prevent structural failure of hardware, which could lead to hazards to the crew, the ISS, or other end items.

4.2.1 SAFETY CRITICAL STRUCTURES AND FRACTURE CONTROL

End item structure can be defined as safety critical, which means it has the potential to create a critical or catastrophic hazard upon failure. The ISRP, with input from the ISS Structures and Mechanisms Group, is the final authority to determine if an end item has a safety critical structure. End items that meet any of the following conditions are often classified as safety critical (please note this is not a comprehensive list):

- Mounted to unpressurized portion of ISS.
- Launched in the unpressurized section of the visiting vehicle.

SSP 51721

Baseline

- Hard-mounted in the pressurized section of the visiting vehicle.
- Contains a pressurized system as defined in any column of Table 4.2.3-1, Pressure Classifications.
- Contains a hazardous material (see Section 4.7.2, Hazardous Materials for additional information). Please note ziplock bags used as a level of containment for hazardous material are not necessarily considered structure but should be assessed for puncture potential.
- Contains a shatterable material (see Section 4.7.2, Hazardous Materials for additional information).
- End items may be classified as safety critical at the discretion of the ISRP if they are hard-mounted in the pressurized section of the ISS, or include rotating machinery, mechanical stops, or containment devices. As a minimum, fasteners used in the following manner are often classified as safety critical:
 - Used on components that are required to function to prevent a hazard.
 - Used on pressure systems.
 - Used on components used to contain hazardous materials.
 - Used on safety critical mechanisms.
 - Used on safety critical preloaded joints that are required to maintain their preload.
 - Used to restrain external components.
 - Used to restrain a rotating device that has a kinetic energy greater than 14,240 foot-pounds (ft-lbs) (19,310 Joules (J)) and is not contained.
 - Fail safe fasteners (i.e., when a certain number of fasteners can be lost without overall failure). Used for pyrotechnic mechanical containment. Note: Fail-safe fasteners used in other applications are not necessarily considered safety critical.

4.2.1.1 PAYLOAD STRUCTURES AND FRACTURE CONTROL

Payload safety critical structures **shall** be designed in accordance with SSP 52005, Structure Requirements and Guidelines for Safety Critical Payloads.

4.2.1.1.1 VERIFICATION – PAYLOAD STRUCTURES AND FRACTURE CONTROL

Verification is considered successful when all applicable analysis, test and inspections per SSP 52005 are complete.

4.2.1.2 NON-PAYLOAD STRUCTURES

Safety critical structures (non-Payload) **shall** be designed in accordance with SSP 30559, Structural Design and Verification Requirements.

SSP 51721

Baseline

4.2.1.2.1 VERIFICATION - NON-PAYLOAD STRUCTURES

Verification is considered successful when all applicable analysis, test and inspections per SSP 30559 are complete.

4.2.1.3 NON-PAYLOAD FRACTURE CONTROL

Safety critical structures (non-Payload) **shall** be designed in accordance with SSP 30558, Fracture Control Requirements for Space Station.

4.2.1.3.1 VERIFICATION – NON-PAYLOAD FRACTURE CONTROL

Verification is considered successful when all applicable analysis, test and inspections per SSP 30558 are complete.

4.2.2 SAFETY CRITICAL MECHANISMS

Mechanisms are defined as movable mechanical systems, which are operated and if failed, present a hazard to the ISS or crew. Mechanisms which are static (non-operational state) may be considered as structure. A mechanism that can cause – or act as a control for – an identified hazard, is considered safety critical. The ISRP, with input from the ISS Structures and Mechanisms Group, is the final authority to determine if a mechanism is safety critical. Safety critical mechanisms must meet requirements for failure tolerance, such that mechanical failures do not cause or fail to control the associated hazards. The level of required failure tolerance is dependent upon the hazard severity. Preferably, actual physical failure tolerance is provided by redundant design features and the mechanism meets requirement in Section 4.2.2.15, Mechanism Load Redistribution. Redundant designs are evaluated by the ISS Structures and Mechanisms Group and may be required to meet requirements in Sections 4.2.2.1 through 4.2.2.14, as applicable.

Alternatively, equivalent failure tolerance may be possible through the evaluation process known as DFMR. A DFMR designation can be considered to be one or two fault tolerant and must meet requirements in Sections 4.2.2.1 through 4.2.2.14, as applicable. DFMR mechanisms are designed such that credible failure modes have been reliably and effectively controlled as a result of a thorough design, build and test process. Failure modes that must be considered for credibility include, but are not limited to, binding, jamming, inadvertent operation, structural failure, and failure to function. In addition to addressing those failure modes, to be considered DFMR equivalence to two-failure tolerance the mechanism must be robust with relatively few moving parts and demonstrate low sensitivity to environmental and operational conditions. Whether the DFMR designation with equivalence to one or two failure tolerance is granted or not is determined by the ISRP, following receipt of recommendations provided by the ISS Structures and Mechanisms Group. Mechanisms that remain unused when hazard potential is present may be evaluated as structure provided that load requirements for structure are met and failures which could cause inadvertent operation are controlled.

Safety critical mechanisms must also adhere to the structural and fracture control requirements per Section 4.2. All FOS utilized within the mechanisms requirements are

SSP 51721 Baseline

the program-levied FOS specified in those documents. Program FOS requirements apply to all loading conditions including those that occur after credible mechanism failure.

Push in Pull (PIP) pins are small mechanisms and subject to common mechanical and structural failure modes. Most commercial-off-the-shelf pins are not designed to withstand space flight environments and past use has resulted in a wide array of problems with most components of the pins. For this reason, safety critical PIP pins must meet all safety critical mechanism requirements. Due to a history of failures with pip-pins, the DFMR two failure tolerance approach identified above is not applicable. In the past Avibank, (part number 56789) has been approved for safety critical applications and is the preferred PIP pin for EVA crew activities. Interfaces designed to release mechanical degrees of freedom and threaded interfaces that are operated at ISS to control hazard potential, including fasteners, are considered mechanisms.

4.2.2.1 MECHANISMS CLEARANCE

Safety Critical Mechanisms **shall** have static and dynamic clearance (internally and externally) to prevent binding/jamming/seizing and collision with other hardware.

Rationale

External clearance is between the mechanism and any other structure, component, thermal covering, etc. Internal clearance refers to clearance within the mechanism itself (i.e., individual parts/subcomponents of the mechanisms).

The established clearance requirements must account for the following:

- *Manufacturing, assembly, and alignment tolerances.*
- *Temperature.*
- *Temperature gradients.*
- *Vibration.*
- *Deflections due to external loads, including gravity effects.*
- *Deflections due to operational loads.*
- *Deflections due to pressurization or depressurization effects, including thermal blanket billowing.*
- *Motion of cable harnesses, tubing, and sensor wiring.*
- *Environments arising from transportation.*
- *Adjustability and rigging of the mechanism parts.*

Maintaining clearances within and around mechanisms is necessary both to maintain proper mechanism function and to prevent the mechanism from causing problems with other systems.

SSP 51721

Baseline

The necessary clearances required have to be established to enable design and verification, and the design has to maintain those clearances. It is difficult to specify a minimum clearance that works for all applications. The appropriate clearance for the particular application must be determined by taking into consideration of the above factors.

Many of the factors affecting the overall (dynamic) clearance are not present when inspections are performed; these effects have to be accounted for and included in the static clearance specified on the drawings. Tolerancing, thermal expansion effects, and deflections are the most important factors to consider in establishing the clearances. Thermal blanket billowing behavior is notorious for causing unexpected interferences with mechanisms. Additional factors could be appropriate for consideration based on individual applications. Motion under transportation loads is often not considered, but clearances in this situation are also important.

Appropriate design provisions include, but are not limited to, dual rotating surfaces or other mechanical redundancies, robust strength margins such that self-generated internal particles are precluded, shrouding and debris shielding, proper selection of materials and lubrication design to prevent friction welding or galling.

4.2.2.1.1 VERIFICATION – MECHANISMS CLEARANCE

Verification is considered successful when the following are completed: A and (B or C):

- A. Inspection of drawing and as-built hardware reflects clearance. (I)
- B. Inspections of all identified critical clearances on the as-built hardware after installation or assembly to ensure the existence of as-designed initial clearances that are sufficient to ensure clearance under flight conditions. A measurement of each clearance is to be made when the mechanism is in the configuration that generates the closest proximity to other structure/hardware and shows no opportunity for contact. (I)
- C. If clearances cannot be directly measured, positional measurements that allow clearance to be calculated can be substituted. (A)

4.2.2.2 MECHANISMS TOLERANCES

Dimensional analysis of safety-critical mechanical systems **shall** account for the following:

1. Manufacturing, assembly, and alignment tolerances.
2. Temperature and temperature gradient-induced deformations.
3. Static and dynamic load-induced deflections.
4. Deflections due to pressurization or depressurization effects, including thermal blanket billowing.
5. Motion of cable harnesses, tubing, and sensor wiring.
6. Full range of adjustability of the mechanism parts.

SSP 51721
Baseline

Worst-case conditions to be considered include but are not limited to:

- Thermally induced in-plane distortions.
- Thermally induced out-of-plane distortions.
- Differential thermal growth and shrinkage.
- Vibration, load-induced deflections (external and operational loads).
- Adjustability and rigging of the mechanism parts.

Rationale

Dimensional analysis is important for ensuring external clearances and proper mechanism function. Establishing the tolerances via a documented dimensional analysis helps determine the effects of tolerances and other factors, and allows for easy review and revision later. Tolerances should encompass worst-case conditions. These conditions cover common causes of mechanism failure. ASME Y14.5 and ISO 2768 can be used to assist in tolerance determination.

4.2.2.2.1 VERIFICATION – MECHANISMS TOLERANCES

Verification is considered successful when the dimensional analysis documentation addresses items 1-6 listed in the requirement. (A).

4.2.2.3 MECHANISMS LUBRICATION

Safety critical mechanisms that have contacting surface motion **shall** be lubricated.

Rationale

Lubrication is one of the most important factors in successful mechanism design and operation. All contacting surfaces that are expected to move with respect to one another need to be lubricated in some way, regardless of material choices, load, or life requirements. Use of dissimilar metallic materials for the wear surfaces, though strongly encouraged, is not an equivalent to or substitute for lubrication and does not meet the intent of this requirement. A successfully complete life test per Section 4.2.2.14.1 also contributes to verification of this requirement.

Additional rationale for this requirement can be found at Appendix D.4.2.2.3.

4.2.2.3.1 VERIFICATION - MECHANISMS LUBRICATION

Verification is considered successful when each of the following are completed:

- A. Analysis that reflects compatibility between the lubricant and interfacing materials, other lubricants used in the design, and the worst-case environments. (A)
- B. Analysis that reflects there is enough lubricant to meet the operational lifetime of the mechanism based on the environments the mechanism is expected to encounter. (A)
- C. Inspection of drawing reflects correct lubrication. (A)

4.2.2.4 MECHANISMS SPRINGS

Springs in applications where a spring failure will result in a hazard **shall** be failure tolerant unless spring failure can be shown to be non-credible.

Rationale

Springs are a common mechanism component as well as a common source of problems. Spring failure tolerance provides for increased mechanism reliability. In rare cases, spring failures can be declared non-credible by showing compliance with a comprehensive set of structural, life and fracture control requirements, in which case this requirement is not applicable.

Additional rationale for this requirement can be found at Appendix D.4.2.2.4.

4.2.2.4.1 VERIFICATION – FAILURE TOLERANT MECHANISM SPRINGS

Verification is considered successful when the following are completed: A or B

- A. Inspection of design that reflect redundant springs. (I)
- B. Performance analysis confirms spring failure tolerance by showing that the spring can meet performance requirements after fracture. (A)

4.2.2.5 MECHANISM ACTUATION FORCE/TORQUE STALL

The design of the safety critical mechanism **shall** maintain a positive margin of safety for an actuation force/torque stall condition at any point of travel.

Rationale

Many situations can cause a mechanism to reach its stall torque or force. Designing the mechanism with strength to withstand stall ensures that the mechanism is undamaged by a stall condition that may otherwise damage the mechanism and preclude recovery of mechanism functionality. The usual FOS apply.

4.2.2.5.1 VERIFICATION-MECHANISM ACTUATION FORCE/TORQUE STALL

Verification is considered successful when the structural analysis reflects positive margin of safety for actuation force/torque stall condition. (A)

4.2.2.6 MECHANISM MECHANICAL STOPS

The design of the safety critical mechanism components **shall** maintain a positive margin of safety with the appropriate FOS applied when subjected to worst-case transient loads at the mechanical stop.

Rationale

The impact against the mechanical stop can create elevated loads on other parts of the mechanism in addition to the stops themselves, and these loads have to be accounted for in the structural analysis. The contact of mechanical stops is often rapid enough that static analysis approaches can lack sufficient conservatism so a dynamic analysis is necessary.

SSP 51721
Baseline

Additional rationale for this requirement can be found in Appendix D.4.2.2.6.

4.2.2.6.1 VERIFICATION - MECHANISM MECHANICAL STOPS

Verification is considered successful when the structural analysis reflects positive margin of safety for worst-case transient loading conditions. (A)

4.2.2.7 MECHANISM INADVERTENT IMPACT LOADS

Safety critical mechanisms design **shall** maintain a positive margin of safety against strength and deflection for inadvertent impact loads where a hazard may result.

Rationale

Mechanism deformation due to impact loads can result in binding/jamming condition or inadvertent mechanism operation. Analysis of these cases must use full FOS. Impact loads include those resulting from ISS remote manipulator system, payload operations, and EVA/Intravehicular Activity (IVA) crew operations.

4.2.2.7.1 VERIFICATION - MECHANISM INADVERTENT IMPACT LOADS

Verification is considered successful when the structural analysis reflects positive margins against strength and deflection on inadvertent impact loads to preclude hazards. (A)

4.2.2.8 MECHANISM POSITIVE INDICATION OF STATUS

The safety critical mechanism design **shall** provide positive indication that the mechanism has achieved its desired state.

Rationale

The ability to verify that the mechanism is functioning in the proper state is critical to identifying and controlling failures. Without knowledge of status, a hazardous, failed condition may unknowingly exist. State indication can be accomplished in different ways including electrically, tactility or visually.

Additional rationale for this requirement can be found at Appendix D.4.2.2.8.

4.2.2.8.1 VERIFICATION - MECHANISM POSITIVE INDICATION OF STATUS

Verification is considered successful when each of the following are completed:

- A. Review of design confirms mechanism incorporates state indications (I)
- B. Testing confirms mechanism state indicators provide accurate state indications (T)

4.2.2.9 MECHANISM STARTING TORQUE/FORCE MARGINS

Safety critical mechanism design **shall** have a margin of 1.0 or greater for the starting torque or force at points of travel for worst-case conditions.

SSP 51721

Baseline

Rationale

Torque and force margins are intended to ensure that the mechanism retains reserve torque or force capability that can be applied in the event of an unforeseen effect that reduces motive force from the mechanism. Therefore, as with any other capability of the mechanism, the minimum torque or force margin must be verified as intact prior to placement into service.

Additional rationale for this requirement can be found in Appendix D.4.2.2.9.

4.2.2.9.1 VERIFICATION - MECHANISM STARTING TORQUE/FORCE MARGINS

Verification is considered successful when each of the following are completed:

- A. Acceptance test that reflects margin of 1.0 or greater. (T)
- B. Analysis that reflects margin of 1.0 or greater when considering the worst-case environmental conditions. (A)

4.2.2.10 MECHANISM DYNAMIC TORQUE/FORCE MARGINS

Safety Critical Mechanism design **shall** have a margin of ≥ 0.25 for the dynamic torque or force at mechanism contact points of travel for worst-case conditions.

Rationale

Torque and force margins are intended to ensure that the mechanism retains reserve torque or force capability that can be applied in the event of an unforeseen effect that reduces mechanism dynamic motive force. Therefore, as with any other capability of the mechanism, the minimum torque or force margin must be verified as intact prior to placement into service.

4.2.2.10.1 VERIFICATION - MECHANISM DYNAMIC TORQUE/FORCE MARGINS

Verification is considered successful when each of the following are completed:

- A. Acceptance test that reflects margin of 0.25 or greater. (T)
- B. Analysis that reflects margin of 0.25 or greater when considering the worst-case environmental conditions listed above. (A)

4.2.2.11 MECHANISM HOLDING FORCE MARGINS

Safety critical mechanism design **shall** accommodate a margin of ≥ 1.0 for holding configuration(s) in worst-case conditions.

Rationale

Torque and force margins ensure that the mechanism retains reserve torque or force capability that can be applied in the event of an unforeseen effect that reduces holding force from the mechanism. Therefore, as with any other capability of the mechanism, the minimum torque or force margin must be verified as intact prior to placement into service.

SSP 51721
Baseline

Additional rationale for this requirement can be found in Appendix D.4.2.2.11.

4.2.2.11.1 VERIFICATION – MECHANISM HOLDING FORCE MARGINS

Verification is considered successful when each of the following are completed:

- A. Acceptance test that reflects margin of 1.0 or greater. (T)
- B. Analysis that reflects margin of 1.0 or greater when considering the worst-case environmental conditions listed above. (A)

4.2.2.12 MECHANISM CONTAMINATION

Safety critical mechanism cleanliness levels **shall** be established and maintained to prevent contamination during fabrication, handling, transportation, storage, and flight that results in degradation or failure of the mechanism or other safety-critical hardware.

Rationale

Foreign Object Debris (FOD) is a concern for mechanisms and could cause binding/jamming/seizing. Cleanliness requirements help ensure that FOD does not interfere with mechanism function. Mechanism fabrication and handling must be completed in a clean environment. Attention must be given to avoiding non-particulate (chemical) as well as particulate air contamination.

4.2.2.12.1 VERIFICATION – MECHANISM CONTAMINATION

Verification is considered successful when cleanliness levels have been provided and justified by the hardware provider and the levels have been approved by the ISS Structures and Mechanisms Group. (I)

4.2.2.13 MECHANISM FUNCTION

The end item safety critical mechanism **shall** function without creating a hazard in the worst-case environment.

Rationale

End items with safety critical mechanism must ensure that mechanical function works as intended and does not impact ISS.

Additional rationale for this requirement can be found in Appendix D.4.2.2.13.

4.2.2.13.1 VERIFICATION - MECHANISM FUNCTION

Verification is considered successful when each of the following are completed:

- A. Acceptance tests show mechanism function without creation of a hazard. (T)
- B. Qualification tests show mechanism function without creation of a hazard. (T)

4.2.2.14 MECHANISM LIFE

End item safety critical mechanism design **shall** have an expected life as specified in Table 4.2.2.14-1.

TABLE 4.2.2.14-1 SERVICE LIFE OF A MECHANISM

Hazard Severity	Expected Life
Critical	2X Service Life
Catastrophic	4X Service Life

Rationale

All functions of the mechanism have to be life tested to verify life of the system, including back-up or redundant provisions; however, the appropriate number of cycles to be applied to the back-up or redundant provisions should be consistent with the possible failure scenarios. Typical design life concerns include fatigue limits, Deterioration of lubrication, excessive wear, and deterioration during extended quiescent periods.

Additional rationale for this requirement can be found in Appendix D.4.2.2. 14.

4.2.2.14.1 VERIFICATION - MECHANISM LIFE

Verification is considered successful when expected life testing demonstrates mechanism life is greater than the appropriate factor of the service life. (T)

4.2.2.15 MECHANISM LOAD REDISTRIBUTION

Positive margins of safety under the redistributed loading conditions **shall** be maintained for the resultant configurations of credible safety critical mechanism failures (one or two depending on the hazard category).

Rationale

Whether a particular failure is considered credible will be determined by the ISRP, with input from the appropriate subject matter expert. This minimizes the number of structural configurations to be analyzed.

Additional rationale for this requirement can be found in Appendix D.4.2.2. 15.

4.2.2.15.1 VERIFICATION - MECHANISM LOAD REDISTRIBUTION

Verification is considered successful when the structural analysis reflects two-failure tolerance against load redistribution caused by credible failures. (A)

4.2.3 PRESSURE SYSTEMS

Pressure systems can be classified as low pressure or high pressure and can contain fluids or gasses that are considered either hazardous or nonhazardous. Low pressure system are classified as either low energy fail-safe or sealed containers. A high pressure system has internal pressure >100 pounds per square inch absolute (psia) or stored energy greater than 14,240 ft-lbs (19,310 J). Maximum Design Pressure (MDP)

**SSP 51721
Baseline**

derivations are necessary to understand the capabilities of the pressure systems to preclude rupture hazards. Table 4.2.3-1 describes pressure systems classifications and document references.

TABLE 4.2.3-1 PRESSURE SYSTEMS CLASSIFICATIONS

Classification	Sealed Container with no Analysis/ Testing	Sealed Container	Low Energy Fail Safe Pressure Systems	High Pressure Systems	
				Pressure Vessel	Lines, Fittings, Components
Classification Criteria	<ul style="list-style-type: none"> • ≤22 psia • ≤14,240'ft-lbs • Toxicity Hazard Level (THL) 0³ 	<ul style="list-style-type: none"> • >22 and ≤ 100 psia • ≤14,240'ft-lbs • THL 0³ 	<ul style="list-style-type: none"> • ≤100 psia • THL 0³ • <1000 Ft-lbs • Meets DOT Standards 	<ul style="list-style-type: none"> • 100 psia • >14,240 ft-lbs • Includes metallic, composite, dewars, cryostats, pressure stabilized tanks • THL>0 with appropriate levels of containment 	<ul style="list-style-type: none"> • 100 psia • >14,240 ft-lbs • Includes metallic, composite, dewars, cryostats, pressure components • THL>0 with appropriate levels of containment
SSP 51721 Reference	4.2.3.1	4.2.3.1	4.2.3		4.2.3.3

Note: Additional levels of containment would be required for higher THL material.
This table is not an all-inclusive list of classification criteria. <TBR 4-2> and <TBR 4-3>

Not all pressure systems are high energy pressure systems that fail catastrophically. Many pressure systems are small, low energy, fail-safe, pressure systems. Fail Safe is a condition where, after failure of a single individual pressurized component, the remaining components (considered unflawed) can withstand the redistributed pressure, and the failure will not release components or if contents are released, they will not cause an over-pressurization of the system, a hazardous environment, or damage other hardware including the Environmental Control and Life Support System (ECLSS). If the pressure system is determined to be low energy and fail-safe (per Table 4.2.3-1), then it can be declared as a low energy pressure system with a system description in the SDP and a Rupture/Leakage of Pressure System HR is not necessary.

4.2.3.1 PRESSURE SYSTEMS – SEALED CONTAINER

Sealed containers **shall** provide positive margins of safety.

Rationale

A sealed container consists of only one pressurized compartment or vessel and has Maximum Design Pressure (MDP) is > 22 psia and ≤100 psia <TBR 4-3>, Containing non-hazardous materials, and stored energy ≤ 14,240 ft-lbs. When sealed container has an MDP ≤ 22 psia, no additional testing or analysis is required. When the MDP is greater than 100 psia, it is considered a high pressure component and high pressure system safety requirements are applicable. End items that are comprised of more than one pressurized component are considered a pressure system. <TBR 4-4>

Additional rationale for this requirement can be found in Appendix D.4.2.3.1.

SSP 51721

Baseline

4.2.3.1.1 VERIFICATION – SEALED CONTAINER

Verification is considered successful one of the following is provided: <TBR 4-3>

- A. An analysis shows that the container has a positive margin against burst when a factor of 2.5 on MDP is used. (A)
- B. The flight unit is successfully proof tested to 1.5 times the MDP or greater. (T)

4.2.3.2 PRESSURE SYSTEMS - PRESSURE VESSELS

A pressure vessel is a container designed primarily to sustain internal pressure, but which can also sustain some vehicle-induced loads. More specifically, a container that stores pressurized fluids or gases and: (1) Contains stored energy of >14,240 ft-lbs (19,310 J) based on adiabatic expansion of a perfect gas; or (2) Contains a gas or liquid in excess of 15 psia which will create a hazard if released. Verification is based on the type of pressure vessel used.

System integrity is necessary to be maintained during exposure to all applicable environments and for the entire service life of the pressure vessel. <TBR 4-3>

Additional rationale for this requirement can be found in Appendix D.4.2.3.2.

4.2.3.2.1 PRESSURE SYSTEMS – PAYLOAD PRESSURE VESSELS

Payload pressure vessels **shall** be designed in accordance with SSP 52005, Structure Requirements and Guidelines for Safety Critical Payloads.

4.2.3.2.1.1 VERIFICATION - PRESSURE SYSTEMS – PAYLOAD PRESSURE VESSELS

Payload verification is considered successful when all applicable analysis, tests, and inspections per SSP 52005 are complete.

4.2.3.2.2 PRESSURE SYSTEMS – SYSTEM PRESSURE VESSELS

Systems pressure vessels **shall** be designed in accordance with SSP 30558, Fracture Control Requirements for Space Station and SSP 30559, Structural Design and Verification Requirements.

4.2.3.2.2.1 VERIFICATION - PRESSURE SYSTEMS – SYSTEM PRESSURE VESSELS

Systems verification is considered successful when all applicable analysis, tests, and inspections per SSP 30558 and SSP 30559 are complete. (A, I, T)

4.2.3.3 PRESSURE SYSTEMS PRESSURIZED LINES, FITTINGS AND COMPONENTS RESTRAINT

Pressurized lines, fittings and components **shall** be restrained.

Rationale

SSP 51721
Baseline

Restrained to protect the components pressurized lines, fittings and components is necessary prevent injury to the crew and/or damage to adjacent hardware due to hose whip during normal operations.

4.2.3.3.1 VERIFICATION PRESSURIZED LINES, FITTINGS AND COMPONENTS RESTRAINT

Verification is considered successful when each of the following are completed:

- A. Design includes restraint of pressurized flex hoses, fittings, components, and lines with delta pressure. (I)
- B. Design prevents excessive/deformational component loads and displacements with a positive margin of safety. (A)

4.3 ELECTRICAL

Electrical safety requirements are levied to prevent hazards such as electric shock, molten metal, toxic material release, fire, touch temperature hazards and electronic interference. These requirements include design and operational considerations for the selection of wiring and circuit protection, connector mate/demate, biomedical instrumentation, batteries, capacitors, Electromagnetic Interference (EMI), Electrostatic Discharge (ESD), corona, and Radio Frequency (RF) signals.

Circuits used in the control of critical and catastrophic hazards are safety critical circuits. It is important to note that a safety critical circuit has certain implications that may not apply in every requirement case.

There is differentiation between circuits as part of a hazard control and the circuits' ability to function in the ISS environment (i.e. ISS Electromagnetic Effects (EME)). For example, when a bimetallic thermostat is used to control a touch temperature hazard – it is safety critical, but the thermostat would not be subject to EME susceptibility testing.

Safety critical circuits are:

- Circuits whose loss of function could result in a critical or catastrophic hazard, or
- Circuits whose malfunction or degradation of performance could result in a critical or catastrophic hazard, or
- Circuits that control inhibits whose loss could result in critical or catastrophic hazards, or
- Circuits that control inhibits whose loss could result in critical or catastrophic hazards, or
- Circuits that are inhibited or not operational to prevent operation a critical or catastrophic hazard.

4.3.1 ELECTRICAL SYSTEMS

Electrical Systems include requirements for wire derating, circuit protection, direct current return leg inhibit, and safety critical circuit independence. <TBR 4-6>

**SSP 51721
Baseline**

4.3.1.1 RESERVED

4.3.1.2 WIRE DERATING

Wire size **shall** be derated such that maximum upstream current capability of the Electrical Power Consuming Equipment (EPCE) or upstream EPS does not exceed the values defined in Table 4.3.1.2-1.

TABLE 4.3.1.2-1 WIRE SIZE DERATING AND CIRCUIT PROTECTION

	Column A		Column B		Column C
	Maximum Continuous Current Rating (100% of Circuit Protection Rating)		130% of Circuit Protection Rating (or worst case upstream current >1 second)		Current Limits to meet touch temperature limited for crew accessible wire/cables
	IVA	EVA	IVA	EVA	IVA
Wire Size (AWG)	Upstream Current Protection Limit for a Single Wire (I _{sw}) (amps) <small>1, 2, 3, 7</small>	Upstream Current Protection Limit for a Single Wire (I _{sw}) (amps) <small>1, 5, 6, 7</small>	Maximum Allowed Smart Short Current (amps) <small>1, 2, 4</small>	Maximum Allowed Smart Short Current (amps) <small>1, 4, 5</small>	Maximum Wire Current < 45C/113F ⁷
26	3.8	3.4	4.9	4.4	1.7
24	5.4	4.7	7.0	6.1	2.7
22	7.4	6.5	9.6	8.4	3.5
20	10.0	8.8	13.0	11.4	4.8
18	13.2	11.6	17.2	15.1	6.0
16	15.0	13.3	19.5	17.3	7.6
14	20.0	18.0	26.0	23.4	9.5
12	29.0	25.0	37.7	32.5	12.8
10	40.0	34.8	52.0	45.2	17.7
8	63.0	56.0	81.9	72.8	29.7
6	92.0	80.0	119.6	104.0	43.1
4	120.0	110.0	156.0	143.0	58.6
2	170.5	150.5	221.6	195.6	90.9
1/0	260.0	220.5	338.0	286.6	108

Note 1 – Wire size deratings listed are for wire insulation rated for 200°C.

Note 2 - These currents are for Intravehicular Activities (IVA) wires on-orbit in cabin ambient at 22°C (72°F).

Note 3 – IVA Wire with these currents will reach 118°C (242°F). The wires are not to be accessible to the crew. For IVA crew accessible wires, use Column C.

Note 4 - This current is the maximum sustained fault current allowable by the circuit protection device. Wire temperature could reach 185°C (365°F).

Note 5 - These currents are for IVA wires in a vacuum at 94°C (200°F) ambient.

Note 6 - Wire with these currents will reach 147°C (295°F) and are not to be accessible to the IVA crew.

Note 7 –It is necessary that wire bundle derating account for maximum continuous current rating and current limits.

Note 8 - Bundle derating may not be necessary if bundled power wiring is not significantly loaded. When wire is bundled, maximum design current for each individual wire is derated according to the following:

For N < 15 For N > 15
 Bundled Wire (IBW) = Single Wire (ISW) × (29 - N)/28
 IBW = (0.5) × ISW
 Where: N = number of wires
 IBW = current, bundle wire
 ISW = current, single wire

Rationale

Electrical current passing through wire (if not controlled or limited for specific wire size) can generate excessive heat which could result in insulation pyrolyzation or safety critical circuit damage. This damage can cause crew toxicity hazards, crew touch temperature hazards, or propagation to other wires in a bundle resulting in loss of safety critical circuits.

4.3.1.2.1 VERIFICATION - WIRE DERATING

Verification is considered successful when each of the following are completed:

- A. Analysis of design confirms wire sizes are chosen based on the maximum nominal current draw and the upstream current protection limit of the primary upstream protection device as shown in Table 4.3.1.2-1, Column A, B, and C. (A)
- B. Inspection of as-built hardware confirms EPCE wire sizes reflects the design per approved drawings. (I)

4.3.1.3 CIRCUIT PROTECTION

Circuit protection devices **shall** prevent sustained short currents from exceeding derated single wire current defined in Table 4.3.1.2-1, Column B.

Rationale

Circuit protection devices include fuses, circuit breakers (thermal or electronic), current limiting circuits, positive temperature coefficients (PTC) thermistors, and/or Remote Power Controllers (RPCs). Circuit protection can be provided by other upstream devices that are not in the EPCE (e.g. ISS EPS devices).

Additional rationale for this requirement can be found in Appendix D.4.3.1.3.

4.3.1.3.1 VERIFICATION – CIRCUIT PROTECTION

Verification is considered successful when each of the following are completed:

- A. Analysis of design to show that circuit protective devices prevent currents in excess of Table 4.3.1.2-1, Column B, and Column C (when wires, bundles, or cables are crew accessible). (A)
- B. Inspection shows that circuit protective devices are provided that prevent currents in excess of Table 4.3.1.2-1, Column B. Circuit protection can be provided by upstream devices that are not in the EPCE. (I)
- C. For end items which rely on ISS upstream circuit protective devices, verification is considered successful when each of the following are completed:
 - C1. Analysis of design shows that the wiring used is compliant with wire derating criteria of Table 4.3.1.2-1, Column B, and Column C (when wires, bundles, or cables are crew accessible) based on the ISS upstream circuit protective device limits. (A)
 - C2. Inspection of as-built hardware confirms EPCE wire sizes reflects the design per approved drawings. (I)

4.3.1.4 DC CIRCUIT ELECTRICAL INHIBITS USED TO PREVENT CATASTROPHIC HAZARDS

When the prevention of catastrophic hazards requires the interruption of direct current (dc) currents, the end item **shall** provide two independent inhibits that interrupts current in the positive (hot) lead and one inhibit that interrupts current in the negative (return) lead.

Rationale

Electronics boxes could contain numerous “inadvertent” energized sources, loose wires, washers, and debris due to workmanship errors and improper routing of wires in boxes. Inadvertent motion of mechanical systems or activation of transmitters using Direct Current (DC) circuits may have catastrophic consequences.

Additional rationale for this requirement can be found in Appendix D.4.3.1.4.

4.3.1.4.1 VERIFICATION – DIRECT CURRENT (DC) CIRCUIT ELECTRICAL INHIBITS USED TO PREVENT CATASTROPHIC HAZARDS

Verification is considered successful when each of the following are completed:

- A. Analysis of design drawings show at least three independent inhibits interrupt power to the catastrophic function controlled by Direct Current (DC) circuits, of which one of the inhibits is in the ground return. (I)
- B. Testing demonstrates that each inhibit independently removes power from the end item function. (T)
- C. Inspection of as-built flight hardware to approved design drawings for three (3) independent inhibits interrupt power to the catastrophic function, with each inhibit independently controlled by DC circuits, of which one inhibit is in the ground return leg (I)
- D. Inspection of procedures show
 - 1. Inhibits are in place to protect from the catastrophic hazard and
 - 2. Commands that enable (close) an inhibit are labeled in appropriate safety documentation and procedures. (I)

4.3.1.5 SEPARATION OF REDUNDANT SAFETY CRITICAL CIRCUITS

Redundant safety critical circuits **shall** be physically separated.

Rationale

As a result of increased emphasis on the routing of redundant safety critical circuits, it is necessary to ensure separation of redundant paths to eliminate common cause failures.

Additional rationale for this requirement can be found in Appendix D.4.3.1.5.

4.3.1.5.1 VERIFICATION – SEPARATION OF REDUNDANT SAFETY CRITICAL CIRCUITS

Verification is considered successful when A and B are completed:

SSP 51721

Baseline

- A. Inspection shows as built hardware is as designed per drawings confirms redundant safety critical circuits are routed in separate cable bundles via different routing paths, which are separated. (I)
- B. Analysis shows physical barrier prevents failures in one safety critical circuit from propagating to adjacent safety critical circuits, or safety critical circuit is separated by the maximum possible distance in the connector to eliminate bent pins from bypassing inhibits or shorting power sources used for hazardous functions. (A)

4.3.2 ELECTRIC SHOCK

Electrical shock is considered a catastrophic hazard when voltages are $\geq 32V$ dc/rms. Electrical Shock considerations are necessary for the safety of the crew in the current spacecraft design since crew accessible conductible surfaces, ISS electrical power systems (EPS), electrical power consuming equipment (EPCE), and batteries can be a source of electrical shock hazards. These considerations include EPS requirements for non-patient electrical current leakage, protective covers for electrical power conductors/terminations, electrical bonding/grounding, and electrical isolation requirements. These requirements apply to all dc and ac voltages (dc/rms). Crew bioinstrumentation electrical requirements are defined in Section 4.3.4.

Additional rationale for this requirement can be found in Appendix D.4.3.2.

4.3.2.1 GENERAL EPCE WITH NO DIRECT INTERFACE TO MEDICAL EQUIPMENT

Touch currents for general EPCE $\geq 32V$ dc/rms that do not directly interface with medical equipment **shall** be $\leq 0.5mA$. **<TBR 4-7>**

Rationale

EPCE designs control leakage currents and touch currents at crew accessible surfaces that can result in electrical shock to the crew. A preferred alternative to EPCE leakage current controls can be EPCEs that provide three hazard controls through compliance with the bonding, grounding, and electrical isolation design requirements of Section 4.3.2.4, which can also satisfy the leakage current requirement. The definition of touch current is provided in Appendix D.4.3.2.1.

Additional rationale for this requirement can be found in Appendix D.4.3.2.1.

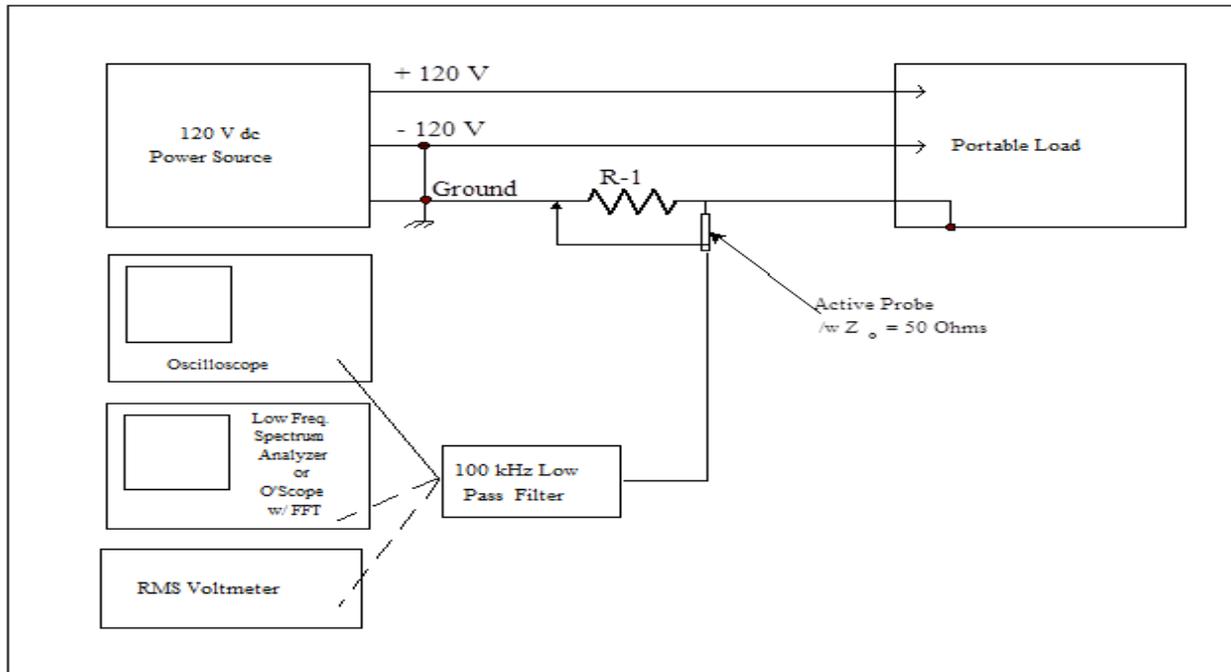


FIGURE 4.3.2.1-1 TOUCH CURRENT VERIFICATION NETWORK

4.3.2.1.1 VERIFICATION – GENERAL EPCE WITH NO DIRECT INTERFACE TO MEDICAL EQUIPMENT

Verification is considered successful when each of the following are completed: (A, B and C for Leakage Current) or D (for the three hazard controls alternative):

- A. Testing of in circuit connections show leakage currents in the ground paths are $\leq 0.5\text{mA}$ with voltage measured across the network in series with grounding conductors. (Refer to Figure 4.3.2.1-1, Touch Current Verification Network) (T)
- B. Inspection of test procedures ensure dc powered equipment testing does not include reversed polarity input tests. (I)
and
- C. Analysis and Test of EPCE to show it provides electrical isolation $>1\text{Mohm}$ of primary power input (hot/return) from device chassis ground (single point ground per SSP 30240) and primary power input (hot/return) from secondary power output (hot/return) (A& T).
- D. EPCE provides three hazard controls that comply with Section 4.3.2.4.

4.3.2.2 GENERAL EPCE WITH DIRECT INTERFACES TO MEDICAL EQUIPMENT

Touch currents for general EPCE $\geq 32\text{V}$ dc/rms with direct interfaces to medical equipment **shall** be $< 0.1\text{mA}$.

SSP 51721
Baseline

Rationale

Most general EPCE allows a much higher leakage or touch current than medical equipment. General equipment that have direct interfaces to medical equipment can introduce extraneous electrical currents to lower impedance paths. In this case, the lower impedance could result in heart fibrillation when the crew is connected to medical equipment. A preferred alternative to leakage current controls is EPCE that provide three hazard controls through compliance with the bonding, grounding, and electrical isolation requirements of Section 4.3.2.4 have satisfied this requirement.

Additional rationale for this requirement can be found in Appendix D.4.3.2.2.

4.3.2.2.1 VERIFICATION – GENERAL EPCE WITH DIRECT INTERFACES TO MEDICAL EQUIPMENT

Verification is considered successful when (A, B, and C) or D are completed.

- A. Testing of in circuit connections show touch currents are $\leq 0.1\text{mA}$ with voltage measured across the network in series with grounding conductors. (Refer to Figure 4.3.2.1-1 in Section 4.3.2.1) International Electrotechnical Commission (IEC) and Underwriters Laboratories (UL) 60601-1 recommend using metal foil in contact with the enclosure for this test. The size of the foil is typically 10 x 20 cm (roughly the size of a hand) depending on the size of the device. (T)
- B. Inspection of test procedures ensure dc powered equipment testing does not include reversed polarity input tests. (I)
- C. Analysis and Test of EPCE to show it provides electrical isolation $>1\text{Mohm}$ of primary power (hot/return) from device chassis ground (single point ground per SSP 30240) and electrical isolation $>1\text{MOhm}$ of primary power input (hot/return) from secondary power output (hot/return) (A& T).

or

- D. EPCE provides three hazard controls that comply with Section 4.3.2.4. (A, I, T)

NOTE: Battery powered devices may require additional assessment for safety when C or D cannot be verified.

4.3.2.3 PROTECTIVE COVERS – ELECTRICAL POWER CONDUCTORS AND TERMINATIONS

Protective covers **shall** be provided to prevent crew contact with exposed power conductors, terminations, and unterminated power connections.

SSP 51721
Baseline

Rationale

Exposed power conductors, terminations, and unterminated power connectors can result in electrical shock to the crew as a result of a crewmember direct or inadvertent contact or result in molten metal generation when > 3A upstream available power at the exposed power conductors, terminations, and unterminated power connectors.

4.3.2.3.1 VERIFICATIONS – PROTECTIVE COVERS – ELECTRICAL POWER CONDUCTORS AND TERMINATIONS

Verification is considered successful when all of the following are completed:

- A. Analysis of design shows all EPCE power conductors, terminations, and unterminated power connectors accessible to the crew are double insulated with dielectric material that provides insulation to >4X available voltage. (A)
- B. Inspection of hardware shows all EPCE power conductors, terminations and unterminated power connectors >32V dc/rms (or any voltage with >3A) accessible to the crew are double insulated with dielectric material. (I)
- C. Review of design inspection of hardware, and test shows all EPCE power conductors, terminations, and unterminated power connectors >32V dc/rms accessible to the crew provide redundant or DFMR Class H bonded/grounded covers. (I)
- D. Inspection of procedures shows protective covers are in place for EPCE power conductors, terminations, and unterminated power connections >32V dc/rms (or any voltage with >3A) accessible to the crew are in place. (I)

4.3.2.4 BONDING AND ISOLATION

Electrically powered end items **shall** provide three controls to protect the crew from shock hazards when voltages are > 32V dc/rms.

Rationale

Electrical shock is considered a catastrophic hazard. End items are required to provide three controls to protect the crew from shock hazards when voltages are > 32V dc/rms.

A UHR is required to define electrical shock hazard controls in the following situations:

- *The end item that uses or generates voltages greater than 32V dc/rms.*
- *Operational controls are necessary to preclude shock hazards.*
- *End item spacecraft charging or incompatibility with the plasma environment that may lead to shock hazards.*

Additional rationale for this requirement can be found in Appendix D.4.3.2.4.

SSP 51721

Baseline

4.3.2.4.1 VERIFICATIONS – BONDING AND ISOLATION

Verification is considered successful when the hazard control methods implemented by the EPCE show that A, B, C, D & F (for EPCE with crew accessible electrically conductive surfaces) are completed, or C, D, E (for EPCE with crew accessible electrically non-conductive [electrically insulated] surfaces) are completed:

- A) Analysis and Inspection of each Class H (<0.1 Ohm) bonding interface are shown to be in compliance with SSP 30245 and ground paths are shown to be compliant with SSP 30240 from EPCE chassis ground to power source ground(s) (A&I)
 - B1) Analysis, Inspection, and Test of Independent and redundant bond interfaces and ground paths are provided for indirect class H (<0.1 Ohms) bonds and ground paths not classified as DFMR. (A, I, & T)
- or
- B2) Analysis, Inspection, and Test Class H (<0.1 Ohm) Bond interfaces and ground paths classified as DFMR are >4X the surface area of a similar wire AWG (American Wire Gauge) sizing derated to carry worst case fault currents back to the power ground from all crew accessible surfaces. (A, I, & T)
- C) Analysis and Test EPCE complies with primary isolation requirements (>1MOhm) of SSP 30240. (A & T)
 - D) Analysis and Test of Low voltage EPCE (<32V power interfaces) that generate hazardous voltages (>32V internally) demonstrate electrical isolation >1Mohm of primary power input (hot/return) from device chassis ground (single point ground per SSP 30240) and electrical isolation >1MOhm of primary power input (hot/return) from secondary power output (hot/return) in accordance with SSP 30240. (A & T)
 - E) Analysis, Inspection, and Test of EPCE where all Crew accessible surface(s) are non-metallic, non-conducting surfaces (including cabling) shall show UL and/or CSA double insulated listing for Commercial Off the Shelf Hardware, or show the dielectric strength of the crew accessible non-metallic EPCE surfaces (including cabling) is verified >4X the highest (worst case) voltage of the EPCE (external and internal). (A, I, & T)
 - F) Analysis, Inspection, and Test of Crew accessible EPCE surfaces that are conductive, with internal double insulation shall demonstrate isolation between electrical conductors and conductive surfaces in accordance with SSP 30240. (A, I, & T)

4.3.3 ELECTRICAL SHOCK AND MOLTEN METAL – CREW MATING/DEMATING OF ELECTRICAL CONNECTORS

There are three potential hazards created by mate/demate of electrical power connections:

SSP 51721

Baseline

- Generation of molten metal from power connectors that could arc/spark during mate/demate (>3A).
- Crew electric shock during mate/demate of high voltage (HV) connections (>32V dc/rms).
- Damage to safety critical circuits or removal of safety critical inhibits as a result of connector bent pins or conductive FOD shorting connector pins/sockets.

4.3.3.1 SCOOP-PROOF POWER CONNECTORS

Electrical connectors with >3A current capability **shall** employ design features that totally enclose or shroud pins and sockets during mate/demate.

Rationale

The use of mechanical design features are necessary to fully enclose or shroud the power connector pins and sockets during mate/demate activities. This minimizes the potential for molten metal caused by FOD or bent pins. Scoop Proof designs provide a longer shell design on the pin half of a connector.

Additional rationale for this requirement can be found in Appendix D.4.3.3.1.

4.3.3.1.1 VERIFICATIONS – SCOOP-PROOF POWER CONNECTORS

Verification is considered successful when the following are completed:

- A. Inspection of design drawings for all power connector(s) with >3A current capability that can be mated/demated by the crew provides mechanical features that completely enclose or shroud the pins and sockets during mate/demate, and prevent contact with the mating connector pins/sockets during mate/demate activity (i.e., the diameter of the male connector is such that it is physically unable to contact female connector pins/sockets (or of a similar design)). (I)
- B. Inspection of the as-built hardware conforms to the approved drawings. (I)

4.3.3.2 POWER CONNECTOR SOCKETS

The powered side of electrical connectors with >3A current capability **shall** be terminated in sockets.

Rationale

Exposed conductors and terminations can result in electrical shock to the crew as a result of direct or indirect contact. The powered side of the connectors are to be terminated in sockets (versus pins). This minimizes the risks of molten metal caused by FOD or bent pins, and precludes inadvertent shorting when the connector is unmated or exposed to the crew. This requirement is applicable to both EVA and Intravehicular Activity (IVA) connectors.

Additional rationale for this requirement can be found in Appendix D.4.3.3.2.

4.3.3.2.1 VERIFICATION – POWER CONNECTOR SOCKETS

Verification is considered successful when each of the following are completed:

- A. Inspection of design drawings for all power connector(s) shows the power side is terminated in sockets. (I)
- B. Inspection of the as-built hardware conforms to the approved drawings. (I)

4.3.3.3 UPSTREAM VERIFIABLE INHIBIT FOR POWER CONNECTORS

One upstream verifiable inhibit **shall** be provided for mate/demate of electrical connectors with >3A current capability.

Rationale

Power connectors with upstream available current >3A can present shock or molten metal hazards to the crew and/or equipment during power connector mate/demate. A verifiable upstream inhibit provides one level of control to prevent shock and/or molten metal hazards to the crew. This requirement is applicable to both EVA and Intravehicular Activities (IVA) connectors.

Additional rationale for this requirement can be found in Appendix D.4.3.3.3.

4.3.3.3.1 VERIFICATION – UPSTREAM VERIFIABLE INHIBIT FOR POWER CONNECTORS

Verification is considered successful when the following are completed:

- A. Inspection of the design shows a verifiable electrical inhibit is in place upstream of the power connection(s) that removes power or reduces upstream power to 32V and <3A from the intended connector and that power removal is confirmed. (I)
- B. Inspection of hazard reports shows operational controls are necessary procedures shows operational controls are in place to ensure the inhibit is inserted and confirmed prior to crew manipulation of electrical connector. (I)

4.3.3.4 EVA 2ND UPSTREAM INHIBIT FOR MATING/DEMATING ELECTRICAL POWER CONNECTORS <200VDC/RMS, <65A, <8.2 KW, OR A BATTERY OCV <40VDC

Each powered circuit >3A and <200V dc/rms that requires EVA mate/demate **shall** contain a second independent upstream inhibit or have the ability to reduce downstream loads to the lesser of 180W maximum (for typical 120 Volts Direct Current (VDC) circuits) or <3A for typical 28VDC circuits per conductive path.

Rationale

The second inhibit is required for EVA because arcing and molten metal can cause a hole in the Extravehicular Activity Mobility Unit (EMU) or potentially ignite the 100 percent Oxygen in the EMU. This requirement can only be applied to end items that have <200V OCV dc/rms, <65A short circuit current, <8.2Kw power capabilities, or <40V dc batteries. A second inhibit is not necessary for Extravehicular Activity Robotics since the crew is not mating or demating electrical connectors.

Additional rationale for this requirement can be found in Appendix D.4.3.3.4.

TABLE 4.3.3.4-1 INPUT EMI FILTER ENERGY STORAGE CAPABILITY CALCULATION

Connector Pin Gauge	Allowable EMI Filter Stored Energy I
4	49.0
8	20.5
10	13.0
12	8.0
14	4.9
16	3.0
18	2.0
20	1.3
22	0.8
Energy storage is calculated using the following equation: $E = \frac{1}{2} C V^2$	
E = Energy (Joules) ; C = Input line to line capacitance; V = Line voltage maximum	

4.3.3.4.1 VERIFICATION - EVA 2ND UPSTREAM INHIBIT FOR MATING/DEMATING ELECTRICAL POWER CONNECTORS <200V DC/RMS, <65A, <8.2 KW, OR A BATTERY OCV <40VDC

Verification is considered successful when (A, B, E and F) or (C, D, E and F) are successfully completed:

- A. Inspection of the design upstream of the power connection(s) shows a second independent electrical inhibit is in place that removes power from the intended connector thereby limiting current <3A. (I)
- B. Test of the 2nd inhibit is shown to remove upstream power from the intended connector. (T).
- C. Analysis shows that end item downstream current is reduced to the lesser of 3A for 32V OCV or 180W (for 120V) prior to the EVA mate/demate activity based on power supply capacity or upstream circuit protection. (A)
- D. Tests show that the downstream load shedding to >3a for <32V OCV or 180W for 120V OCV is successful for the configuration planned for EVA demate/mate. (T)
- E. Analysis of pin gauge shows upstream input EMI filter upstream (of the switching device) is less than energy storage capability defined in Table 4.3.3.4-1 - Input EMI Filter Energy Storage Capability Calculation. (A)
- F. Inspection of procedures shows operational controls are in place to ensure 2nd upstream inhibit for mating/demating electrical power connectors <200V DC/rms, <65A, <8.2Kw, or battery OCV < 40V is inserted and confirmed prior to crew manipulation of electrical connector. (I)

SSP 51721
Baseline

4.3.3.5 BATTERY CONNECTORS WITH OCV <40VDC

Batteries that are inserted into an enclosure that shrouds the battery connections and have an open circuit voltage <40Vdc and current >3A **shall** provide one verifiable upstream inhibit or limit short-circuit current to < 20 A within 0.5 seconds in a short circuit condition.

Rationale

When battery voltages are <40Vdc with >3A worst case current capabilities, there is a molten metal and shock hazard. Either providing one verifiable upstream inhibit of all power sources or limiting short-circuit currents is necessary.

Additional rationale for this requirement can be found in Appendix D.4.3.3.5.

4.3.3.5.1 VERIFICATION - BATTERY CONNECTORS WITH OCV <40VDC

Verification is considered successful when the following are completed: (A and B), or (C, D, and E)

- A. Inspection of the design upstream of the power connection(s) shows an electrical inhibit is in place that removes < 40V battery power from the intended connector and that power removal can be confirmed. (I)
- B. Inspection of procedures shows operational controls are in place to ensure the inhibit is inserted and confirmed prior to crew manipulation of electrical connector. (I)
- C. Analysis of the battery circuit protection device that limits the current from the <40V battery connector contacts to < 20A in <0.5 seconds in approved design drawings, and that the EPCE battery enclosure completely shrouds the battery during battery mate/demate activities. (A)
- D. Inspection of the as-built battery hardware circuitry and battery enclosure conforms to the approved drawings. (I)
- E. A test exhibits that the battery capacity is reduced to <20A in < 0.5s in a short circuit condition. (T)

4.3.3.6 BLIND MATE OR REMOTE CONNECTORS >32V DC/RMS

End items that by design make repeatable bond paths (s) prior to the mate/demate of any blind mate/demate power connections with remote or blind connectors >32V dc/rms **shall** provide redundant or DFMR Class H bonds (<0.1Ω) and chassis isolation from power input ≥ 1 MΩ.

Rationale

Electric shock can result when crew connects or disconnects remote connectors. Molten metal is not considered a risk since the crew is removed from the local area of the connector. This requirement is applicable to both EVA and IVA connectors.

Additional rationale for this requirement can be found in Appendix D.4.3.3.6.

4.3.3.6.1 VERIFICATION – BLIND MATE OR REMOTE CONNECTORS >32V DC/RMS

Verification is considered successful when each of the following are completed:

- A. Inspection of the circuit design drawing shows the EPCE case provides a redundant or DFMR Class H bond after blind mate or remote connector > 32V dc/rms separation. (T)
- B. Inspection of the circuit design drawing shows the EPCE isolation of $\geq 1 \text{ M}\Omega$ between the primary power source input pins (hot/return) and end item device chassis.(I)
- C. Inspection of the as-built hardware conforms to the approved drawings (I)
- D. A pre-flight test show a low impedance path $<0.1\Omega$ (ground) is provided to the EPCE case to the power source ground during all power connector mate/demate activities for remote or blind-mate power connectors >32V. (T)

4.3.3.7 SECOND VERIFIABLE UPSTREAM INHIBIT FOR POWER CONNECTORS >200V DC/RMS, >65A, >8.2KW, AND/OR >40VDC BATTERIES

Electrical connectors >200V or >65A or >8.2Kw, or batteries >40Vdc that are mated or demated **shall** provide a second verifiable independent upstream inhibit.

Rationale

An additional (2nd) verifiable upstream inhibit is necessary when the open circuit voltage is >200 V dc/rms, short-circuit current > 65A, power is >8.2Kw, or batteries are > 40Vdc OCV. This requirement is applicable to both EVA and IVA connectors.

Additional rationale for this requirement can be found in Appendix D.4.3.3.7.

4.3.3.7.1 VERIFICATION - SECOND VERIFIABLE UPSTREAM INHIBIT FOR POWER CONNECTORS >200V DC/RMS, >65A AND/OR >40VDC BATTERIES

Verification is considered successful when each of the following are completed:

- A. Inspection of the circuit design upstream of the power connection(s) shows two independent electrical inhibits are provided that remove power from the intended connector thereby removes power from the connector to be mated/demated and that power removal is confirmed via prerequisite monitoring. (I)
- B. Inspection of operational controls to ensure inhibits are inserted and verified prior to crew manipulation of electrical connector and monitored during the mate/demate activity. (I)

4.3.4 BIOMEDICAL INSTRUMENTATION

Biomedical instrumentation (or “bioinstrumentation”) is classified as either clinical (diagnosis, care, and treatment) or research (acquiring new knowledge). Research instrumentation is more complex, specialized, and designed to provide a higher degree of accuracy and resolution. With respect to electrical safety, bioinstrumentation forms a

SSP 51721

Baseline

special case because here it is necessary and intended to expose the human body to very small electrical currents. In most cases, bioinstrumentation has been qualified for patient use. For space applications, it is expected that the human interface is equivalent and safe (as the use in microgravity would not, by itself, induce additional risk) so the focus for space certification is on the hazard controls related to the isolation between the equipment and the source power supply, as well as other electrical equipment. Battery powered bioinstrumentation devices can provide an additional level of electrical isolation to ISS powered hardware (i.e., leakage current contact hazards, etc.).

The requirements in this section are intended to coincide with SSP 50005, International Space Station Flight Crew Integration Standard, Section 6.4, to provide clarity as well as rationale and verification direction. To prevent electric shock in medical environments, the IEC/UL 60601-X series of standards for electrical medical equipment standards have been established. The IEC/UL 60601 series of documents are available through the NASA Technical Standards program <https://standards.nasa.gov/>. (NASA credentials are required for login.)

Safety requirements for the electrical connection to vehicle power (Section 4.3), the use of batteries (Section 4.3.5), and the requirements for ambulatory equipment (Section 4.3.4.4), as applicable, are necessary regardless of certification to IEC/UL 60601. The requirements in this section cover the interface between the bioinstrumentation device and the ISS crewmember. Section 4.3 covers potential crew hazards between the power supply and the bioinstrumentation device.

IEC/UL 60601 uses the term “applied part” to refer to the part of the medical device which comes into physical contact with the patient in order for the device to carry out its intended function.

Applied parts are classified as Type B, Type BF or Type CF according to the nature of the device and the type of contact. Each classification has differing requirements from the point of view of protection against electrical shock. Refer to Table 4.3.4-1.

TABLE 4.3.4-1 MEDICAL ELECTRICAL EQUIPMENT TYPES

Type	Symbol	Definition
B		Type B, "Body", is the least stringent classification, and is used for applied parts that are generally not conductive and can be immediately released from the patient (e.g., blood pressure cuffs and thermometers).
BF		Type BF, "Body Floating", is less stringent than CF, and is generally for devices that have conductive contact with the patient, or having medium or long term contact with the patient (e.g., ECGmonitors). This is considered a <i>non-invasive interface</i> where the electrode is placed topically to the skin.
CF		Type CF, "Cardiac Floating", is the most stringent classification, being required for those applications where the applied part is in direct conductive contact with the heart (e.g., intra-aortic pressure monitors and dialysis machines). This is considered an <i>invasive interface</i> where the electrode is inserted below the skin.

Notes:

- 1) If the symbols above have the markings of "⊥" and "⊥" on either side, then the equipment is defibrillation proof (i.e., equipment does not have to be disconnected in the event defibrillation is necessary).
- 2) Type B applied parts may be connected to ground, while Type BF and CF are "floating" and needs to be separated from ground.

Although IEC/UL 60601 does not stipulate which classification is to be used for specific devices, the particular standards, IEC/UL 60601-2-XX series of documents, generally specify which classification is required.

If the hazard severity for bioinstrumentation classification is unclear, the ISRP will determine the hazard potential (critical or catastrophic) based on NASA medical community input.

Review by the NASA/Institutional Review Board (IRB) is required when the crew is being used as a test subject.

In order to maintain 2 failure tolerance to electrical shock:

- 1) Unmodified COTS bioinstrumentation that is certified to IEC/UL 60601 is required to meet the requirements in Sections 4.3.4.1 and 4.3.4.2.
- 2) New and/or modified bioinstrumentation hardware, or devices that are not certified to IEC/UL 60601, are required to meet the requirement in Section 4.3.4.2.
- 3) All bioinstrumentation that intentionally applies current to the crewmember is required to also meet the requirement in Section 4.3.4.3.
- 4) Additionally, ambulatory crewmember bioinstrumentation is also required to meet the requirement in Section 4.3.4.4 while attached to a crewmember. A crewmember/patient is considered ambulatory when they are not restrained in any way during nominal or emergency operations and are free to move about the ISS IVA volume (e.g., not a patient restrained on the Crew Medical Restraint System (CMRS)).

SSP 51721

Baseline

4.3.4.1 BIOINSTRUMENTATION CERTIFICATION

Bioinstrumentation **shall** be certified to IEC/UL 60601.

Rationale

IEC/UL 60601 provides rigorous certification and operation requirements to ensure patient safety, at a minimum, in a one failure tolerant manner (typically electrical insulation and electrical isolation design features). Bioinstrumentation should meet the IEC/UL 60601 requirements and Section 4.3.4.2 below to be two failure tolerant for use on-orbit due to the additional risk the microgravity environment and the electrical design of ISS poses to the crew. The <End Item> provider should also take steps to ensure that the equipment is genuine. UL provides resources to help identify genuine vs. counterfeit parts.

4.3.4.1.1 VERIFICATION - BIOINSTRUMENTATION CERTIFICATION

Verification is considered successful when the following are completed: A and B:

- A. Inspection of vendor/manufacturer certification shows that the bioinstrumentation meets IEC/UL 60601. (I)
- B. Bioinstrumentation is confirmed genuine (not a counterfeit part) per the UL database. (I)

4.3.4.2 BIOINSTRUMENTATION TOUCH/LEAKAGE CURRENT

The touch/leakage current for bioinstrumentation **shall** meet the limits defined in Table 4.3.4.2-1.

TABLE 4.3.4.2-1 MAXIMUM PERMISSIBLE FAULT TOLERANT TOUCH/LEAKAGE CURRENT FOR BIOINSTRUMENTATION

Body Contact	Frequency	Number of Faults	Maximum Permissible Current (mA)
Invasive ⁽¹⁾ (Type CF)	DC to 1 kHz	0	0.01
		1 (critical)	0.02
		2 (catastrophic)	0.05
	> 1 kHz	0	$f \text{ (kHz)} \times 0.01$ (must be $\leq 1 \text{ mA}$)
		1 (critical)	$f \text{ (kHz)} \times 0.02$ (must be $\leq 1 \text{ mA}$)
		2 (catastrophic)	$f \text{ (kHz)} \times 0.05$ (must be $\leq 1 \text{ mA}$)
Noninvasive ⁽²⁾ (Type B & BF)	DC to 1 kHz	0	0.1
		1 (critical)	0.5
		2 ⁽³⁾ (catastrophic)	1
	> 1 kHz	0	$f \text{ (kHz)} \times 0.1$ (must be $\leq 5 \text{ mA}$)
		1 (critical)	$f \text{ (kHz)} \times 0.5$ (must be $\leq 5 \text{ mA}$)
		2 ⁽³⁾ (catastrophic)	$f \text{ (kHz)} \times 1.0$ (must be $\leq 5 \text{ mA}$)
⁽¹⁾ Invasive refers to contact that bypasses the protection of the skin (e.g. indwelling catheters). Invasive bioinstrumentation is not allowed in the EMU. ⁽²⁾ Noninvasive refers to contact with the skin (e.g., surface electrodes). ⁽³⁾ For crew in a captive environment (e.g., EMU), the maximum current from noninvasive bioinstrumentation is limited to 0.5 mA.			

Rationale

This applies to nominal and failure cases of new and/or modified bioinstrumentation Class I (grounded) and Class II (double insulated) equipment and to Types B, BF and CF equipment as defined in IEC 60601-1, summarized in Table 4.3.4-1.

Additional rationale for this requirement can be found in Appendix D.4.3.4.2.

4.3.4.2.1 VERIFICATION – BIOINSTRUMENTATION TOUCH/LEAKAGE CURRENT

Verification is considered successful when the following are completed: A, B, C, and D

- A. Analysis shows that invasive and non-invasive bioinstrumentation nominal, worst-case single failures, and worst-case two-failure leakage currents meet the limits in Table 4.3.4.2-1. (A)
- B. Inspection of design that shows that protection features that limit leakage current to limits defined in Table 4.3.4.2-1. (I)
- C. Testing of bioinstrumentation shows leakage currents meet Table 4.3.4.2-1. (T)

Note that testing of bioinstrumentation to single and two fault cases may damage the hardware. Therefore, a qualification unit will need to undergo these tests.

SSP 51721

Baseline

- D. Inspection of test procedures to ensure DC powered equipment testing does not include reversed polarity input tests. (I)

4.3.4.3 BIOINSTRUMENTATION INTENTIONAL CREW APPLIED CURRENT

Medical equipment intended to apply > 0.1mA nominal electrical current to the crew **shall** be designed to comply with the applicable document in the IEC 60601-2-XX series.

Rationale

Intentionally applied currents are designed to produce a specific physiological response. Individual standards exist for devices such as AEDs and muscle stimulators (e.g., IEC 60601-2-10 “Medical electrical equipment – Part 2-10: Particular requirements for the basic safety and essential performance of nerve and muscle stimulators.”).

4.3.4.3.1 VERIFICATION – BIOINSTRUMENTATION INTENTIONAL CREW APPLIED CURRENT

Verification is considered successful when the following are completed: A and B

- A. Inspection of documentation shows design is in compliance with the applicable IEC 60601-2-XX specification. (I)
- B. Functional testing shows that output current/power is within limits specified in the applicable IEC 60601-2-XX specification. (T)

4.3.4.4 AMBULATORY CREW BIOINSTRUMENTATION

4.3.4.4.1 BATTERY POWERED

Bioinstrumentation **shall** be battery powered when attached to an ambulatory crewmember.

Rationale

The crew is intended to be mobile while using ambulatory equipment, remaining tethered to a power source will not only hinder that ability, but also create snag/entanglement/etc. hazards and increase the potential for electric shock hazards (as outlined in IEC/UL 60601). The device is not considered battery powered when charging. Battery charging is only permitted when not attached to the crew due to potential shock hazards from upstream power sources combined with bioinstrumentation connected to crew.

4.3.4.4.1.1 VERIFICATION –AMBULATORY CREW BIOINSTRUMENTATION - BATTERY POWERED

Verification is considered successful when the following are completed: A and B

- A. Inspection of procedures indicates the ambulatory device, while attached to the crew, will only be used on battery power. (I)
- B. Inspection of procedures indicates the ambulatory device, will only be charged when not attached to the crew. (I)

SSP 51721
Baseline

4.3.4.4.2 ELECTRICALLY INSULATED

Bioinstrumentation devices **shall** be electrically insulated from crew contact when attached to an ambulatory crewmember.

Rationale

Electrical insulation provides a physical barrier (typically a suitable dielectric material with minimum dielectric strength) that provides durable electrical insulation between a crewmember and electrical circuitry that could pose a shock or molten metal hazard for the crew. Electrical insulation is needed to protect the crew from electric shock hazards. Single insulation is required (double insulation preferred) such that the enclosure sufficiently insulates the crew from electrical potential(s) inside the device (other than bioinstrumentation electrodes) and from other electrical devices on ISS during use. Double insulation may provide the equivalent of 2 levels of control (i.e., 1 failure tolerance).

4.3.4.4.2.1 VERIFICATION – AMBULATORY CREW BIOINSTRUMENTATION – ELECTRICALLY INSULATED

Verification is considered successful when:

- A. For instruments that are certified to IEC/UL 60601 , one of the following is met: (1 or 2):
 - 1. Inspection shows that bioinstrumentation is UL and/or CSA and has the double insulated (double square - ) symbol displayed. (I)
 - 2. Inspection shows that bioinstrumentation enclosure is UL and/or CSA listed and uses non-conductive materials for the device enclosure (i.e., single insulation) with no other conductive surfaces. (I)
- B. For new/modified instruments, the following is met: (1 and 2)
 - 1. Inspection of drawings indicate that bioinstrumentation is DC isolated from chassis, structure, equipment conditioned power return/reference, crew accessible low voltages, and signal returns. (I)
 - 2. Workmanship resistance measurements of bioinstrumentation show that the non-metallic/non-conductive housing provides insulation that limits leakage current per “Allowable Leakage Current” referenced in Table 4.3.4.2-1 through industry standard dielectric withstanding testing, or Hi-Pot testing. (T)

4.3.4.4.3 ELECTRICALLY ISOLATED

Bioinstrumentation chassis and enclosures **shall** be electrically isolated from input power when attached to an ambulatory crewmember.

SSP 51721

Baseline

Rationale

Electrical Isolation provides electrical circuit decoupling through a high resistance between crewmember contact (through downstream or secondary power output, or through the device chassis) and the source power. Electrical isolation is needed to provide protection to the crew from electric shock hazards by uncoupling the crew from the power source and power source ground (i.e., metallic handrails, seat tracks, etc.), which includes isolation from secondary power (such as ISS power or secondary power) and/or when secondary power exits the device for downstream use (i.e., bioinstrumentation leads). Exceptions are provided for direct battery power (maximum current at electrodes is limited to less than Allowable Leakage Current per Table 4.3.4.2-1, or secondary power output current is limited to less than Let-Go-Current when the device battery is inaccessible to the crew member during crew use and battery charger circuitry not integral to the device).

4.3.4.4.3.1 VERIFICATION – AMBULATORY CREW BIOINSTRUMENTATION – ELECTRICALLY ISOLATED

Verification is considered successful when:

- A. For instruments that are certified to IEC/UL60601, the following is met: (1 and 2)
 - 1. Inspection shows that bioinstrumentation is UL and/or CSA listed. (I)
 - 2. Testing shows the device design provides >1M Ω electrical isolation between the power source input Hot/Return leads and the device chassis or electrical ground, and between the device source power input (hot/return) and any secondary power (hot/return) or electrode that exits the device. (T)
- B. For new/modified instruments, the following is met: (1 and 2)
 - 1. Inspection of drawings indicate that bioinstrumentation is DC isolated from chassis, structure, equipment conditioned power return/reference, crew accessible low voltages, and signal returns. (I)
 - 2. Workmanship resistance measurements of bioinstrumentation show that the source power (hot/return) is electrically isolated from the device chassis, and source power (not/return) is electrically isolated from secondary power (if it exits the device or is crew accessible in the form of leads, cables, connectors, electrodes, etc.) by >1 M Ω isolation. (T)

4.3.5 BATTERIES

Battery hazards are 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, internal and external shorts, reverse current, cell reversal, leakage,

SSP 51721

Baseline

recharging of over discharged batteries, and overpressure. Electrical, mechanical or environmental abuse could cause internal cell pressure build-up that leads to rupture of battery, leakage of electrolyte, venting, fire or explosion with potential injury to the crew, or damage to equipment, ISS or other crewed space environment.

Battery is defined as one cell or a packaged or unpackaged assembly of two or more cells that provide stored electrical energy. Specific design and verification requirements for a battery are dependent upon the battery chemistry, capacity, complexity, charging, environment, and application. The variety of battery chemistries available, combined with the variety of battery-powered applications, results in each battery application having specific, unique requirements pertinent to the specific battery application.

Detailed design information for all batteries on crewed spacecraft, including vehicle, payload, and crew equipment batteries are contained in JSC 20793, Crewed Space Vehicle Battery Safety Requirements. Separate sections include:

- Section 4, General Battery Requirements: Basic requirements for all battery designs and applications.
- Section 5, General Battery Hazards and Controls: Description of hazards and controls and also includes requirements.
- Section 6, Safety Relevant to Specific Battery Chemistries: Chemistry-specific information. No requirements appear in this section, only best practices.

Battery Failure Tolerance

Failure tolerance is the preferred approach of NASA safety for Battery systems used in crewed spacecraft to control all catastrophic hazards. The level of failure tolerance achieved must be determined by an integrated design and safety analysis. (Refer to JSC 20793, Section 4.1.1.) This method is applied in all safety evaluations unless it can be proven that a failure tolerance approach is not practical. Failure tolerance for batteries must consider the toxicity as well as the energy content. This takes into consideration the causes resulting in leakage, rupture, electrical shock, fire, and explosion hazards. All inhibits needed will be in accord with the hazard potential presented.

Battery Design for Minimum Risk

Some potentially critical or catastrophic hazards, such as leakage, cannot practically be controlled using failure tolerance. Batteries may be exempted from the failure tolerance approach, at the discretion of the ISRP, provided the risk they pose is mitigated using DFMR to the maximum practical extent through a defined process in which approved standards and margins are implemented. (Refer to JSC 20793, Section 4.1.2.)

Battery Risk Classification

JSC 20793 defines three levels of risk classifications for battery systems. The classification of hazardous risk for a battery is determined by the total potential energy, size, chemistry, crew safety, vehicle, and mission. Battery Risk Classification (BRC) will be characterized as Low, Medium or High.

SSP 51721
Baseline

For systems which do not conform to established limits, the next higher level of classification is recommended. Threshold limits for each chemistry are defined in JSC 20793, Section 6, and are outlined below. Risk classes are defined as:

- Low BRC– Batteries within this classification are:
 - Low energy < 4 Watt-Hours (Wh) per battery pack where each battery is thermally and electrically isolated (or < 60Wh for Alkaline Primary Batteries) where Watt hour (Wh) = Cell Capacity (Ah) × Cell Voltage (V), and
 - Rated with a THL of 1 or 2, and
 - Contained within a not intentionally sealed compartment, and
 - Meet one of the following criteria based on battery chemistry:
 - Alkaline Primary Batteries (meets all five):
 1. Non-rechargeable cells in sizes D or smaller and,
 2. Maximum of 12 V and 60 Wh and,
 3. Cells either all in series or all in parallel and,
 4. No potential charging source and,
 5. Cells located in a vented compartment.

Note: Silver oxide cells are also considered alkaline chemistry.

- *Lithium-ion Secondary Batteries – COTS (rechargeable) lithium-ion button, cylindrical, or pouch batteries of up to 1000 mAh capacity.*
- *Lithium Primary Batteries – COTS (non-rechargeable) lithium button cells (i.e., Li-MnO₂, Li-CFx and LiFeS₂) of up to 1000 mAh capacity.*
- *Nickel Cadmium Batteries – Nickel-cadmium (rechargeable) batteries and cells of up to 1000 mAh capacity.*
- *Nickel-Metal Hydride Batteries – Nickel-metal hydride (rechargeable) batteries and cells of up to 1000 mAh capacity.*
- *Silver-Zinc Batteries – Silver-zinc (rechargeable) batteries and cells of up to 1000 mAh capacity.*
- *Zinc-Air Primary Batteries – Zinc-air (non-rechargeable) batteries and cells of up to 1000 mAh capacity.*
- *Note: For primary cells, rated cell capacity is defined as the maximum stated capacity per cell product data sheet.*

Medium BRC– Batteries within this classification meet the following criteria:

- Energy levels < 80 Wh per battery pack where each battery is thermally and electrically isolated (or > 60Wh for Alkaline Primary Batteries) where Wh = Cell Capacity × Cell Voltage, and
- Rated with a THL of 1 or 2, and

SSP 51721
Baseline

- Contained within a not intentionally sealed compartment, and
- Meet one of the following criteria based on battery chemistry:
 - *Alkaline Primary Batteries (meets all five):*
 1. Non-rechargeable cells in sizes D or smaller and,
 2. Greater than 12 V and/or 60 Wh and,
 3. Cells either all in series or all in parallel and,
 4. No potential charging source and,
 5. Cells located in a vented compartment.

Note: Silver oxide cells are considered alkaline chemistry.

- *Lithium-ion Secondary Batteries – COTS (rechargeable) lithium-ion button, cylindrical, or pouch batteries > 1000 mAh capacity and ≤ 20 V.*
- *Lithium Primary Batteries – COTS (non-rechargeable) lithium button cells (i.e., Li-MnO₂, Li-CFx and LiFeS₂) > 1000 mAh capacity and ≤ 20 V.*
- *Nickel Cadmium Batteries – Nickel-cadmium (rechargeable) batteries and cells > 1000 mAh capacity.*
- *Nickel-Metal Hydride Batteries – Nickel-metal hydride (rechargeable) batteries and cells > 1000 mAh capacity.*
- *Silver-Zinc Batteries – Silver-zinc (rechargeable) batteries and cells > 1000 mAh capacity.*
- *Zinc-Air Primary Batteries – Zinc-air (non-rechargeable) batteries and cells > 1000 mAh capacity.*

High BRC– Batteries within this classification do not meet the Low and Medium BRC classification and are typically custom, high energy, or high power designs.

4.3.5.1 LOW BRC BATTERIES

Low BRC Batteries **shall** meet manufacturer’s specifications.

Rationale

UHRs for Low BRC batteries should use ISS Hazards System (IHS) Template # 29075. The HR Battery Description Form will be attached to the UHR and is available as an attachment to the template.

Additional rationale for this requirement can be found in Appendix D.4.3.5.1.

4.3.5.1.1 VERIFICATION – LOW BRC BATTERIES

Verification is considered successful when either A or B of the following exist:

- A. Inspection of UL database to confirm cells and/or Batteries meet UL Certification.
(I)
Refer to searchable UL database: <http://www.ul.com/database>.

SSP 51721

Baseline

- B. All flight cells/batteries pass nondestructive testing to verify manufacturer's specifications:
 - 1. OCV Measurement (T)
 - 2. Mass Measurement (T)
 - 3. Capacity/Load Check Measurement (T)
 - 4. Internal Resistance Measurement (T)
 - 5. Visual Inspection (I)

4.3.5.2 MEDIUM/HIGH BRC BATTERIES

Medium and High BRC Batteries **shall** be designed to prevent internal cell pressures that result in cell/battery failure in the worst-case flight environments with margin of +/- 20 degrees F for thermal testing and 0.1 psi (8-10 psi for pouch cells) for vacuum testing.

Rationale

UHRs for Medium and High BRC batteries should use IHS Template # 28907. The HR Battery Description Form will be attached to the UHR and is available as an attachment to the template.

Additional rationale for this requirement can be found in Appendix D.4.3.5.2.

4.3.5.2.1 VERIFICATION – FUNCTIONAL BASELINE TEST

The following five procedures make up the functional baseline test and are performed before and after steps in many verifications. Success/failure is based on comparison with cell or battery manufacturer specifications.

- A. OCV measurement(T)
- B. Mass measurement(T)
- C. Capacity/load test measurement (for rechargeable chemistries or load check for primaries) (T)
- D. Internal resistance measurement(T)
- E. Visual inspection (I)

4.3.5.2.2 VERIFICATION – QUALIFICATION TEST

Verification for Medium and High BRC cell lots and/or batteries (including COTS battery lots) is considered successful when Qualification Testing (JSC 20793 section 4.2.2) of the flight battery design has successfully passed the following:

- A. Environmental Testing
 - 1. Functional baseline test (Verification Section 4.3.5.2.1) (T)
 - 2. Perform vibration test to qualification levels (T)

SSP 51721

Baseline

3. Functional baseline test (Verification Section 4.3.5.2.1) recheck with minimal performance degradation (T)
 4. Charge/discharge cycles (for rechargeable batteries) or a load test (for primary batteries) at 20 degrees Fahrenheit (°F) margin above and below worst-case hot and worst-case cold, respectively (T)
 5. Functional baseline test (Verification 4.3.5.2.1) recheck with minimal performance degradation (T)
 6. Vacuum or equivalent leak checks (T)
 7. Functional baseline test (Verification 4.3.5.2.1) recheck with minimal performance degradation (T)
- B. Flight cell lot radiographic inspection shows acceptable manufacturing quality and absence of defects (T)
- C. Flight cell lot Destructive Physical Analysis (DPA) shows acceptable manufacturing quality and absence of defects (T)
- D. Operation of cell safety devices, if used as a control at the battery level, is verified by a qualification test at the battery level or at a level that accurately simulates the level at which the control is required to confirm the operation of the safety device.
1. Test the Circuit Interrupt Device in order to demonstrate that it activates in the case of a short circuit or overcharge condition. (T)
 2. Expose cells to external shorts to characterize internal PTC performance. (T)
- E. Circuit protection features of battery
1. Review of battery circuit drawing shows that the controls are present. (I)
 2. Expose banks/battery to external shorts to verify that the short does not result in rupture or leakage. (T)
 3. Confirm that battery has over voltage and current monitoring hardware and/or software which controls hardware (Metal Oxide Semi-conductor Field Effect Transistor (MOSFETs), fuses, switches, etc.) to prevent overcharge. (T)
 4. Confirm that Low Voltage Cut-off hardware functions correctly in the battery to cut-off the discharge circuit. (T)
- F. Charger has controls to prevent improper charging or overcharging
1. Review of charging circuit shows appropriate features. (I)
 2. Charger test to confirm that the charger cannot overcharge a flight-like battery. (T)
 3. Battery accepts the maximum allowable current and voltage the charger is able to output during credible failure(s) without going into thermal runaway, venting or leaking. Note that a combination of two credible failures are bypassed for this test. (T)
 4. Confirm that charger detects that the low voltage limit has been reached and does not attempt to charge the battery. (T)
 5. Confirm that charger cannot charge an over discharged battery.(T)

4.3.5.2.3 VERIFICATION – MEDIUM AND HIGH BRC CUSTOM FLIGHT BATTERIES

Verification is considered successful for medium and high BRC custom flight batteries when cell lots pass 100-percent flight acceptance (nondestructive) testing (JSC 20793, Section 4.2.3). Success/failure is based on comparison with cell or battery manufacturer specifications.

- A. Visual inspection of bare cell with shrink wrap removed, if present, shows no manufacturing defects, leakage, etc. (I)
- B. Mass measurement meets manufacturer specifications. (T)
- C. OCV retention measurement meets six sigma analysis and shows no performance degradation. (T)
- D. Alternating current (AC) and/or direct current (DC) impedance test meets manufacturer specifications. (T)

4.3.5.2.4 VERIFICATION – MEDIUM AND HIGH BRC BATTERIES FLIGHT ACCEPTANCE

Verification is considered successful for medium and high BRC batteries intended for flight pass acceptance (nondestructive) testing (JSC 20793, Section 4.2.3) when the following are completed:

- A. Functional baseline test (Verification Section 4.3.5.2.1). (T)
- B. Perform vibration test to flight acceptance levels. (T)
- C. Functional baseline test (Verification Section 4.3.5.2.1) recheck with minimal performance degradation. (T)
- D. Perform vacuum or equivalent leak checks. (T)
- E. Functional baseline test (Verification Section 4.3.5.2.1) recheck with minimal performance degradation. (T)

4.3.5.2.5 VERIFICATION – PRIMARY MEDIUM AND HIGH BRC CELLS/OR BATTERIES

Verification is considered successful for primary (non-rechargeable) medium and high BRC cells and/or batteries that demonstrate devices, controls, and procedures are in place to prevent inadvertent charging (JSC 20793, Section 5.1.2.1d) when:

- A. Inspection of design includes protection from inadvertent charging of primary cells and/or batteries. (I)
- B. Test hardware to show that protective features are in place and functioning. (T)

4.3.5.2.6 VERIFICATION – HIGH BRC END ITEM THERMAL RUNAWAY

Verification for a high BRC end item thermal runaway is considered successful when a Thermal Runaway Assessment with no propagation can be substantiated by: A and (B and/or C)

SSP 51721

Baseline

- A. Analysis is performed to determine whether thermal runaway with propagation can be substantiated. (A)
- B. Analysis to quantify the magnitude (consequence) of the event in the intended application and environment (A)
- C. Test to quantify the magnitude (consequence) of the event in the intended application and environment (T)

4.3.6 CAPACITORS

This section covers non-solid/liquid electrolyte capacitors and Electrochemical Capacitors (EC). Capacitors with only solid electrolyte are not in scope because there are no toxic byproducts that can be released. Capacitors are passive two-terminal electrical components that store electrical energy in an electric field across a dielectric. They are commonly used in modern electronics and Printed Circuit Board designs for applications such as energy storage, power conditioning, suppression, and coupling.

Electrolytic capacitor is a generic term for: (1) Aluminum electrolytic capacitors, (2) Tantalum electrolytic capacitors, and (3) Niobium electrolytic capacitors. All electrolytic capacitors are polarized components whose anode (+) is a metal on which an insulating oxide layer is formed which then acts as the dielectric of the electrolytic capacitor. A non-solid or solid electrolyte which covers the surface of the oxide layer in principle serves as the cathode (-) of the capacitor.

Among the types of electrolytic capacitors, aluminum electrolytic and tantalum electrolytic capacitors have both non-solid electrolyte (liquid when added at construction but absorbed into components thereafter) and solid (or “dry”) electrolyte types. Niobium electrolytic capacitors use a solid electrolyte. There are various types of capacitors with some using a liquid electrolyte as one of its electrode “plates” (terminal). The two most common types are aluminum electrolytic capacitors – most commonly seen in COTS assemblies – and wet slug tantalum electrolytic capacitors – most commonly seen in military and aerospace applications. These types are within the scope of this section.

All flight units are to be tested based on Capacitor Risk Classification (CRC) as shown in Table 4.3.6-1.

TABLE 4.3.6-1 CAPACITOR RISK CLASSIFICATION (CRC)

Risk Classification	Individual Capacitor Case Volume	Vent
Low CRC	≤ 4000 [mm ³]	Yes or No
Medium CRC	> 4000 [mm ³] OR unable to determine volume	No
High CRC	> 4000 [mm ³] OR unable to determine volume	Yes

Hardware is considered Low Capacitor Risk Classification (CRC) if the case volume of its largest wet electrolytic capacitor is less than or equal to 4,000 [mm³].

Hardware is considered Medium or High CRC hardware if the case volume of its largest wet electrolytic capacitor is unknown or exceeds 4,000 [mm³] in volume. Medium and High CRC hardware are distinguished from one another by the presence of a vent on the hardware enclosure. The use of “vent” in this context should not be confused with the pressure relief device, or score, on aluminum electrolytic capacitors.

ECs commonly referred to as “super capacitors” or “ultra capacitors” have hazards associated with their use, similar to battery hazards. ECs include electric double layer capacitors and asymmetric capacitors, e.g., lithium-ion capacitors.

For liquid electrolytic capacitors and ECs, the common hazard is the toxicity of the liquid electrolyte and/or their additives (including acids and salts). Due to this, these type of capacitors are considered to contain hazardous material. Though the electrolyte is nominally contained within the body of the capacitor, venting and leaking cannot be precluded with certainty over the life of a given part without adequate controls in place. In order to assess the criticality of the hazard, a toxicological assessment must be obtained. Refer to Section 4.7.2.

4.3.6.1 ELECTROLYTIC CAPACITORS

The electrolyte in electrolytic capacitors **shall** be designed to minimize the release of electrolyte at ambient conditions.

Rationale

Containment can be compromised when the internal pressure of the capacitor rises due to internal heat. The pressure rise can be due to a number of production and application causes.

Additional rationale for this requirement can be found in Appendix D.4.3.6.1.

SSP 51721
Baseline

4.3.6.1.1 VERIFICATION – ELECTROLYTIC CAPACITORS

Verification is considered successful when **one** of the following is completed (A or B or C or D or E):

- A. If THL-2 or higher (catastrophic hazards), the design includes three predominantly sealed containers as follows:
 - 1. Layer 1: Capacitor case and seal
 - a. Vendor Certificate of Compliance (CoC) or data sheet is provided. (I)
 - b. Incoming inspection by project that capacitors were intact and not leaking upon receipt. (I)
 - 2. Layer 2: Primary sealed assembly
 - a. Containment seal testing shows seal is intact. (T)
 - 3. Layer 3: Secondary sealed assembly
 - a. Containment seal testing shows seal is intact. (T)
- B. If THL-1 (critical hazards), the design includes two predominantly sealed containers as follows:
 - 1. Layer 1: Capacitor case and seal
 - a. Vendor CoC or data sheet provided. (I)
 - b. Incoming inspection by project that capacitors were intact and not leaking upon receipt. (I)
 - 2. Layer 2: Primary sealed assembly
 - a. Containment seal testing shows seal is intact. (T)
- C. Low CRC DFMR:
 - 1. Analysis shows that each individual wet electrolytic capacitors is ≤ 4000 [mm³] case volume based on external dimensions. (I)
 - 2. Successful completion of hardware functional test. (T)
- D. Medium CRC DFMR
 - 1. 3 hours capacitor-screening test at room/lab ambient temperature with at least 3 hours continuous and 5 on/off cycles. (T)
 - 2. Successful post-capacitor functional test. (T)
- E. High CRC DFMR: (Complete (1 OR 2) and 3)
 - 1. 100 hour Capacitor Screening and Test.

**SSP 51721
Baseline**

- a. 100 hours capacitor-screening test at room/lab ambient temperature with at least 3 hours continuous and 5 on/off cycles. (T)
- b. Successful post capacitor-screening functional test. (T)

OR

2. Design and 20 hour Capacitor Screening and Test:
 - a. Proper use of capacitor by design:
 1. Voltage and temperature de-rating (60% or project-required value) (I)
 2. Review of Design for proper polarity (I)
 - b. Inspection of as-built End Item for proper installation polarity or CoC. (I)
 - c. 20 hours capacitor-screening test at room/lab ambient temperature with at least 3 hours continuous and 5 on/off cycles. (T)
 - d. Successful post capacitor-screening functional test. (T)

AND

3. Special Limited Life Component:
 - a. Shelf or Calendar Life: Power on for a minimum of either one continuous hour or two sessions each lasting at least 30 continuous minutes to extend its unpowered shelf life by one year. (I)

Note: If the High CRC End Item is turned on for two sessions each lasting at least 30 minutes, the sessions must take place within 6 months of one another in order to extend the High CRC End Item's shelf life by a year from the date of the second session.
 - b. Service Life: For High CRC hardware that is intended to be operated for more than 10,000 cumulative hours, prepare an assessment of the safe operational life of the hardware. (A)

4.3.6.2 ELECTROCHEMICAL CAPACITORS

An EC (also known as: super capacitor, ultra capacitor, or double layer capacitor) is an energy storage capacitor where electrical charge is stored as a result of non-Faradaic processes at one or both of the electrodes. A subset of ECs known as "asymmetric ECs" have non-Faradaic processes at one electrode and Faradaic processes at the other electrode. The electrodes are highly-porous which results in a large surface area that holds charge resulting in much larger capacitance and energy density than other types of capacitors. ECs are different than the electrolytic capacitors in the previous section in that they store charge at the liquid-solid interface of the electrodes when a voltage potential is applied as opposed to the solid dielectric material that covers the

SSP 51721
Baseline

surface of the electrodes. They typically store 10 to 100 times more energy per unit volume or mass than electrolytic capacitors, can accept and deliver charge much faster than batteries, and tolerate many more charge and discharge cycles than rechargeable batteries.

For traditional EC, if the toxicological assessment indicates a THL-1 or lower and only one device is used, then only open-circuit voltage measurements need to be recorded on flight units and documented on a "Capacitor Description Document" using the HR template IHS # 33029. If the EC is THL 2 or higher then, at a minimum, the approach defined for electrolytic capacitors in the previous section must be followed.

If EC is in series and THL 2 or higher, then a safety assessment similar to that of batteries must be carried out and the requirement owner (JSC Power Systems Branch) should be contacted for guidance.

Asymmetric capacitors are more similar to batteries and must always undergo an assessment similar to that of batteries and, depending on the chemistry, the relevant battery chemistry requirements and processes in JSC 20793 must be used. For example, lithium-ion capacitors must be treated in a manner similar to lithium-ion batteries.

There are three levels of risk classifications for EC systems. The classification of hazardous risk for an EC is determined by the total potential energy, size, chemistry, crew safety, vehicle, and mission. EC risk will be characterized as Low, Medium or High.

For systems which do not conform to established limits, the next higher level of classification is recommended. Risk classes are defined as:

- Low – ECs within this classification are:
 - Energy levels < TBR 4-8> J where each EC is thermally isolated where $J = 0.5 \times \text{Capacitance} \times (\text{Maximum Voltage}^2 - \text{Minimum Voltage}^2)$ and
 - There is no more than 1 EC in series, and
 - Rated with a THL of 1 or 2, and
 - Contained within a not intentionally sealed compartment, and
 - Aqueous electrolyte chemistry
- Medium – ECs within this classification meet the following criteria:
 - Energy levels < TBR 4-8> J per pack where each EC is thermally isolated where $J = 0.5 \times \text{Capacitance} \times (\text{Maximum Voltage}^2 - \text{Minimum Voltage}^2)$, and
 - Rated with a THL of 1 or 2, and
 - Contained within a not intentionally sealed compartment, and
 - Acetonitrile electrolyte chemistry

SSP 51721

Baseline

- High – ECs within this classification do not meet the Low and Medium classification and are typically custom, high energy, or high power designs.

4.3.6.2.1 LOW RISK ELECTROCHEMICAL CAPACITORS

Low Risk ECs **shall** meet manufacturer's specifications.

Rationale

By meeting manufacturer specifications, the end item provider will have confidence that the Low Risk ECs will perform as expected. The lowest level of hazard control is reserved for low energy designs for which standard emergency procedures are written and practiced. These ECs have a low likelihood of causing injury or damage, therefore a minimal amount of verification is requested for the end item.

4.3.6.2.1.1 VERIFICATION – LOW RISK ELECTROCHEMICAL CAPACITORS

Verification is considered successful when one of the following is completed:

- A. Documentation shows that ECs meet 810A UL Certification. (I)
- B. All flight ECs pass nondestructive testing to verify manufacturer's specifications:
 1. OCV Measurement (T)
 2. Mass Measurement (T)
 3. Visual Inspection (I)

4.3.6.2.2 MEDIUM/HIGH RISK ELECTROCHEMICAL CAPACITORS

Medium and High Risk EC **shall** be designed and used in such a way to prevent internal cell pressures that result in EC failure.

Rationale

Medium risk ECs are typically manufactured in high volumes for the consumer and have commonly available means to help determine the reliability and safety of the products. Due to the consequence of a failure, these end items will follow a comprehensive test and validation plan taking into consideration the worst-case relevant flight environments.

High Risk ECs are typically custom, high energy, or high power designs. Due to the extreme consequence of a failure, these end items will follow a comprehensive test and validation plan that includes testing to determine the result of single EC thermal runaway. The analysis of the thermal runaway can lead to a redesign of the EC assembly to mitigate the consequence.

Additional rationale for this requirement can be found in Appendix D.4.3.6.2.2.

4.3.6.2.2.1 VERIFICATION – MEDIUM/HIGH RISK ELECTROCHEMICAL CAPACITORS

Verification is considered successful when the following are completed:

- A. Engineering Evaluation Tests:

SSP 51721

Baseline

1. Abnormal charge tests that include overvoltage, overcurrent and reversed polarity charge. (T)
2. Over-discharge tests that include going into reversal and going into reversal with recharging. (T)
3. Short Circuit testing that include external shorts and internal shorts (e.g., crush, impact). (T)
4. Dielectric Voltage Withstand Test. (T)
5. Heat to Vent test that determines vent and burst pressure. (T)
6. Shock test. (T)
7. Vibration test. (T)
8. DPA of capacitor. (T)

B. Functional baseline test

The following six procedures make up the functional baseline test and are performed before and after steps in many verifications. Success/failure is based on comparison with EC manufacturer specifications.

1. Physical Characteristics
 - a. Visual Inspection (I)
 - b. Dimensions and Mass (T)
2. Electrical Characteristics
 - a. OCV (T)
 - b. Charge/Discharge Cycling Conditioning (T)
 - c. Capacitance (T)
 - d. Internal Resistance (T)

C. Medium and High Risk ECs (including COTS) pass Qualification Testing (JSC 20793 Section 4.2.2) of the flight design:

1. Environmental Testing
 - a. Functional baseline test (Verification B) (T)
 - b. Vibration to qualification levels (T)
 - c. Functional baseline test (Verification B) recheck (T)
 - d. Thermal Cycles: Charge/discharge cycles at 20 degrees Fahrenheit (°F) margin above and below worst-case hot and worst-case cold, respectively (T)
 - e. Functional baseline test (Verification B) recheck (T)
 - f. Vacuum or equivalent leak checks (T)
 - g. Functional baseline test (Verification B) recheck (T)
2. Flight cell lot DPA (T)
3. Operation of cell safety devices, if used as a control at the module level, will be verified by a qualification test at the module level or at a level that accurately simulates the level at which the control is required to confirm the operation of the safety device. (T)

SSP 51721
Baseline

4. Circuit protection features of EC
 - a. Review of EC circuit drawing shows that the controls are present. (I)
 - b. Expose banks to high, low, and smart external shorts to characterize performance. (T)
 - c. Confirm that capacitor has over voltage, charge balancing, and current monitoring hardware and/or software, which controls hardware (MOSFETs, fuses, switches, etc.) to prevent overcharge or imbalance (chemistry-dependent). (T)
5. Charging circuitry has controls to prevent improper charging or overcharging
 - a. Review of charging circuit shows appropriate features. (I)
 - b. Test to confirm that the charging circuitry cannot overcharge a flight-like battery. (T)
 - c. EC accepts the maximum allowable current and voltage the charging circuitry is able to output during credible failure(s) without going into thermal runaway, venting or leaking. Note that a combination of two credible failures are bypassed for this test. (T)
 - d. Confirm that charging circuitry will detect that the low voltage limit has been reached and will not attempt to recharge the EC. (T)
- D. If applicable, for custom Medium and High Risk ECs, cell lots pass 100-percent flight acceptance (nondestructive) testing (JSC 20793, section 4.2.3):
 1. Visual inspection of bare cell with shrink wrap removed, if present (I)
 2. Mass (T)
 3. OCV (T)
 4. Alternating current (AC) and/or direct current (DC) impedance (T)
 5. Capacitance (T)
- E. Medium and High Risk ECs intended for flight pass acceptance (nondestructive) testing (JSC 20793, Section 4.2.3):
 1. Functional baseline test (Verification B) (T)
 2. Vibration to flight acceptance levels (T)
 3. Functional baseline test (Verification B) recheck (T)
 4. Vacuum or equivalent leak checks (T)
 5. Functional baseline test (Verification B) recheck (T)
- F. High Risk ECs must also complete a Thermal Runaway Assessment with no propagation: A and (B and/or C)
 1. Analysis is performed to determine whether thermal runaway with propagation can be substantiated. (A)
 2. Analysis to quantify the magnitude (consequence) of the event in the intended application and environment. (A)
 3. Test to quantify the magnitude (consequence) of the event in the intended application and environment. (T)

4.3.7 ELECTROMAGNETIC COMPATIBILITY

4.3.7.1 ELECTROMAGNETIC EFFECTS

EME includes such areas as EMI, ESD, corona, electrical grounding, electrical bonding, and RF compatibility. RF emitter safety requirements are defined in Section 4.3.8 – RF Transmitter Compatibility.

EME compliance relies on verification activities defined in ISS specifications (e.g., SSP 30237, SSP 30243, SSP 30240, SSP 30245, etc.) or equivalent specifications to protect the vehicle and crew. Evaluation of the end item for determination of EME safety critical circuits is the purview of the ISRP or its designee (e.g., ISS Electromagnetic Effects Panel (EMEP), ISS Frequency Spectrum Management). In the event end items are not compliant with EME IRD or equivalent ISS specifications and the non-compliance effects a hazard control, it is the responsibility of the end item provider to present an HR to the ISRP to define alternate controls to prevent the hazard.

EMI susceptibility testing is required when end items contain EME safety critical circuits. When EME safety critical circuits are identified, ISRP expects projects to address HR controls and verifications with appropriate susceptibility (immunity) testing to show that the EME environment cannot lead to a loss of function, malfunction or degraded performance, or loss of control of inhibits that result in critical or catastrophic hazard.

RF Transmissions Hazards

RF transmissions hazards include intentional RF transmissions during ISS operations and/or unintentional RF transmissions not planned while in close proximity to ISS (e.g. cubesats).

Additional rationale can be found in Appendix D.4.3.7.1.

4.3.7.2 PROTECTING AGAINST HAZARDOUS RF IRRADIATION

End items Intentional RF transmitters **shall** provide protection against hazardous irradiation.

Rationale

Intentional RF transmissions can result in circuit degradation, damage, malfunction, inadvertent operations of ISS safety critical systems, crew contact hazards, or hazards to ISS EMU. Intentional RF levels are to be defined for worst case RF output without attenuation or firmware/software controls that limit transmitter power to a level lower.

Additional rationale can be found in Appendix D.4.3.7.2.

4.3.7.2.1 VERIFICATION - PROTECTING AGAINST HAZARDOUS RF IRRADIATION

Verifications are considered successful when A B, C, or (C and D) are completed:

- A. Approved EMEP Tailoring/Interpretation Agreement (TIA) that defines analysis that defines successful mitigation of End Item RE-02 non-compliance and RS-03 non-compliance (if applicable) (A)

SSP 51721

Baseline

- B. Review of design shows End Item provides containment of any produced RF frequencies (A)
- C. Analysis and testing that shows mechanical stops locations provide KOZ based on the RF transmitter frequency, maximum Effective Isotropic Radiated Power (EIRP) and the RS-03 exposure limit (A)
- D. RF Transmitter is inhibited during the time-to-effect of the hazard when RF radiation exceeds specification limits by more than 6db
 - 1. End Item provides documentation identifies RF transmitter power level, center frequency, tuning range, maximum data rate, modulation, filter characteristics, measured bandwidth, occupied bandwidth, EIRP, cable loss, antenna gain, and harmonic levels (I)
 - 2. End Item Inhibits, controls and monitors
 - a. Critical Hazards
 - i. Review of design shows End Item **critical** RF hazards provide a minimum of 2 independent inhibits, 2 controls, and 1 monitor to preclude inadvertent hazardous RF transmission. (I)
 - ii. Tests demonstrate proper function and independence of 2 inhibits, 2 controls, and 1 monitor to preclude RF transmissions during the time-to-effect of the hazard. (T)
 - iii. Test and Analysis shows end item non-DC RF systems design does not bypass or remove more than one inhibit to the hazardous function due to single events/failures. (T, A, I)
 - b. Catastrophic Hazards
 - i. Review of design shows End Item catastrophic RF hazards provide a minimum of 3 independent inhibits, 3 controls, and 2 monitors to preclude inadvertent hazardous RF transmission. (I)
 - ii. Tests demonstrate proper function and independence of 3 inhibits, 3 controls, and 2 monitors to preclude RF transmissions.
 - iii. Test and Analysis shows end item non-DC RF systems design does not bypass or remove more than one inhibit to the hazardous function due to single events/failures. (T, A, I)
 - 3. Analysis and inspection shows at least one inhibit is interrupted in the circuit return path when DC circuits are used. (I)
 - 4. Operational control or IVA/EVA/EVR Keep Out Zone to mitigate End Item RF emissions. (I)

4.3.7.3 DEPLOYABLE END ITEM RADIO FREQUENCY TRANSMITTERS

Deployable end items with RF radiating devices not planned for ISS operation or in close proximity to the ISS **shall** maintain frequency, radiated susceptibility, and power densities below the levels as defined in Tables 4.3.7.3-1 and 4.3.7.3-2.

TABLE 4.3.7.3-1 CHARACTERISTICS OF DEPLOYABLE END ITEMS RF TRANSMITTERS

Frequency Range	Maximum Radiated Power	Maximum Contact Current
110 kHz – 450 MHz	< 7 watts	<100mA
450 MHz – 1500 MHz	7 watts x 450 / frequency (MHz)	<100mA
> 1500Mhz	Specific Absorption Rate < 0.4 W/kg	<100mA

Note 1: Limits assume no hardware failure scenario will allow deviation below the 110 kHz output.

Note 2: Radiated power in this table is specifically the total power radiated into free space in the absence of any nearby objects with no directivity.

Note 3: In the event that these Maximum Radiation Power levels are exceeded or cannot be determined, comprehensive analysis per SSP 50005 **shall** apply.

TABLE 4.3.7.3-2 CHARACTERISTICS OF DEPLOYABLE END ITEMS RF TRANSMITTERS

Frequency Range	RS03 – 10dB	Power Density from RS03 – 10dB ⁽¹⁾
14kHz to 200MHz	1.58V/m (124dBμV/m)	0.0066 (W/m ²)
200 MHz to 8 GHz	19 V/m (145.6dBμV/m)	0.955 (W/m ²)
8GHz to 10 GHz	6.3 V/m (136dBμV/m)	0.106 (W/m ²)
10 GHz to 13.7 GHz	(linear)	(linear)
13.7 GHz to 15.2 GHz	79 V/m (158dBμV/m)	16.58 (W/m ²)

Note 1: Measured at a point 1 meter from the radiation source.

Note 2: ISS System integration review is necessary regardless of any payload RF power and frequency. This ISS integration review allows for spectrum management assessment and electromagnetic compatibility margin determination to discern if RF transmitter potentially degrades ISS system capabilities or require additional methods to attenuate RF signals (e.g., KOZ).

Rationale

Deployable end items that contain intentional RF radiating devices and maintain frequency, radiated susceptibility, and power densities below the levels in Tables 4.3.7.3-1 and 4.3.7.3-2 while in the pressurized volume of the ISS are not considered a threat to ISS. This includes inadvertent activation of the deployable end item RF emitter.

4.3.7.3.1 VERIFICATION - DEPLOYABLE END ITEM RADIO FREQUENCY TRANSMITTERS

Verification is considered successful when inspection analysis, testing and/or inspection show RF transmitter frequency, radiated susceptibility, and maximum radiated power, and power densities are below the levels defined in Tables 4.3.7.3-1 and 4.3.7.3-2 while in the pressurized volume of the ISS. (I, A, and/or T)

4.3.8 RADIO FREQUENCY-TRANSMITTER COMPATIBILITY

RF transmissions hazards include:

- Intentional (or unintentional) RF emitters during ISS IVA operations and
- Intentional (or unintentional) RF transmissions not planned while in close proximity to ISS (e.g., cubesats).

RF compatibility relies on verification activities defined in ISS specifications (e.g., SSP 30237, SSP 30243, SSP 30240, SSP 30245, SSP 50005) or equivalent specifications to protect the vehicle and crew. In the event end items RF transmitters do not show successful compliance with ISS EME (or equivalent ISS specifications), and it effects a hazard control, it is the responsibility of the end item provider to present a HR to the ISRP to define alternate controls to prevent the hazard. ISS Human Health and Performance (HHP) also review end item safety data to determine RF impact to human health and safety per SSP 50005 “ISS Crew Integration Standard”. In the event that end items RF do not show successful compliance with occupational exposure limits, it is the responsibility of the end item provider to present a HR to the ISRP to define alternate controls to prevent the hazard.

ISS Human Health and Performance (HHP) also review end item safety data to determine RF impact to human health and safety per SSP 50005 “ISS Crew Integration Standard”. In the event that end items RF do not show successful compliance with occupational exposure limits, it is the responsibility of the end item provider to present a HR to the ISRP to define alternate controls to prevent the hazard.

4.3.8.1 PROTECTING AGAINST HAZARDOUS RF IRRADIATION

End items RF transmitter passband frequencies shall provide protection against hazardous irradiation.

Rationale

Hazardous irradiation includes RF transmission levels that can impact ISS and Crew safety because RF transmitter levels are beyond ISS certifications levels.

Examples include:

- *Interference with ISS and Visiting Vehicle safety critical functions,*
- *Malfunction/inadvertent operations of safety critical systems,*
- *IVA crew health and/or*
- *Interference or malfunction of EMU functions.*

The passband frequency is the bandwidth which a modulated RF signal needs to transmit information without attenuation. RF levels are to be defined for worst case RF output without attenuation or firmware/software controls that limit transmitter power to a level lower. For example, the bandwidth of a Tracking and Data Relay Satellite (TDRS)

SSP 51721
Baseline

spread spectrum signal is center frequency +/- 3 MHz for a total of 6 MHz. In an EMI test, the bandwidth which an intentional transmitter is designed to operate is not limited to the radiated emissions limits.

The End Item may not have the insight to conduct the necessary analyses to show that no hazard occurs. It is necessary for the EMEP, Frequency Spectrum Management, and HH&P are involved in assessing the RF transmitter impacts. For example, one antenna placement may be of sufficient distance to prevent a hazardous irradiation, but another antenna position may create a hazard.

Deployable end items (i.e., cubesats) that contain intentional RF radiating devices and maintain frequency, radiated susceptibility, and power densities below the levels in Table 4.3.8.1-1 while in the pressurized volume of the ISS are not considered a threat to ISS. This includes inadvertent activation of the deployable end item RF emitter. Table 4.3.8.1-1 is a guideline for determining whether a deployable end item requires a Unique Hazard Report (UHR). Some End Items may have much higher power levels but the hazard may be controlled through other means.

Additional rationale for this requirement can be found at Appendix D.4.3.8.1.

TABLE 4.3.8.1-1 CHARACTERISTICS OF DEPLOYABLE END ITEMS RF TRANSMITTERS

Frequency Range	RS03 – 10dB	Power Density from RS03 – 10dB⁽¹⁾
14kHz to 200MHz	1.58V/m (124dBμV/m)	0.0066 (W/m ²)
200 MHz to 8 GHz	19 V/m (145.6dBμV/m)	0.955 (W/m ²)
8GHz to 10 GHz	6.3 V/m (136dBμV/m)	0.106 (W/m ²)
10 GHz to 13.7 GHz	(linear)	(linear)
13.7 GHz to 15.2 GHz	79 V/m (158dBμV/m)	16.58 (W/m ²)

Note 1: Measured at a point 1 meter from the radiation source.

Note 2: ISS System integration review is necessary regardless of any payload RF power and frequency. This ISS integration review allows for spectrum management assessment and electromagnetic compatibility margin determination to discern if RF transmitter potentially degrades ISS system capabilities or require additional methods to attenuate RF signals (e.g KOZ).

Recommended verification activity for RF transmitters are listed in Table 4.3.8 “Safety Verification Activity for RF transmitters”. In some cases, only two verifications may be necessary in verifying the hazard is controlled. In other cases, it is necessary to complete two or more verification activities to show the RF transmitter is controlled.

TABLE 4.3.8.1-3 SAFETY VERIFICATION ACTIVITY FOR RF TRANSMITTER HAZARDS

Hazard to:	IVA Crew	Visiting Vehicle	IVA Safety Critical Circuits	External Safety Critical Circuits	EMU Unit	ISS Structure, Elements, Systems
Verification Type	A, E, G, H, and/or I	A, B, C, D, F, G, H, and/or I	A, B, D, F, G, H, and/or I	A, B, C, D, F, G, H, and/or I	A, B, C, D, F, G, H, and/or I	G and J
Verifications						
A- Containment	X	X	X	X	X	
B - Insensitivity with at least 6db margin		X	X	X	X	
C - External Hardstops		X		X	X	
D - Table 4.3.8-1 (Deployable End Items with RF Transmitters)		X	X	X	X	X
E - SSP 50005 (5.7.3.2.1)	X	X	X	X	X	
F- KOZ Ops Control		X	X	X	X	
G- Exception – TIA and/or Ops Control	X	X	X	X	X	
H – Fault Tolerance	X	X	X	X	X	
I- Passband $f \frac{1}{2}$ radiated susceptibility specification (ISS structure, elements)						X

4.3.8.1.1 VERIFICATION - PROTECTING AGAINST HAZARDOUS RF IRRADIATION

Verifications are considered successful when verification G and at least one of the other verifications are complete:

- A. Review of design shows End Item provides containment of any produced RF frequencies. (A)
- B. Analysis and testing show end item passband frequency are at least 6 dB below ISS (or equivalent) specifications.
- C. Analysis and testing that shows mechanical stops locations provide KOZ based on the RF transmitter frequency, maximum (EIRP) and the RS-03 exposure limit. (A)
- D. Analysis, testing and/or inspection show RF transmitter frequency, radiated susceptibility, and maximum radiated power, and power densities are below the

SSP 51721
Baseline

- levels defined in Table 4.3.8.2-1 while in the pressurized volume of the ISS. (I, A, and/or T)
- E. Analysis or testing shows RF transmitter radiation exposure is limited as defined in SSP 50005 (A or T)
 - F. Operational control implementing Keep Out Zone to mitigate End Item RF emissions (I).
 - G. JSC EMEP, JSC FSM, and HHP review and approval of End Item passband frequency analysis and testing.
 - H. Approved EMEP TIA that defines analysis that defines successful mitigation of End Item RE-02 non-compliance and RS-03 non-compliance, if applicable.
 - I. RF Transmitter is inhibited during the time-to-effect of the hazard when RF radiation exceeds specification limits by more than 6db.
 - 1. End item provides documentation identifies RF transmitter power level, center frequency, tuning range, maximum data rate, modulation, filter characteristics, measured bandwidth, occupied bandwidth, EIRP, cable loss, antenna gain, and harmonic levels (I)
 - 2. End item inhibits, controls and monitors
 - a. Critical Hazards
 - i. Review of design shows End Item critical RF hazards provide a minimum of two independent inhibits, two controls, and one monitor to preclude inadvertent hazardous RF transmission. (I)
 - ii. Tests demonstrate proper function and independence of two inhibits, two controls and one monitor to preclude RF transmissions during the time-to-effect of the hazard. (T)
 - iii. Test and Analysis shows end item non-DC RF systems design does not bypass or remove more than one inhibit to the hazardous function due to single events/failures. (T, A, I)
 - b. Catastrophic Hazards
 - i. Review of design shows End Item catastrophic RF hazards provide a minimum of three independent inhibits, three controls, and three monitors to preclude inadvertent hazardous RF transmission. (I)
 - ii. Test demonstrate proper function and independence of three inhibits, three controls, and two monitors to preclude RF transmissions.
 - iii. Test and Analysis shows end item non-DC RF systems design does not bypass or remove more than one inhibit to the hazardous function due to single events/failures. (T, A, I)
 - 3. Analysis and inspection shows at least one inhibit is interrupted in the circuit return path when DC circuits are used. (I)
 - 4. Operational control or IVA/EVA/EVR Keep Out Zone to mitigate End Item RF emissions. (I)

**SSP 51721
Baseline**

- J. Analysis and testing shows end item RF passband frequencies is 1/2 the ISS (or equivalent) radiated susceptibility specification for ISS structure, elements, systems are (A, T)

4.4 COMMAND AND DATA HANDLING

This section contains requirements for Computer Based Control Systems (CBCS) and hazardous commanding and requirements.

4.4.1 COMPUTERS BASED CONTROL SYSTEMS

Computer Based Control Systems (CBCS) are complex electronic devices used to protect against a hazardous event. CBCS includes hardware, software, and firmware. Figure 4.4.1-1 provides a description related to the implementation of ISS CBCS requirements.

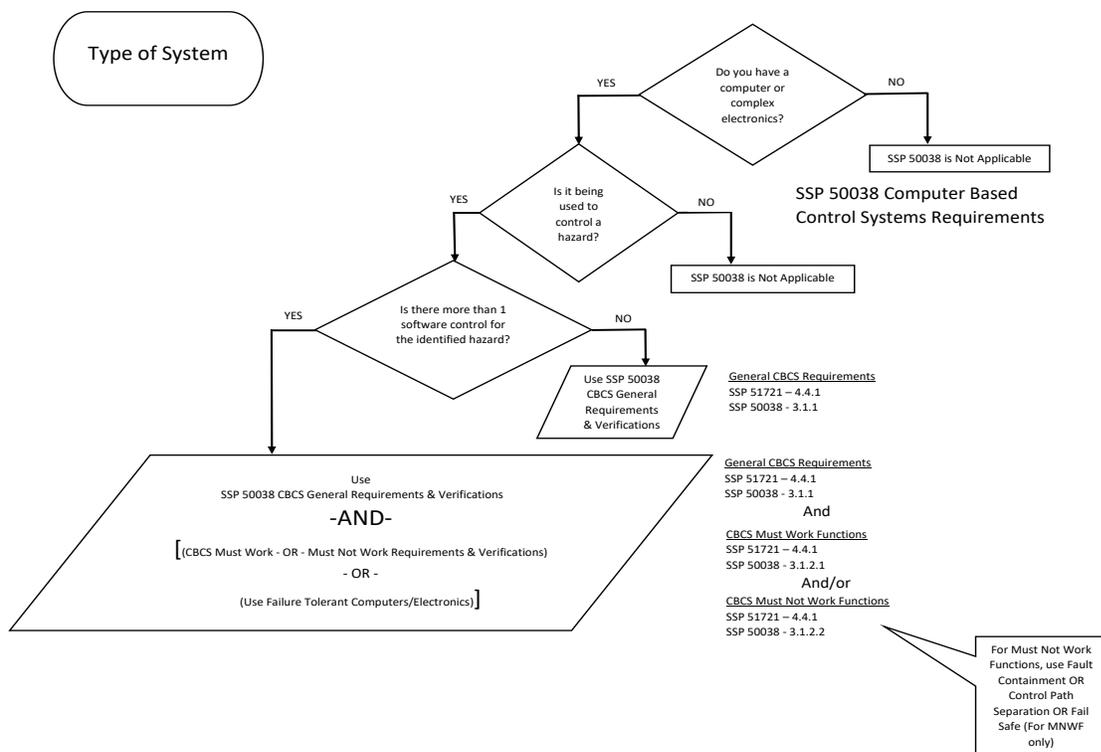


FIGURE 4.4.1-1 – CBCS REQUIREMENTS APPLICABILITY

4.4.2 HAZARDOUS COMMANDING

Commanding

Commanding provides capabilities to conduct ISS science, configure ISS systems, and respond to nominal and off-nominal situations. Commanding is performed using ISS S-Band system, ISS Local Area Network (LAN) (i.e., Ku Ban forward link), end item resources (internal computers), or by the crew.

SSP 51721

Baseline

Hazardous Commands

Hazardous commanding can be initiated or received by a control center, on-board computer (e.g., internal to end item, or ISS PCS), or via crew intervention. If a command meets any of the criteria below, even if only during certain situations, the command is still considered a hazardous command.

Hazardous commands are those that can:

- Remove inhibits to a hazardous function.
- Activate an unpowered hazardous system.
- Reduce safety critical redundancy or reduce failure tolerance.
- Create a hazardous condition.
- Control actively safed systems (such as robotics) during the timeframe the system is safed (or not in use).

A systems is considered “safed” when appropriate controls are implemented and requisite failure tolerance to a hazard is provided (e.g., inhibits verified in place, power is removed).

Hazardous Commanding and Operational Controls

Based on the design order of precedence, operational controls (including the ones used for hazardous commands) are the least desired hazard control strategy. Operational controls are not accepted by the ISRP when they are not operationally feasible.

4.4.2.1 ON-BOARD COMPUTER SYSTEMS

On board computer systems (OCS) or complex electronics with commanding access/interfaces to hazard controls **shall** meet SSP 50038, Computer-Based Control System Safety Requirements.

Rationale

Crew commanding via the Power Control System (PCS) or any computer that connects (hardline or RF) to the 1553 data bus is required to meet the SSP 50038 CBCS requirements. The issuance of a single command cannot result in a hazard or reduction of a hazard control when the hazard exists. Non-deployable OCS end items which control hazardous functions are subject to SSP 50038 review. Deployables which have fault tolerant controls to prevent activation of computers or complex electronics to ensure that it is not using a CBCS strategy for hazards while at ISS (e.g., it is inactive), do not have to meet the CBCS compliance.

Additional rationale for this requirement can be found in Appendix D.4.4.2.1.

4.4.2.1.1 VERIFICATION ON BOARD COMPUTER SYSTEMS HAZARDOUS COMMANDING

Verification is considered successful when inspection of analysis, testing and/or demonstrations are completed per SSP 50038.

4.4.2.2 BI-DIRECTIONAL KU-BAND (KU) ACCESS FOR LOCAL AREA NETWORK (LAN) (KU/LAN)

The requirements in this section helps assure ISS and End Items are protected when telemetry, command, and other data is transported on the Ku/LAN and/or ISS LAN services. <TBR 4-9>

All ISS Projects using Ku/LAN must meet requirements in Sections 4.4.2.2.1, 4.4.2.2.2, and 4.4.2.2.3.

If the End Item has hazardous commands via Ku/LAN as determined by any ISS safety panel, the requirements in Sections 4.4.2.2.4 and 4.4.2.2.5 must also be met.

4.4.2.2.1 KU/LAN SAFETY ASSESSMENT

End Items requesting use of Ku/LAN **shall** assess commanding of systems/subsystems and the segregation of command interfaces to determine hazard potential.

Rationale

All End Items using the Ku/LAN for commanding are required to assess commanding of systems/subsystems to determine hazard potential. It is necessary to identify all End Item hazardous commands. A summary of the End Item hazardous commanding analyses should be included in the safety data package. It is also necessary for the ISRP to concur if there are no hazardous commands.

Segregation of command interfaces for end item hazardous commands is necessary to protect against inadvertent hazardous commanding. End items computer isolation is necessary to control hazards or hazardous commands from being issues or transmitted via systems that are not compliant with Section 4.4.1. Hazardous commands via the S Band/1553 path must be segregated from a non-compliant (per section 4.4.2.5) LAN path, and hazardous commands via a Section 4.4.2.5 compliant Ku/LAN path must also be segregated from non-compliant (per Section 4.4.2.5) LAN path.

4.4.2.2.1.1 VERIFICATION – KU/LAN SAFETY ASSESSMENT

Verification is considered successful when the following are completed:

- A. Hazard analysis defines hazard potential for all end item commands transported on the Ku/LAN. (A).
- B. Inspection of the design shows that all hazardous commands and command paths are isolated/segregated from the noncompliant CBCS resources (i.e., no command interface). (I)
- C. Analysis, Testing and inspections show end item noncompliant CBCS compliant system commands and command paths are isolated/segregated and do not allow:
 - 1. Removal of inhibits to a hazardous function (A, T, and I)
 - 2. Activation of an unpowered hazardous system (A, T, and I)
 - 3. Reduction of safety critical redundancy or reduce failure tolerance (A, T, and I)
 - 4. Creation of a hazardous condition (A, T, and I)

SSP 51721

Baseline

5. Control of actively safed systems (such as robotics) during the timeframe the system is safed (or not in use) (A, T, and I)
- D. Analysis, testing and inspection to show that noncompliant CBCS interface do not have the capability to change the status of any hazardous function. (A, T, and I)

4.4.2.2.2 KU/LAN INFORMATION TECHNOLOGY (IT) SECURITY ASSESSMENT

End Items that utilize the Ku/LAN **shall** provide an IT Security Assessment Report (SAR) per SSP 50974 (or 50989 for International Partners & Program (IP&P)).

Rationale

All End Items that interface with the ISS Ku/LAN are required to perform IT Security Assessments. SSP 50974

(or SSP 50989) defines policy for all information systems and information collected, processed, transmitted, stored, or disseminated with respect to the ISS for End Items. This is applicable to End Items active/inactive connections, wired (Ethernet), wireless (Wi-Fi, Bluetooth, etc.), and/or removable media (USB drives, memory cards.) This assessment provides information to NASA that confirms End Item issues or vulnerabilities are identified, risk rating defined, finding are documented, testing is completed, and recommended mitigations implemented.

SSP 50974 (or 50989 for IPs) provides a SAR template in the appendices. All SAR information is protected from unauthorized disclosure, destruction, or modification while being generated, collected, processed, transmitted, stored, or disseminated by means of the three elements: integrity, confidentiality, and availability of ISS/systems information for ISS IT onboard systems.

4.4.2.2.2.1 VERIFICATION: KU/LAN (IT) SECURITY ASSESSMENT

The verification is considered successful when A and B are completed:

- A. End Item SAR shows that End Item is “low risk” as defined in SSP 50974 (or SSP 50989 for International Partners and Participants.) This SAR includes the following data:
1. Description of End Item active/inactive connections, wired (e.g., Ethernet), wireless (e.g., Wi-Fi, Bluetooth, etc.), or removable media (e.g., Universal Serial Bus (USB) drives, memory cards). (A)
 2. Issues, concerns or degradation/loss of capability End Item vulnerabilities. (A)
 3. Risk rating for each finding. (A)
 4. Test results summaries (T) and
 5. Recommended eliminations, remediations and/or mitigations. (A)
- B. NASA/Partner IT Security Team approval that End Item SAR shows KU/LAN IT SAR is “low risk” (A).

4.4.2.2.3 ON BOARD SOFTWARE PROTECTIONS WITH KU/LAN INTERFACES

End Items connected to the ISS KU/LAN that utilize onboard software for hazard control and/or monitoring **shall** protect network activity from impacting End Item onboard software controlled hazards.

Rationale

The ISS Ku/LAN network activity can potentially corrupt or influence End Item onboard software. Denial of service (DoS) or network storm events can cause interrupts to central processing units or complex electronic device that affect hazard controls and monitors even if there are no direct hazardous commands which can be sent from the Ku/LAN to the processing unit.

Ku/LAN is a single string system (OFT). A single Ku/LAN failure can result in loss of commanding. This can occur based on DoS, noise, or other issues in the on-board LAN or the Ku-band communications system which could prevent safety critical commands from reaching an end item.

4.4.2.2.3.1 VERIFICATION - ON BOARD SOFTWARE PROTECTIONS WITH KU/LAN INTERFACES

Verification is considered successful when A and B are completed:

- A. Onboard end items show that loss of LAN interface will not cause a reduction of hazard control or cause a hazard. (A and T)
- B. Onboard end items show that DoS, network storms, abnormally high traffic to the end item, or noise on the LAN will not cause a reduction of hazard control or cause a hazard. (A and T)

4.4.2.2.4 KU/LAN AND HAZARDOUS COMMANDING - MUST WORK FUNCTIONS

End Items using Ku/LAN for hazardous commanding or safety critical software updates **shall** assure Ku/LAN commands and telemetry do not include any safety critical "Must Work Functions".

Rationale

The Ku/LAN is a single-string (zero fault tolerant) uncertified hazardous command system. Although the Ku/LAN can provide uplink and downlink capabilities (science and situational awareness), a single Ku/LAN failure can result in loss of commanding. There is no guarantee that the Ku/LAN will be available 24 hours a day/7 days a week, and as such, responses in enabling Must Work Functions may not meet time to effect to implement hazard controls. Hazardous commanding interactions through the LAN require additional verification activity since the Ku/LAN has vulnerabilities.

4.4.2.2.4.1 VERIFICATION – KU/LAN AND HAZARDOUS COMMANDING – MUST WORK FUNCTIONS

The verification is considered successful when analysis shows that the End Item does not contain any Must Work Functions that rely upon the Ku/LAN as a control for that function. (A)

SSP 51721
Baseline

4.4.2.2.5 KU/LAN AND HAZARDOUS COMMANDING – COMMAND AND DATA INTEGRITY

End Items using the Ku/LAN for hazardous commanding **shall** maintain data and command integrity from the source to end item.

Rationale

When Ku/LAN is used for control or monitoring of a hazardous function (either uplink or downlink capabilities), it is necessary for the End Item to:

- *Protect against command replay (using time authentication or other functionality),*
- *Provide message content protection (e.g., encryption),*
- *Enable command initiator user authentication,*
- *Provide design unique command routing, and*
- *Maintain file Integrity features (ensure transmission/receipt of expected information).*

4.4.2.2.5.1 VERIFICATION KU/LAN AND HAZARDOUS COMMANDING – COMMAND AND DATA INTEGRITY

Verification is considered successful when the following items are completed:

- A. Replay resistance features (e.g. time authentication) are incorporated to prevent command replay events. (T)
- B. Message content protection for commanding are utilized to protect End Item commands from alteration or disclosure while in transit on the Ku/LAN (e.g., encryption or other secure approach). (A and T)
- C. Command initiator user authentication isolates initiating source of commanding. (A and T)
- D. Unique command routing to the End Item provides independent path for command initiation to End Item function. (A)
- E. File Integrity features provide transmission and receipt of the expected information for data and files. (A and T)

4.4.2.3 GROUND INITIATED HAZARDOUS COMMANDING

Ground operations control centers which can issue hazardous commands **shall** be considered “certified” for hazardous commanding ensuring all of the following:

- A. Command System Availability
- B. Hardware Failure/Software Error Detection
- C. Command System Initialization/Termination
- D. Command Hardware/Software Validation and Configuration Control
- E. Data Transfer Error Detection
- F. Data Integrity
- G. Safing Capability
- H. Command Access Restrictions

SSP 51721
Baseline

I. Operational Fault Tolerance

Rationale

This requirement applies to ground operation centers which are initiating hazardous commands utilizing the SB and 1553 data path and/or the Ku Band/LAN data path. End item devices with the potential for hazardous command uplink can choose to utilize a NASA approved control center (e.g. Payload Operations Integration Center (POIC), when they are not a NASA approved control center. This requires the initiation of the hazardous command to be at the NASA approved control center and is integrated into the existing capabilities of that control center. If providers are utilizing a NASA approved control center, this requirement is already met by that NASA approved control center. In the event remote control centers are not “certified” to provide the protections to prevent inadvertent commands, isolation of the remote ground operations center via a certified control center isolation capability is permissible to ensure inadvertent commands are not uplinked from the uncertified remote ground operations center.

Additional rationale for this requirement can be found in Appendix D.4.4.2.3.

4.4.2.3.1 VERIFICATION – GROUND INITIATED HAZARDOUS COMMANDING

Verification is considered successful when each of the following verifications are complete:

- A. Command system availability (Only applies to control of must work functions)
 - 1. Analysis, Test, Inspection and/or demonstration to show the ability of the command hardware and software to perform the desired hazardous commanding (MW functions) within the time-to-effect (availability requirement). (A, T, I, and/or D)
- B. Hardware Failure/Software Error Detection
 - 1. Analysis, Test, Inspection, and/or demonstration to show the ability of the command hardware and software to perform the desired hazardous commanding (MW functions) within the time-to-effect (availability requirement). (A, T, I, and/or D)
 - 2. Analysis, Test, Inspection, and/or demonstration to show that initialization or termination will result in an ability to issue a hazardous command without further action. (A, T, I, and D)
- C. Command System Initialization/Termination
 - 1. Analysis, Test, Inspection and/or demonstration to show that initialization or termination will result in an inability to issue a hazardous command without further action. (A, T, I and D)
- D. Command Hardware/Software Validation and Configuration Control
 - 1. Analysis, Test, Inspection, and/or Demonstration of software management process for development of commanding applications. This includes software classification, software criticality, software development

SSP 51721
Baseline

- processes, and verification requirements along with configuration management of the command system software. (A, T, I, and/or D)
2. Analysis, Test, Inspection, and/or Demonstration of processes to ensure proper configuration management of all portions of the command application software, user accesses, data routing devices and flight software command products are defined correctly for a use case. (A, T, I, and/or D)
 3. Analysis, Test, Inspection and/or Demonstration of capability of the applications, that manipulate commands data or generate command data or other for commands that have significant hazardous consequences, to do their intended functions without causing a hazard. (A, T, I, and/or D)
- E. Data Transfer Error Detection
1. Analysis, Test, Inspection, and/or demonstration of data transmission within the system (including into and out of internal or external storage areas) to ensure no data corruption has occurred during transit. This includes within command facility and through the uplink transmission. (A, T, I, and/or D)
- F. Data Integrity
1. Analysis, Test, Inspection, and/or demonstration of the command system application to ensure data structure for validity prior to uplink, including data formatting, and routing wrappers. (A, T, I and/or D)
 2. Analysis, Test, Inspection, and/or demonstration to show the integrity of the SW development process for delivery of the command data to the remote control center to ensure the correct products are delivered for implementation within the command applications. (A, T, I, and/or D)
- G. Safing Capability – Safed or unsafed commands in this terminology implies an additional guard or check performed by the control center prior to being processed for uplink.
1. Analysis, Test, Inspection, and/or demonstration of proper identification of all hazardous commands within the command system. (A, T, I, and/or D)
 2. Analysis, Test, Inspection, and/or Demonstration of design protocols in place to ensure no single inadvertent operator action or error could send (uplink) a hazardous command or string of commands. This includes design implementation of command safing of hazardous commands, or other system safing to preclude inadvertent transmission, as well as verifying the ability to inhibit all commands from being sent (uplinked). (A, T, I, and/or D)
 3. Analysis, Test, Inspection, and/or Demonstration that shows the command system is not capable of uplinking safed (hazardous) commands until the requirements for processing such a command are satisfied (i.e., the command is unsafed). (A, T, I, and/or D)
 4. Analysis, Test, Inspection, and/or Demonstration show hazardous commands are not “chained” into a command string unless command

SSP 51721
Baseline

- checking capability is implemented prior to uplink of each of the hazardous commands. (A, T, I, and/or D)
5. Analysis, Test, Inspection, and/or Demonstration show chained command string (command block) removes no more than on inhibit to a hazardous function. (A, T, I and/or D)
- H. Command Access Restrictions
1. Analysis, Test, Inspection, and/or Demonstration of user permissions and access to ensure integrity of access to the command applications, secure protocols for access to the command application, and proper access to approved commands within the command application. (A, T, I, and/or D)
 2. Analysis, Test, Inspection, and/or Demonstration of design features that provide verification of the commands selected by the user for uplink prior to the uplink occurring, and the ability to cancel uplink when necessary. (A, T, I, and/or D)
 3. Analysis, Test , Inspection, and demonstration that protections are in place to restrict physical access to facilities with command systems.
- I. Operational Failure Tolerance
1. Analysis, Test, Inspection, and/or demonstration of processes and protocols show verification of user manipulation of command stat that ensures data corruption or user error has not occurred. (A, T, I, and/or D)
 2. Analysis, Test, Inspection, and/or Demonstration of processes and protocols that ensure proper command authorization and permissions for issuance of commands. (A, T, I, and/or D)
 3. Analysis, Test, Inspection, and/or demonstration of processes and protocols that ensure command success (end item) between commands, including scripted or chained commands. (A, T, I, and D)

4.5 MONITORING

Monitors are indicators used to obtain status of functions, devices, inhibits and parameters. Incorporating monitors into circuits requires design considerations and risk trades. The problems identified below should not occur when monitors are working properly. In some cases, monitors can:

- Defeat inhibits or controls
- Provide false status indications (loss of input without providing an indicator change), or
- Prohibit response time to recover from end item failures.

Monitors must be available at all times and not affect the inhibits. Monitoring of two of three electrical inhibits is required when inadvertent operation could result in a catastrophic hazard and/or for electrical inhibits that can be removed by the crew, ground, or computer control commanding.

SSP 51721
Baseline

Monitoring is applied to Must Not Work (MNW) functions, Must Work (MW) functions, and Actively Safed systems.

- MNWF – A function, if performed inadvertently or at an in-opportune time, results in a hazard.
- MWF – A redundant function, if not performed, can result in a catastrophic hazard if the function is not performed.
- Actively Safed Systems – Only hazardous when system exceeds pre-defined limits.

End item designs should be such that real-time monitoring is not required to maintain control of catastrophic functions. Figures 4.5-1 through 4.5-3 provide visual diagrams for MNW, MW, and Actively Safed functions.

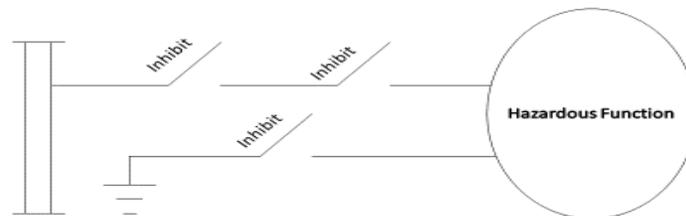


FIGURE 4.5-1 MUST NOT WORK SYSTEM (INHIBITS)

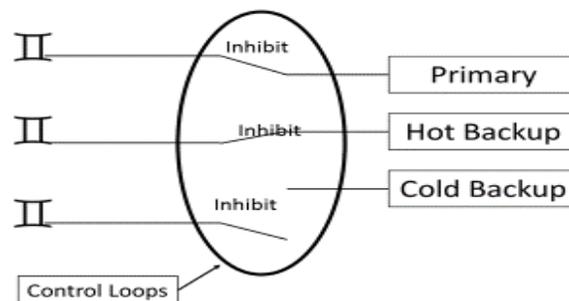


FIGURE 4.5-2 MUST WORK SYSTEM (REDUNDANCY)

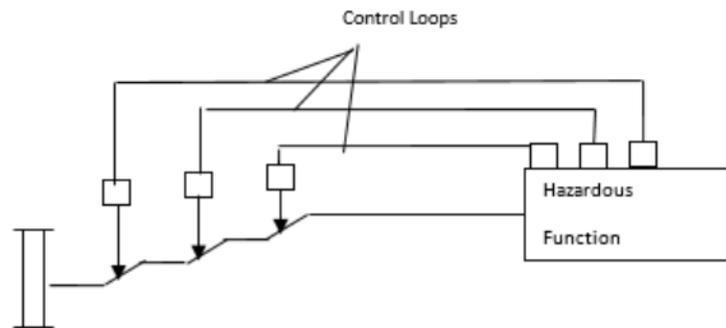


FIGURE 4.5-3 ACTIVELY SAFED SYSTEM (SHUTDOWN WHEN OUT OF LIMITS)

4.5.1 MONITORING – MONITOR CAPABILITIES

When monitoring is required, powered end items **shall** monitor the status of two of the three inhibits to catastrophic hazardous functions.

Rationale

Monitoring includes status of inhibits, state of operations, and execution of safing functions. Monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible.

When monitors are in circuits with inhibits and controls, monitors provide current-limiter functions to prevent load current from enabling, damaging, or disabling the inhibit. Current limiter functions can protect circuits from harmful effects due to a short-circuit or similar problems in the load.

SRP Review of Monitoring Provisions

Monitoring may not always be appropriate and status of inhibits may not be required. With ISRP approval, monitoring and hazard detection, and safing may be utilized to support control of hazardous functions provided there is adequate crew response time available (time-to-effect (TTE) of the hazard) and safing procedures are developed. The TTE of the hazard is the time between the loss of an inhibit and the occurrence of the hazard.

Requirements for monitoring critical hazards are not normally imposed, but may be required by the ISRP on a case-by-case basis. Monitoring of one of the two inhibits is prudent and the capability to restore inhibits to a safe condition should be available. When inhibits are not directly monitored, ISRP review to discern whether monitoring of the control of that inhibit may be considered on a case-by-case basis.

4.5.1.1 VERIFICATION – MONITORING – MONITOR CAPABILITIES

Verification is considered successful when each of the following are completed:

- A. Testing of monitors shows status of the function. (T)

SSP 51721

Baseline

- B. Testing shows that loss of input or failure of the monitor provides a change in state of the indicator. (T)
- C. Testing shows monitor electrical power does not impact the operation of hazardous function, inhibits, or controls. (T)

4.5.2 MONITORING FREQUENCY

Monitoring only provides indication of the status of inhibits and controls. Implementation of monitoring requires notification to allow for response to the change of state of an inhibit. Monitoring provides periodic insight to allow for detection and safing due to latent failures (e.g., failed open valves).

Monitoring frequency depends on the hazard TTE. The TTE of the hazard is the time between the loss of an inhibit and occurrence of the hazard. The need for hazard detection and safing by the flight crew to control time-critical hazards will be minimized and implemented only when an alternate means of reduction or control of hazardous conditions is not available.

Notification of systems hazards may be provided via on-board automated systems (Fault Detection, Isolation and Recovery (FDIR) Systems) that initiate programmed responses to identified failures, or the ISS Caution and Warning (C&W) System which requires flight crew and/or ground safing actions.

Monitoring frequency is classified as Real-Time Monitoring (RTM) or Near Real Time Monitoring (NRTM). Table 4.5.2-1 describes hazardous function monitoring categories.

TABLE 4.5.2-1 HAZARDOUS FUNCTION MONITORING CATEGORIES

Monitoring Category	Monitoring Frequency	Catastrophic Hazards			Type of Notification	Who gets Notified
		MNWF	MWF	Actively Safed		
RTM	Immediate		X	X	On Board System ISS C&W	Crew
NRTM	Nominally Once per Orbit	X	X		ISS C&W Crew Detection Ground Detection	Crew and/or Ground

4.5.2.1 MONITORING FREQUENCY – RTM

RTM **shall** be provided when end item failures require immediate response to prevent a catastrophic hazard.

Rationale

Immediate means that a rapid response is required in order to control a catastrophic hazard that has a short time-to-effect.

Additional rationale for this requirement can be found in Appendix D.4.5.2.1.

4.5.2.1.1 VERIFICATION – MONITORING FREQUENCY – RTM

Verification is considered successful when the following are completed: (A or B)

A. CBCS Verification

CBCS analysis and testing results show FDIR is implemented per CBCS requirements (4.4.2.1 – General Requirements, 4.4.2.2 – MWF requirements, 4.4.2.3 – MNWF requirements).

B. RTM Verification

1. Analysis shows crew time allows for monitoring/response time to detect and/or safe the system within the time-to-effect of the hazard. (A)
2. Test show monitoring functions operate as designed during both ground and flight phases. (T)
3. Inspection of crew procedures shows safing steps in response to ISS C&W (Caution and Warning) alerts are included in procedures. (I)

4.5.2.2 MONITORING FREQUENCY – NEAR REAL TIME MONITORING (NRTM)

End items **shall** provide NRTM (or RTM) when TTE of a catastrophic hazard is > 90 minutes because a response is required to prevent a catastrophic hazard.

SSP 51721
Baseline

Rationale

NRTM is defined as notification of changes in inhibit or safety status on a periodic basis. Periodic monitoring every 90 minutes allows for review of the inhibit status once per orbit. NRTM is normally used for MNW systems and redundant MW systems with long TTEs. NRTM can be accomplished via monitored telemetry data via ground control center or crew monitoring.

Additional rationale for this requirement can be found in Appendix D 4.5.2.2.

4.5.2.2.1 VERIFICATION– MONITORING FREQUENCY – NRTM

Verification is considered successful when the following are completed:

- A. Analysis and testing shows NRTM notifications are provided to the ground or crew (A and T)
- B. Inspection of procedures inputs shows inhibits are periodically monitored based on the TTE of the hazard. (I)
- C. Prerequisite Monitoring
 - 1. Testing that shows indicators provide accurate status of inhibits. (T)
 - 2. Inspection of procedures that control strategy provides inhibits are monitored prior to the hazardous procedure being implemented. (I)

4.5.2.3 MONITORING FREQUENCY - WHEN INHIBIT MONITORING IS NOT REQUIRED

End items with no monitoring capability (e.g., electrical inhibits that cannot be removed by crew, ground, or CBCS **shall** ensure one or more inhibits are in place during the TTE of the hazard.

Rationale

End item inhibits used to protect against a hazardous function with no monitoring capability will ensure that inhibits between the power source and the hazardous function are de-energized during the timeframe that the hazard is present. Hazard severity determines the number of inhibits required to control the hazard. The inhibit can either be provided by the end item or by other upstream ISS resources. This requirement is specific to end items that demonstrate inhibits are susceptible only to hardware failures. Monitoring is required for electrical inhibits that can be removed by the crew, ground command, or computer control commanding when observations are continually available.

Additional rationale for this requirement can be found in Appendix D.4.5.2.3.

4.5.2.3.1 VERIFICATION – MONITORING FREQUENCY – WHEN INHIBIT MONITORING IS NOT REQUIRED

Verification is considered successful when the following are completed: (A, or B, or C)

SSP 51721
Baseline

- A. Fourth Inhibit Verification
 - 1. Analysis, testing and inspections show 4th inhibit isolates the power between the power source and other three inhibits and control circuitry. (A, T, and I)
 - 2. Analysis, testing, and inspections show at least three independent inhibits provide isolation of source power to end item function. (A and, T and, I)
 - 3. Analysis shows no single failure in the control circuitry results in the removal of the 4th inhibit during the time the hazard exists. (A)
- B. Three Inhibit Verification
 - 1. Workmanship, proto-flight, acceptance, and/or thermal cycle testing show three inhibits remain in a safe state for all launch and on-orbit environments and mission phases. (T)
 - 2. Analysis shows inhibits cannot be bypassed by computers, ground commanding, or crew. (A)
 - 3. Analysis that shows hardware failure (i.e., structural) that results in loss of requisite inhibit(s) would need to occur for the hazardous event to occur. (A)
- C. On Orbit Preparation Verification
 - 1. Analysis shows that inhibits cannot be bypassed by computers, ground commanding, or crew. (A)
 - 2. Testing shows that planned reconfiguration changes do not remove inhibits. (T)
 - 3. Review of hazard controls show inhibits are in place prior to and after end item configuration change (I)

4.5.3 MONITORING OF DEPLOYABLE END ITEMS FROM ISS

Deployable end items **shall** provide inhibit monitoring when removal of any combination of inhibits results in an ISS catastrophic hazard after deployment.

Rationale

Verification of inhibits is not required post separation of most deployable end items since inhibit state is verified prelaunch, prior to deployment (before environments can change the state of inhibit), or are not an ISS hazard after deployment. When removal of any combination of inhibit (1, 2, or 3) results in a catastrophic hazard after deployment, monitoring is required.

When timers are used to change the status of an inhibit to hazardous functions, complete separation of the end item from the ISS will be achieved prior to the initiation of the timer. (Refer to Section 4.5.4.) Timer independent control of each inhibit is

SSP 51721
Baseline

required consistent with the severity of the hazard (e.g., independent timer for each inhibit).

4.5.3.1 VERIFICATION – MONITORING OF DEPLOYABLE END ITEMS FROM ISS

Verification is considered successful when:

- A. Testing of monitors that show indicators provide accurate status of inhibits. (T)
- B. Analysis shows inhibit is in place until the hazard potential no longer exists. (A)
- C. Inspection of procedures inputs include steps for monitoring of the inhibit state during the time the catastrophic hazard exists. (I)

4.5.4 USE OF TIMERS

End items with timing functions used for complete control of inhibits to protect from a catastrophic hazard **shall** provide three independent timer inhibits or three independent timer safing capabilities.

Rationale

Timers are considered only one control to a hazard since there are many credible failure modes that can allow the timer to start prior to the desired time. Monitoring of timers is typically not available. Failure of a timer, or a computer causing bypass of a timer or any other credible failure to satisfy one inhibit is still just one failure.

A single timer that allows transfer of more than one inhibit without other controls renders the inhibits dependent. In this case, all inhibits transferred by a single timer are effectively only 1 inhibit enabled by a single timer.

The use of a timer can be used as one level of control of an inhibit when:

- *Timers cannot be bypassed by computers, ground commanding, or crew,*
- *Timers show no credible failure modes that result in loss of an inhibit.*

When credible failure modes exist that could allow the timer to start prior to a desired time, a safing capability will be provided. If this safing is via a RF command, then the command capability will be provided to the flight crew.

4.5.4.1.1 VERIFICATION – USE OF TIMERS

Verification is considered successful when A or (B and C) are completed:

- A. Test and analysis of timers confirm no credible failure modes can defeat inhibits. (T and A)
- B. Test and analysis confirm end item safing capabilities upon timer failure. (T and A)
- C. When the safing function is via RF command.

SSP 51721

Baseline

1. Analysis and testing show RF command provides safing function, (A and T)
2. Inspection of the as built design shows RF command function is as designed per drawings. (I)
3. Inspection of procedure inputs confirm steps to safe the end item hazardous function. (I)

4.6 EXTERNAL ENVIRONMENTS

This section includes requirements for plasma and external ionizing radiation environments.

4.6.1 PLASMA

Plasma is a quasi-neutral gas of particles (charged and neutral) that exhibits collective behavior distinct from normal gasses allowing the flow of electricity. A space vehicle's interactions with plasma is based on plasma thermal properties and orbital altitudes. Relatively cold, dense plasma of the ionosphere interacts differently than those of tenuous plasma at very high orbits. There are also different plasma interactions in the aurora regions where the currents originating from higher altitudes penetrates to low Earth orbit. Plasma can also be created by the release of ionized gas from end items.

No unique plasma safety requirements are imposed on end items. However, plasma environments can create a safety concern when analysis shows potential impacts to safety critical circuits. Space Environments Subsystem Problem Resolution Team (SPRT) provides evaluations of end item generated plasma to determine hazard potential.

Plasma and the ISRP

ISS Space Environments SPRT review of plasma is necessary to determine whether end item plasma is a concern. When the ISS Space Environments SPRT determines the end item's plasma can result in a hazard, it is the responsibility of the end item provider to disclose the concerns to the ISRP. End items may be requested to generate UHR when controls are necessary to protect ISS from plasma hazards.

ISRP review of the potential concern could determine that a UHR is required to document additional safety controls to protect ISS from end item plasma contributions. Operational controls could be necessary to preclude ISS Floating Potential (FP) excursion (including ISS or end item provided Plasma Contactor Units (PCUs)) and impacts to safety critical circuit safety margins and failure tolerance.

Spacecraft Charging due to Plasma

A spacecraft accumulates electric charge from the plasma. Spacecraft FP is the voltage difference between spacecraft structure and the surrounding plasma. Changes due to the collection of positive and negative currents, and changes in the geomagnetic field determine what FP the spacecraft will reach. The plasma properties, the spacecraft design, and spacecraft operating characteristics all influence the spacecraft charging process.

Spacecraft Charging and ISS

Per SSP 41000, ISS PCUs can maintain ISS FP within $\pm 40V$. In-flight measurements of ISS charging have demonstrated that violations of the $\pm 40V$ FP certification limits happen but are relatively rare and of such short duration that they pose no threat to ISS core systems. For that reason, ISS PCUs are not operated routinely.

Note: Activation of PCUs is only “necessary” if required during EVA.

Charging of ISS End Items

IRDs or equivalent specifications require externally mounted end items to be designed to survive a +20 to -90 V ISS FP range. The IRDs or equivalent specifications also define data requirements to characterize end item operations. Externally mounted end items can arc in normal ISS conditions, and/or accumulate charge, and possibly generate worst-case FPs that drive the ISS FP outside the $\pm 40V$ FP certification limits (e.g., biased conducting surfaces, high current electron/ ion beams). Biasing of the FP can be a safety concern during EVA. ISS Space Environments SPRT review of end item operation and capabilities are necessary to determine whether end item operation is an ISS charging or arcing concern.

4.6.2 IONIZING RADIATION ENVIRONMENT

Ionizing radiation consists of galactic cosmic rays, trapped electrons, and trapped protons in the ISS orbital flight environment (orbital inclination 51.6 degrees and altitude ranging from 350 to 420 km) and end items with plasma generators, X-ray generators, and radioactive materials. The ionizing radiation environment consists primarily of high kinetic energy charged particles many of which can induce Single Event Effects (SEE) and Total Ionizing Dose (TID) in electronics.

Safety requirements pertaining to ionizing radiation from end item radioactive materials are defined in Section 4.7.2.3.

4.6.2.1 IONIZING RADIATION

End item safety critical circuits **shall** operate as designed during and after exposure to the ISS ionizing radiation environments.

Rationale

Safety critical circuits are circuits whose loss of function, malfunction, performance degradation, or inhibit loss can result in critical or catastrophic hazard.

Ionizing radiation can result in hazard control reduction when critical functions are affected by SEE and TID.

Additional rationale for this requirement can be found in Appendix D.4.6.2.1.

4.6.2.1.1 VERIFICATION – IONIZING RADIATION

Verification is considered successful when analysis (including parts characterization test data) shows end item safety critical circuit design does not create a hazard for Design

SSP 51721
Baseline

Reference Mission (DRM) when exposed to environments as described in SSP 30512 (Sections 3.2.1 and 3.2.2). (A)

4.7 MATERIALS

In establishing safety requirements for materials used in and/or for spaceflight or for materials being studied in the space environment, special considerations are required. Precautions are taken to keep the crewmembers, environment, vehicle's systems hardware, and vehicle safe. Capability and limitations are considered for the clean-up of potential leakage and/or exposure of the crew and system hardware, the compact living environment, and the limited ability to provide assistance and supplies. Altered material properties and physical responses due to the decreased gravitational environment and increased oxygen environment are also be taken into consideration when evaluating and planning for the use of materials. For example, any particulates released are not readily pulled to the ground by gravity and away from the crew's faces; this can result in respiratory and/or ocular hazards for the crew.

The following material requirements are established to prevent and control hazards. Materials selection requirements (reference Section 4.7.1) address hazards from material flammability, offgassing and compatibility. Hazardous materials requirements (reference Section 4.7.2) address hazards from external and internal release.

4.7.1 MATERIALS SELECTION

These requirements are intended to ensure proper material selection. Flammable materials could cause initiation or propagation of a fire in the presence of an ignition source. Offgassing of toxic products in the ISS environment could lead to illness or long term health effects for the crew. Materials compatibility issues could cause unacceptable degradation of the materials and result in hazardous conditions within an end item or within the ISS environment.

Materials used in the fabrication of end items should be selected by considering the operational requirements for the particular application and the design engineering properties of the candidate materials. The operational requirements include, but are not limited to, operational temperature limits, loads, life expectancy, and vehicle related induced and natural space environments. The worst-case anticipated use environment (i.e., most hazardous pressure, temperature, material thickness, and fluid exposure conditions) is used in the evaluation of material suitability.

The design engineering properties to be considered in material selection include mechanical properties, fracture toughness, stress corrosion, thermal and mechanical fatigue properties, fluids compatibility, etc. These are covered with structural design and pressure system requirements (reference Section 4.2). Conditions which could contribute to deterioration of hardware will receive special consideration.

NASA Marshall Space Flight Center (MSFC) Materials and Processes Technical Information System (MAPTIS) contains a listing of materials (both metallic and nonmetallic) with a rating indicating acceptability for each material's characteristic. Although primarily designed for experienced users, it can be used to help select materials that have already been shown to meet the applicable acceptance criteria.

SSP 51721
Baseline

MAPTIS is accessible via the Internet at <http://maptis.nasa.gov> (registration is required) and the ISSP can provide assistance on its use. For materials which create potentially hazardous situations as described in the paragraphs below and for which no prior NASA test data or rating exists, other test results should be provided for ISSP review or the end item provider can request assistance from the ISSP in conducting further evaluation or applicable tests.

The use of materials that do not strictly comply with the requirements in this document might still be acceptable in the specific hardware application and will be assessed on a case-by-case basis. Rationale to demonstrate that a materials application is acceptable will be documented in a Material Usage Agreement (MUA) and/or HR for all materials that are technically acceptable but do not meet the requirements in this document.

For end items supplied by organizations with a Materials and Processes Reciprocal Agreement approved by the ISSP (including heritage agreements grandfathered to the ISS from the Space Shuttle Program), the reciprocal agreement baselines the process for selection and certification of materials used in end items to the requirements herein and verification is conducted by the individual materials and processes organization.

4.7.1.1 FLAMMABLE MATERIALS

End items **shall** be designed or controlled to eliminate fire propagation in the worst-case operating environment for the end item.

Rationale

An end item can not constitute an uncontrolled fire hazard; therefore, all end item materials should either be non-flammable or controlled such that they do not allow fire propagation. Spacecraft fire control is based on minimizing potential ignition sources and eliminating materials that can propagate fire. Controlling the quantity and configuration of flammable materials to eliminate potential fire propagation paths ensures that any fire would be small, localized, isolated, and would self-extinguish without harm to the crew.

End items show compatibility with their intended environment and fulfill this requirement through verifications. Materials are tested or evaluated in the worst-case operating environment for the end item to verify this requirement. The worst-case oxygen environment for ISS is 14.7 psia with 24.1-percent oxygen for all locations except the USOS airlock. The airlock worst-case environment is 10.2 psia with 30-percent oxygen. End items materials should be tested or evaluated in the worst-case airlock environment if they intend to operate in the airlock during EVA preparations.

Materials used outside the pressurized areas should be evaluated for flammability in an air environment at 14.7 psi to account for ground processing hazards.

Additional rationale for this requirement can be found in Appendix D.4.7.1.1.

SSP 51721
Baseline

4.7.1.1.1 VERIFICATION – FLAMMABLE MATERIALS

Verification is considered successful when the following are completed: A and/or B

- A. Flammability assessment (including compatibility with worst-case operating environment) per JSC 29353, Flammability Configuration Analysis for Spacecraft Applications, SSP 30233, Space Station Requirements for Materials and Processes, NASA-STD-6016, or applicable IP materials process/segment specification to include: 1 or 2 (and 3 if applicable).
1. End item materials are A-rated according to MAPTIS or applicable IP materials process/segment specification.(A)
 2. Review of end item design and review of final configuration confirms details and implementation of one of the flammability control strategies listed in the rationale (Section D.4.7.1.1 Rationale – Flammable Materials). (A and I).
 3. Inspection of procedures shows that operational controls are in place to identify specific operational limitations or use of end item flammable materials per MUA and planned operations. (I)
- B. Flammability testing in the ISS worst-case operating environment per NASA STD-6001 (Test 1 for general materials or Test 4 for powered electrical cables) or applicable IP materials process/segment specification shows the materials meet the flammability requirements. (T)

4.7.1.2 MATERIAL OFFGASSING IN HABITABLE AREAS

Offgassing products produced by end items **shall** be below toxic levels.

Rationale

This requirement only applies to end items in the ISS pressurized environment. Offgassing is the release of chemicals from materials – the new car smell is an example of material offgassing. Offgassing can result in a toxic atmosphere if chemical compounds accumulate in a spacecraft closed environment and reach concentrations above their Spacecraft Maximum Allowable Concentrations (SMAC). End items are assessed to ensure they do not generate toxic levels of offgassing products into the ISS environment. MAPTIS contains a listing of materials and end items that have been subjected to offgassing tests. The material offgas rating in MAPTIS is based upon the amount of the material that is allowed. If not all major use materials are listed in the MAPTIS database, toxic offgassing testing is normally required.

If the total mass of polymeric materials in an end item, or a system with multiple end items (such as a set of CubeSats with deployer) is less than 20lb, it is exempt from offgas testing or evaluation unless it contains one of the following excluded materials:

- *COTS end items that include uncured adhesives, lubricants, cleaning wipes, markers, pens, other items with uncontained liquids or gels, and hardware used for uncontained on-orbit processing of materials at elevated temperatures (such as 3D printers) are not exempt.*

SSP 51721

Baseline

- *Custom end items that include the materials listed above or foams and foamed fluorocarbons (cables) are not exempt.*

If excluded materials are present or the total mass of polymeric materials exceeds 20 lb, an offgassing test could be required or an offgassing evaluation could be conducted to verify that all excluded materials and major use polymeric materials are used in quantities less than the ISS maximum limit weight in the MAPTIS database.

Additional rationale for this requirement can be found in Appendix D.4.7.1.2.

4.7.1.2.1 VERIFICATION – MATERIAL OFFGASSING IN HABITABLE AREAS

Verification is considered successful when the following are completed: A or B

- A. The total mass of polymeric materials in an end item, or set of related end items, is shown to be less than 20 lbs and none of the excluded materials (identified in the rationale) is present. This information (total mass, mass of polymeric materials, and that the excluded materials are not present) will be documented in the HR. (A)
- B. All excluded materials and major use polymeric materials have been confirmed to be used in quantities less than the ISS maximum limit weight, based on one or both of the following:
 1. Offgassing evaluation of end item materials. (A)
 2. Offgassing tests of end item per NASA-STD-6001, Test 7 or ISSP approved equivalent are performed and the toxic hazard index (T value) is shown to be less than 0.5 for the total number of identical end items flown. (T)

4.7.1.3 MATERIALS COMPATIBILITY

End item materials and fluids **shall** be compatible.

Rationale

Material compatibility refers to chemical reaction between a fluid and materials in contact with that fluid, resulting in unacceptable degradation of the materials or the fluid. In some cases, chemical reaction can lead to ignition of the materials or the fluid. Ignition of a material may occur in contact with oxidizer fluids like oxygen and ignition of a fluid may occur by a material catalyzing exothermic decomposition of hypergolic fuels like hydrazine. Material compatibility can be a concern with fluids used in cleaning, test, and operation in all system environments and service life. NASA-STD-6001, Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures addresses hazardous fluids such as gaseous oxygen, liquid oxygen, fuels, oxidizers, and other fluids that could chemically or physically degrade the system or cause a potentially hazardous exothermic reaction.

Special attention should be paid to end item materials used for or with an enriched oxygen environment. An Oxygen Compatibility Assessment (OCA), as required by NASA-STD-6001, is necessary for pressurized oxygen system hardware. The assessment may identify areas where testing is required before the hardware can be

SSP 51721
Baseline

approved. An OCA may also be necessary for compressed air systems and pressurized systems containing enriched oxygen (greater than 21 percent oxygen by volume). The need to conduct an OCA for these systems will be determined during the initial safety review. It is recommended that the White Sands Test Facility be consulted when performing an OCA.

4.7.1.3.1 VERIFICATION - MATERIALS COMPATIBILITY

Verification is considered successful when applicable analyses and/or tests per NASA-STD-6001 are complete. (A and/or T).

4.7.2 HAZARDOUS MATERIALS

A hazardous material is any item, substance, or agent (such as physical, chemical, biological, and/or radioactive), which has the potential to cause harm to the crew, the ISS environment, and/or equipment either by itself or through interaction with other materials and/or factors. The use of hazardous materials cannot always be avoided in spaceflight, so requirements are established for hazard prevention through controlling the release of hazardous materials.

The two hazard control schemes (reference Section 3.3) used to control hazardous materials: design to tolerate failures (failure tolerance) and DFMR, are applied to the end item design based on the hazard severity (reference Section 4.1.1). Failure tolerance and DFMR are separate and distinct methods for hazard control. To avoid confusion, and possible error, the respective requirements for failure tolerance and DFMR (including those for joining methods, number of barriers/seals to control hazards, fracture control, materials certification, etc.) should be considered separately when being applied to the end item design. Criteria for utilizing DFMR to prevent release of hazardous materials are provided under the applicable topic-specific safety requirements (reference Section 4.0), such as pressure systems, propulsion, batteries, and capacitors. Criteria for utilizing failure tolerance to prevent release of hazardous materials are provided here.

Using Failure Tolerance to Prevent Release of Hazardous Materials

The failure tolerant design approach applies levels of hazard controls to prevent hazards. The required number of levels of hazard controls are based on the hazard severity. Marginal hazards are required to have one level of hazard control. Critical hazards (single failure tolerant) are required to have two levels of hazard control. Catastrophic hazards (two failure tolerant) are required to have three levels of hazard control. The appropriate number of levels of control should exist for all phases of use of the end item hardware. Phases of use include, but are not limited to, launch, stowage, operations (including sample manipulations and maintenance), return, and/or disposal (including trash/waste). The preferred application of levels of hazard control to prevent the release of hazardous materials is through Levels of Containment (LoC).

Levels of Containment (LoC)

LoC requires concentric independent layers (physical barriers) in the end item design where each individual layer is of a design integrity able to contain the hazardous

SSP 51721
Baseline

material. The required number of independent levels of physical barriers is based on the hazard severity as identified above and is maintained throughout the flight. If any of the levels of containment are opened during the mission and, then, resealed for continued containment or exchanged for a different level of containment, reestablishing the containment is verified by leak test, approved procedure, or design certification. Manipulations or changes in the levels of containment may require the addition of another level of containment prior to removal or exchange in order to maintain the required number of levels of containment. Verification method(s) are approved by the ISRP.

Consideration for Individual Levels of Containment

Each individual level of containment is required to be functionally separate, independent and capable of containment (no leakage or erosion) under the worst-case conditions of use. Conditions of use, also referred to as environments, generally consist of all the environments that the end item will be exposed to, including handling, exposure durations, appropriate combinations of thermal, vibration, pressure (including module depressurization), mechanical, cycle life, and others as appropriate.

Compatibility of the contained hazardous material and materials used for the level of containment is required to be established, including the joints and seals. Compatibility should address exposure of Levels of Containment (LoC) materials over the duration of all phases and conditions of use and any preparatory fluids, such as cleaning fluids.

Joints and closures (metallurgically fused, sealed, or chemically/thermally bonded) are considered to be single barriers for their respective level. A single seal closure is acceptable for a given single level of containment when independent seals are used. Single non-metallic adhesive or heat/chemical-fused joints are acceptable in Levels of Containment (LoC) applications provided that such joints are specifically evaluated for structural capability and compatibility.

Individual levels in the LoC approach are not “fracture critical” and fracture control measures need not be applied when the failure tolerant LoC approach is used.

Common cause failure should be addressed if the same materials are used to provide multiple LoC. For example, use of multiple elastomeric seals should address degradation based on the limited life of the seals.

The following items are routinely used in LoC designs. Guidance is provided here for consideration.

Quick Disconnect (QD) Connectors: QDs may be used as part of an individual level or levels of containment. When using QDs, mating/demating of the connectors may change the LoCs so an additional level of containment may need to be established before the operation takes place to ensure the required number of LoC are maintained. Consideration should be given to the potential for liberation of fluid from dead space in the QD connectors during mating/demating and the formation of micro-droplets (identified below).

SSP 51721

Baseline

Plastic Bags: Plastic bags (e.g., Ziploc® bags) can be used as an individual level of containment; however, there are limitations. Most types of plastic bags are flammable and their use should address flammability concerns. Use of a plastic bag as a level of containment should also assess for material compatibility and potential puncture of the bags. It is recommended that plastic bags be used for no more than one level of containment.

Pressure Systems: Pressure systems, defined based on pressure and contents, can be used to contain hazardous materials. Pressure systems (pressure vessels, components, lines, fittings, etc.) may be used as an individual level or levels of containment in a LoC approach. Compatibility between the pressure container and the contained material is required to be established and each containment level demonstrated to prevent leakage on the flight hardware. Pressure systems that are the only barrier to a catastrophic leakage (for which rupture and leakage are catastrophic) are qualified through DFMR for leakage and rupture. Refer to Section 4.2.3, Pressure Systems for details on utilizing pressure systems and defining the MDP for the system.

Design integrity of each level of containment on flight units is verified by testing or other defined methods approved by the ISRP. Testing should conservatively encompass all phases and conditions of use to which the end item will be exposed. In addition, all potential physical states of the hazardous material (gaseous, liquid, and solid states) are taken into account. It is incumbent on the end item provider to deliver the appropriate verification information, including design, qualification, compatibility assessments, and related testing information and data.

Utilizing Controls Instead of Containment to Prevent Release of Hazardous Materials

The ISSP recognizes the need for flexibility in engineering designs and crew operations to efficiently and safely perform experiments on ISS. The ISSP, ISRP, and NASA SMEs have actively investigated alternative ways of safely working with hazardous materials outside of traditional containment. For biological material that is biohazardous, the preferred failure tolerance approach to prevent release is LoC.

Alternatives to a physically enclosed level of containment should be proven as equivalent to a physical barrier in preventing the release of hazardous materials. Alternatives to levels of containment, levels of control, are also be reviewed and specifically approved by the ISRP with documentation of the full rationale/justification for acceptability included in the SDP and related HRs. The required number of independent levels of control is based on hazard severity as identified above and must be maintained throughout the flight. Each level of control is required to be functionally separate and compatible with the hazardous material that is being controlled over the duration of all phases and conditions of use. Any change or manipulation in the levels of control may require the addition of another level of control prior to removal or exchange in order to maintain the required number of levels of control. Verification method(s) are approved by the ISRP.

SSP 51721 Baseline

Examples of alternatives to containment that have been previously accepted as an equivalent level of control include: use of absorbent/neutralizing materials, hydrophobic membranes, filters or screens, scrubbers or catalysts, short duration of exposure with no forcing function, tortuous leak path, utilization of specific Material Properties as Controls (MPAC) (such as hydrophobicity and hydrophilicity), utilization of unique or special operations, and no physical crew access. Alternatives to containment that may be acceptable as an equivalent level of control with the appropriate verification include: utilization of specific forces in the microgravity environment (such as utilizing airflow to intentionally direct hazardous materials) and utilization of other MPAC (such as surface tension and adhesion, etc.).

Negative pressure might be counted as a control, equivalent to containment, under certain circumstances. It should be independently applied and maintainable, and must exhaust safely and not present a danger of contamination to another system. There may be other alternatives or approaches that alone or used in combination under certain circumstances might be considered an appropriate level of control for the failure tolerance approach.

Any use of operational controls or special instructions for the crew should be coordinated with the operations community. The use of operational controls are reviewed and approved by the ISRP on a case-by-case basis.

For end items planning to utilize controls to prevent release of hazardous material consideration should be given to the following.

Formation of Micro-droplets: Production of micro-droplets should be considered in any end item hazardous material manipulation involving fluids (such as fluid transfer, and/or extraction). Micro-droplets are formed when any two wetted surfaces are separated (for example opening a container with fluid or transferring fluid between containers). The size of one micro-droplet is considered to be 0.5 mm diameter which equates to a volume of $6.5E-5$ cc or 0.0065 μ L. When compared to the size of a droplet which is 0.05 mL (50 μ L), the size of a micro-droplet is quite small and not readily visible. The formation of micro-droplets is seen to produce quantities greater than just 1 micro-droplet. The concern with the production of micro-droplets relates to the hazardous fluid or fluids being manipulated and released. Some hazardous fluids with high hazard ratings (see below) can cause damage or infection in human soft tissues, and contaminate the environment in volumes as small as or smaller than a micro-droplet. With some hazardous fluids, the hazard rating will increase after the fluid evaporates to a more concentrated (less dilute) material. If the material is not hazardous in micro-droplet quantities, then only droplets large enough to be hazardous are controlled.

Airflow in Microgravity: With the change in gravitational force not pulling hazardous materials to the ground in microgravity, other forces acting on hazardous materials are more of a concern and should be considered in preventing the release of hazardous materials. Airflow and air currents produce a force on released hazardous materials and can suspend fluids (such as micro-droplets and droplets) and particles in the air for a long duration. Released hazardous materials can be carried on the air currents

SSP 51721
Baseline

throughout the vehicle, resulting in crew exposure and contamination of the crew living environment.

Contamination: When developing end item protocols and operations, thought should be given to preventing cross contamination through transfer of hazardous materials. Any shared hardware should be appropriately cleaned.

Controls used as alternatives to a level or levels of containment are verified through testing or other quantifiable methods approved by the ISRP. Testing should conservatively encompass all phases and conditions of use to which the end item will be exposed and potential physical states of the hazardous material (gaseous, liquid, and solid states). It is incumbent on the end item provider to deliver the appropriate verification information and to identify any limitations on the level of control (such as a specified time duration). All hazard controls as well as any additional risk in replacing levels of containment or design controls will be carefully reviewed and assessed by the ISRP for adequacy in prevention of hazards. ISRP approval will be given on a case-by-case basis and is not guaranteed.

Levels of Containment/Control (LoC/C)

Levels of containment and levels of control used as alternatives to containment are collectively referred to as LoC/C. These can be combined to prevent the release of hazardous materials. One example of a combined approach for LoC/C is utilization of a capillary tube inside a plastic bag for the launch and stowage phases and removal of the plastic bag and utilization of MPAC (such as adhesion of the hazardous material to the inside surface of the capillary tube) during the end item operations phase. The quantity of levels in this example is based on critical hazard severity. The capillary tube and plastic bag would be qualified as a level of containment and the MPAC would be qualified as a level of control.

Substitutes for End Item Provided Individual Levels of Containment/Control

The ISSP has developed ISS hardware that can be used as substitutes for end item provided levels of containment/control. The end item provider using ISSP resources for LoC/C is responsible for addressing the use of the resources in the end item safety documentation (SDP and related HRs). Specific ISS resources are listed here; there may be other Government Furnished Equipment (GFE) available for use as a level of containment/control.

ISS Glove Boxes: The ISSP has developed and maintains glove boxes (e.g., Microgravity Science Glovebox (MSG) and Life Science Glovebox (LSG)) on ISS to assist in performing experiments on ISS. Utilization of one of the glove boxes on ISS during the removal or opening of an individual level of containment is an acceptable replacement for one level of containment. The ISSP developed glove boxes also have negative pressure capability that functions as a control that is equivalent to a single level of containment. In total, the ISSP glove boxes could be used to provide two separate types of controls (one level of containment and one level of control). Use of one of the glove boxes is coordinated/approved by the ISSP.

SSP 51721

Baseline

ISS Glove Bags: The ISSP has also developed and maintains glove bags (e.g., Disposable Glove Bag (DGB) and ISS Portable Glove Bag (IPGB)) on ISS that are acceptable replacements for one level of containment. Use of one of the glove bags is coordinated/approved by the ISSP.

ISS Systems: End items connecting to ISS Systems can utilize ISS Systems (such as the ISS Vacuum System (VS) and ISS System responses as part of the hazard control scheme. The system response should be appropriate for controlling the hazard and be documented. For example, an end item connecting to and utilizing the ISS Thermal Control System (ITCS) Moderate Temperature Loop (MTL) or Low Temperature Loop (LTL) cooling loops can utilize the ISS System's response when leakage is detected as one of the controls to prevent leakage of ITCS fluid. Use of ISS Systems is coordinated/approved by the ISSP.

Combining Failure Tolerance (LoC/C) and DFMR

LoC/C and DFMR can be combined to prevent the release of hazardous materials. One example of a combined approach is utilization of a single walled metallic enclosure (such as a vessel or box) with multiple seals at all interfaces. The quantity of seals would depend on the hazard severity and would be independently qualified. The metallic enclosure would be qualified as DFMR and the seals would be qualified as LoC. In this case, qualifying the metallic enclosure as DFMR may result in the container being classified as "fracture critical" depending on the hazardous material involved.

ISS Safety Review Panel Responsibility for Hazardous Materials

The ISRP relies on the NASA SMEs to characterize potential risks and the hazard severity associated with the release of a particular hazardous material. The ISRP is responsible for reviewing and approving the end item's design and controls to prevent release of a hazardous material based on the hazard severity through all phases and conditions of use. All final determinations of required LoC/C or appropriate replacements for individual LoC are made by the ISRP.

Hazard Ratings and the Hazardous Materials Summary Table (HMST)

End item hazardous materials are assessed by NASA SMEs and assigned specific hazard ratings based on the type of hazardous material and potential hazards to the crew, the habitable environment and/or equipment. Hazard ratings are scaled to define the potential risk and hazard severity for the release of hazardous materials without regard to physical containment. End item hazardous material hazard ratings may include:

- Toxicity Hazard Level (THL), scale: THL-0 to THL-4 – Addresses all chemicals and potential chemically-induced toxicity hazards; the NASA Subject Matter Experts (SME) is the JSC Toxicology and Environmental Chemistry Group.

Reference Section 4.7.2.2 for Chemicals.

- Biosafety Level ((BSL), scale: BSL-1 to BSL-4) – Addresses all biological material and potential biohazards; the NASA SME is the NASA/JSC Biosafety Review Board (BRB).

SSP 51721
Baseline

Reference Section 4.7.2.4 for Biological Material Release.

- Flammability Hazard Level ((FHL), scale: 0-4) – Addresses chemicals that are flammability hazards; the NASA SME is the NASA/JSC Materials and Processes Branch.

Reference Section 4.7.2.2 for Chemicals.

- ECLSS Hardware Impact Rating (E Ratings, scale: E0 to E6) – Addresses the impacts of exposure to chemicals or physical agents on ECLSS resources, consumables and the rated service life of the system and/or essential components of the system; the NASA SME is the NASA/ISS ECLSS Engineering Group.

Reference Section 4.7.2.2.1 for Chemical Release.

- ECLSS Cabin Environmental Impact Rating (scale: A to D) – Addresses the ability of ECLSS to recover the cabin atmosphere to acceptable levels when hazardous material is released; the NASA SME is the NASA/ISS ECLSS Engineering Group.

(Note: Maintaining and/or recovering the cabin atmosphere is taken into consideration with the final assigned THL.)

Reference Section 4.7.2.2.1 for Chemical Release.

Hazard Response Level ((HRL), scale: 0 to 4) – Identifies what immediate action is required to protect the crew in response to a spill or leakage of a particular hazardous material on orbit; it reflects the minimum for post-spill safety clean-up and does not necessarily reflect the level of containment/control required for the end item design. HRL is an integrated response rating determined by the most severe rating for toxicity, biosafety, and flammability hazards associated with a particular hazardous material or grouping of hazardous materials. The HRL is managed by the ISSP via flight rule and is listed here only for awareness.

The hazard ratings are collectively documented in the end item's HMST to clearly define the range of hazards that are associated with the end item's hazardous materials. The HMST also captures materials that, alone, may be considered to be non- or marginally hazardous but create physiological and environmental hazards when released in significant quantities (for example water and particulates) and are, thus, considered to be hazardous. Physical agents as described in Section 4.7.2.5, Physical Agents, are not rated under a scaled hazard rating but are classified based on potential release and hazard severity.

The HMST is a listing of all identified hazardous materials that is tracked through the development and launch of the end item. Once manifested for a flight, the end item HMST is tracked as part of the flight specific HMST and then the ISS on orbit HMST.

The NASA SME developed and maintained HMST serves as a type of Safety Data Sheet for ISS to identify all the hazardous materials (both materials that are hazardous by rating and by physiological and environmental impacts). The HMST is used to

SSP 51721

Baseline

identify materials in the event of an inadvertent leak or release of hazardous materials; the HRL and any special notes and comments captured in the HMST identify how to respond appropriately.

The hazard ratings should be used by end item providers as criteria in the designing of flight hardware to ensure adequate LoC/C for the hazard severity. If there is more than one hazardous material used within an end item, the hazard severity will be determined by the hazardous material with the highest hazard rating. If an end item's hazardous materials are segregated in separate enclosures or containers, the enclosure is required to have the appropriate LoC/C based on the hazard severity through all phases and conditions of use as described above.

Hazardous materials used in the unpressurized (external) environment are not included in the HMST unless they will be brought into the pressurized habitable environment. Hazard severity of externally released end item hazardous materials is assessed by the NASA/JSC Materials and Processes Branch, the ISS Space Environment Group, and the ISRP.

Samples taken from the ISS environment and crew are included in the HMST. Repurposed ISS items (such as food or drinking water utilized for an experiment) are included upon request by the ISRP.

Additional details and guidance for specific end item hazardous materials and the HMST is provided with the applicable requirement rationale.

Note: Radioactive material is not assigned a scaled hazard rating as all radioactive material is considered to be the highest hazard severity (catastrophic). The NASA SME is the NASA/JSC Space Radiation Analysis Group (SRAG). Radioactive material is documented on JSC Form 44. Details are provided by the SRAG to the JSC Toxicology and Environmental Chemistry Group for inclusion in the end item HMST.

Levels of Containment/Control Reference Table

Table 4.7.2-1 is provided as a guideline for the relationship between LoC/C and hazardous material hazard ratings.

TABLE 4.7.2-1 LEVELS OF CONTAINMENT/CONTROL AND HAZARD RATINGS

	0 LoC/C Not a Hazard	1 LoC/C Marginal Hazard	2 LoC/C Critical Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard
Hazard Response Level (HRL) (Color of Label)	0 (GREEN)		1 (BLUE)	2 (YELLOW)	3 (ORANGE)	4 (RED)
Toxicity Hazard Level (THL)		0	1	2	3	4
Biosafety Level (BSL)		1	2 (Mod)	2 (High)		
Flammability Hazard Level (FHL)	0		1	2	3	4
Environmental Control and Life Support System (ECLSS) Hardware Impact Rating (E-Rating)	E0-E1	E2-E3	E4-E6			
	0 LoC/C Not a Hazard	1 LoC/C Marginal Hazard	2 LoC/C Critical Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard	3 LoC/C Catastrophic Hazard

Notes:

- [1] HRL (color indicated in table) is an indication for the integrated on-orbit response for THL, BSL and FHL; HRL reflects the minimum for post-spill safety clean-up and does not necessarily reflect the level of containment/control required for the end item design
- [2] LoC/C are assessed by the ISRP as part of the safety review process (reference SSP 30599)
- [3] Controls for Marginal Hazards are documented in the SDP and/or may be verified through the applicable IRD
- [4] THL 2-4, BSL-2H, and FHL 2-4 all require 3 LoC/C
- [5] THL 4 requires ISS Program Manager approval for use on ISS
- [6] Varying LoC/C for FHLs are based on hazardous material properties/quantities in the end item
- [7] E-Ratings are included to show the relationship to LoC/C and are not part of the HRL
- [8] LoC/C for physical agents are also based on the hazard severity (reference Section 4.7.2.5)
- [9] The difference between end item design requirements (LoC/C) for FHL 1-3 and on-orbit hazardous response (HRL) is under review.

<TBR 4-10>

Since the end item design is predicated on the hazard ratings, end item hazardous materials should be submitted for NASA SME review as early as possible in the end item's design development. Request for NASA SME review of hazardous materials is submitted for every flight in accordance with SSP 30599, via electronic submittal

SSP 51721
Baseline

spreadsheet (<https://www.nasa.gov/feature/hazardous-material-summary-tables-hmsts>) or JSC Form 44 (Radioactive Materials (NAMS request is required for login)).

NOTE: End items with large numbers of different hazardous materials will require additional time for NASA SME review.

Verification for the HMST

All materials used in an end item are verified throughout the design and development process. There is a two-step process used to verify the data in the end item's HMST. The candidate hazardous materials are approved when they are first proposed for use and documented on the end item's HMST; this is called the Verification-1 or V1 process. After the V1 process is complete, hazardous materials can only be reduced or deleted, no additions are allowed. Hazardous material quantities are finalized when they are loaded into the flight hardware, this is the Verification-2 or V2 process. In the event end item samples need to be reloaded for any reason, the V2 process is repeated. For additional details on the HMST verification process, reference JSC 27472, Requirements for Submission of Data Needed for Toxicological Assessment of Chemicals to be Flown on Manned Spacecraft.

4.7.2.1 HAZARDOUS MATERIALS EXTERNAL RELEASE NEAR OR THROUGH THE ISS

Any material whose external release near or through the ISS would create a hazard **shall** be controlled.

Rationale

The primary concern for this requirement is the release of hazardous fluids (liquids/gases).

This requirement applies to all end items capable of releasing hazardous materials external to the ISS. This includes externally located end items and VVs and internally located end items utilizing the ISS Vacuum System (VS) (consisting of the Vacuum Exhaust System/Waste Gas and the Vacuum Resource System/Vacuum Vent). It is established to prevent immediate and/or latent damage (such as soaking into Multilayer Insulation (MLI) blankets or insulation) damage from corrosion and/or contamination to the EMU, ISS and/or VV equipment. Release of hazardous material near or through the ISS should also not create a hazard to other externally located end items.

Any planned hazardous material release near or through the ISS should be negotiated with the ISSP. Hazardous fluid systems should prevent the release of fluids unless the venting/dumping has been negotiated with the ISSP.

Additional rationale for this requirement can be found in Appendix D 4.7.2.1.

4.7.2.1.1 VERIFICATION – EXTERNAL RELEASE OF HAZARDOUS MATERIALS NEAR OR THROUGH THE ISS

Verification is considered successful when the following are completed: A and (B and/or C) and D (and E if applicable)

- A. Potential hazardous materials are submitted for NASA SME assessment (I)

SSP 51721
Baseline

Chemical Release verifications are addressed in Section 4.7.2.2.1.

- B. DFMR approach for controlling release; verifications are described in detail in the topic-specific safety requirements in Section 4.0.
- C. Failure tolerance approach for controlling release (LoC and/or appropriate controls):
 - 1. Review of end item design shows that LoC and/or controls are commensurate with the hazard severity. (I)
 - 2. End item LoC/control design is confirmed by qualification and acceptance testing, including independent testing of each LoC/C. (T)
 - 3. End item materials and material processing are reviewed and approved by NASA Materials Group, including (if applicable) compatibility with EMU. (A)
 - 4. End item flight hardware is built in accordance with approved drawings and assembled per approved procedures. (I)
 - 5. End item materials compatibility testing or analysis has been performed for both preparatory cleaning materials and hazardous materials. (T or A)
- D. The end item's hazardous materials have been properly loaded per pre-flight procedures/processing (I)
- E. (If applicable) For end items planning to release/vent hazardous materials the following are provided:
 - 1. Intentional release of hazardous materials has been approved by the ISSP. (A)
 - 2. Venting analysis demonstrates that:
 - a) Vent position and orientation are away from ISS and other end items and (A)
 - b) Vent effluents are not chemically reactive with ISS surfaces and do not pose an immediate or latent hazard. (A)
 - 3. Release is controlled to prevent exposure and/or damage to the EMU, ISS and/or VV equipment. (A or I or T)

4.7.2.2 CHEMICALS

Requirements for the use of end item chemicals are established to prevent hazards associated with chemicals such as impacts to crew health and environmental contamination. Chemicals are addressed here based on the prevention of end item chemical release (Section 4.7.2.2.1, Chemical Release) and based on the reduction in hazard controls during operations with THL-1 and FHL-1 liquids (Section 4.7.2.2.2, Reduction in Failure Tolerance for Chemicals (Liquids) During Operations).

4.7.2.2.1 CHEMICAL RELEASE

End item chemicals **shall** be controlled to prevent release.

SSP 51721
Baseline

Rationale

This requirement does not apply to crew food, drinking water from the galley, crew personal preference items, or items considered to be structural components. If any of these items are used in a manner different than what is intended here (such as for experimental purposes), an evaluation may be requested by the ISRP during the safety review process.

This requirement applies to all chemicals that are located in or may be introduced into the pressurized habitable environment (including end items returning from or routinely used in the unpressurized environment). It is established to protect the crew from chemically-induced toxicity hazards and/or to protect the environment and VV/ISS equipment from contamination hazards. Toxicity hazards are chemicals that may be harmful to crews (including physiological effects such as irritation to skin or eyes).

This requirement encompasses all physical states and compositions (for example: solid, liquid, vapor, gas, gel, grease, and powders/particulates) for chemicals and potential products of end item chemical reactions. Radioactive materials are a unique set of chemicals addressed in Section 4.7.2.6, Radioactive Material Release. For particles that are chemically inert and/or insoluble in water, refer to Section 4.7.2.5 for Physical Agents.

Additional rationale for this requirement can be found in Appendix D.4.7.2.2.1.

4.7.2.2.1.1 VERIFICATION - RELEASE OF CHEMICALS

Verification is considered successful when the following are completed: A and (B and/or C) and D (and E and/or F (if applicable))

- A. Chemicals have been assessed and assigned hazard severity ratings through both of the following: (1 and 2)
 - 1. Listing of end items chemicals are submitted for NASA SME assessment via electronic submittal spreadsheet. (I)
 - 2. HMST is reviewed and V1 form signed by end item provider. (I) (V1 process)
- B. DFMR approach for controlling release; verifications are described in detail in the topic-specific safety requirements in Section 4.0. (A, I, T)
- C. Failure tolerance approach for controlling release (LoC and/or appropriate controls) all of the following are provided: (1, 2,3, 4, and 5):
 - 1. Review of end items design for LoC and/or controls are commensurate with the hazard severity. (I)
 - 2. End item LoC/Control design is confirmed by qualification and acceptance testing, including independent testing of each LoC/C. (T)
 - 3. End item materials and material processing are reviewed and approved by NASA Materials Group. (A)

SSP 51721

Baseline

4. End Item flight hardware is built in accordance with approved drawings and assembled per approved procedures (I)
 5. End item materials compatibility testing or analysis has been performed for both preparatory cleaning materials and hazardous materials. (T or A)
- D. Flight sample loading, the end item's chemicals have been properly loaded per pre-flight procedures/processing. (I) (V2 process)
- E. (If applicable) For end items manipulating chemicals on orbit and/or using LoC/C involving operations, to prevent chemical release, both of the following are provided: (1 and 2)
1. The hazard control is identified and proven to be effective in preventing chemical release. (A and/or T)
 2. Inspection of procedures shows that operational controls are in place, including inspection for leakage/loss of containment/control before removing containment/control and cleaning after operations for common use hardware. (I)
- F. (If applicable) For end items returning from exposure to the external environment, both of the following are provided for the controls to prevent contamination of the ISS pressurized environment, both of the following are provided: (1 and 2)
1. The hazard control is identified and proven to be effective in preventing chemical release. (A or T)
 2. Inspection of procedures shows that operational controls are in place to prevent contamination of the ISS pressurized environment. (I)

4.7.2.2.2 REDUCTION IN FAILURE TOLERANCE FOR CHEMICALS (LIQUIDS) DURING OPERATIONS

During operations, end items **shall** provide a minimum of one level of control to prevent release of THL-1 and FHL-1 liquids.

Rationale

This requirement applies exclusively to THL-1 and FHL-1 liquids during the end item's operational phase (i.e., setup, data collection, fluid manipulations, and tear down). This requirement does not apply to THL-1 or FHL-1 liquid that would have a hazard severity higher than critical due to another hazard rating. This requirement also does not apply to any other hazardous material that would be rated under THL or FHL ratings or other hazard ratings (for example: non-liquid THL-1 materials, non-liquid FHL-1 materials, biological materials, radioactive material, etc.). This requirement does not impact the on orbit operational response that would occur in response to an inadvertent spill of hazardous materials.

Controls to prevent release of chemicals are provided through failure tolerance or DFMR based on the hazard severity. This requirement is assuming application of the failure tolerance control method, reference Section 4.7.2 for details. The release of THL-1 or FHL-1 liquid is considered to be a critical hazard severity, which nominally requires

SSP 51721
Baseline

two levels of control (reference Tables 4.7.2-1, 4.7.2.2.1-1, and 4.7.2.2.1-2). When utilizing a failure tolerance approach, the control to prevent release of hazardous materials has traditionally been through the implementation of levels of containment. All chemicals should maintain a minimum of one control to prevent release (containment or other appropriate controls equivalent to containment) at all times.

The single level of control addressed in this requirement should be successfully demonstrated and verified to remain valid during all expected, worst-case environmental conditions and prevent the release of the THL-1 or FHL-1 liquid. Upon completion of operations, the second level of control will be re-established at the earliest opportunity. Two levels of control are still required during launch, stowage/trash, and return..

The ISSP is committed to utilizing the ISS as a functional laboratory. The ISRP in coordination with the NASA/JSC Human Health and Performance Directorate, have concluded that allowing for the reduction in the level of control (for a limited timeframe) during THL-1 and FHL-1 liquid operations presents an acceptable risk that will provide a greater opportunity for the utilization of ISS. THL-1 liquids are irritants and may cause minimal systemic effects but are not expected to result in long-term performance impacts, lasting internal tissue damage, or permanent eye damage. FHL-1 liquids are considered to be low risk for creating a fire with serious consequences.

Verifying Level of Control: End item developers utilizing this requirement should review the information provided in Section 4.7.2 for levels of containment and utilizing controls instead of containment to prevent release of hazardous materials. The utilized one level of control during operations is substantiated through quantifiable means (for example using small quantities of one or two hazardous materials for a specified and limited time frame) by the end item provider. Operations occurring in the open volume of ISS (such as on the Maintenance Work Area (MWA)) should prevent the release of micro-droplets. Documentation of chemical usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP. All final determinations of acceptability of LoC/C and hazard control mitigations (for example: pre-positioning of required contingency cleanup materials and/or personal protective equipment) will be carefully reviewed and assessed by the ISRP for additional risk and adequacy in prevention of hazards. ISRP approval will be given on a case-by-case basis and is not guaranteed.

4.7.2.2.2.1 VERIFICATION - FAILURE TOLERANCE REDUCTION FOR CHEMICALS (LIQUIDS) DURING OPERATIONS

The verifications in Section 4.7.2.2.1.1 should be met for all end item chemicals. The following verifications are additional verifications for using one level of hazard control during the end item's operational phase.

Verification is considered successful when the following are completed: A and B

- A. For end items using one level of containment/control to prevent chemical release during operations, both of the following are provided: (1 and 2)

SSP 51721

Baseline

1. The level of containment/control is identified and proven to be effective in preventing chemical release throughout end item operations. (A or T)
 2. Inspection of procedures shows that operational controls are in place to prevent release. (I)
- B. Upon completion of the operational phase, an additional (second) level of containment/control is established, both of the following are provided: (1 and 2)
1. The control is identified and proven to be effective as a second level of containment/control by qualification and acceptance testing, including independent testing. (T)
 2. Inspection of procedures shows that operational controls are in place to establish or re-establish the second level of containment/control prior to stowing the end item. (I)

4.7.2.3 RADIOACTIVE MATERIAL RELEASE

Radioactive materials **shall** be controlled to prevent release.

Rationale

This requirement applies to all radioactive materials that are located in or may be introduced into the pressurized habitable environment and are not considered exempt or under exemption per the U.S. Nuclear Regulatory Commission (NRC) Regulations Title 10, Code of Federal Regulations (CFR). It is established to protect the crew from physiological impacts and the environment and vehicle from contamination due to exposure to radiation source material and secondary emissions. Radioactive material is a source of ionizing radiation; requirements for other sources of ionizing radiation are addressed in Section 4.6.2, Ionizing Radiation and Section 4.3, Electrical. All radioactive material (for example radioactive isotopes) is classified as a catastrophic hazard (the highest hazard severity) Accordingly, the primary radioactive material or source of radiation is controlled to prevent release through failure tolerance (LoC or appropriate controls) or DFMR, reference Section 4.7.2, Hazardous Materials, for details. A material capable of absorbing any primary or secondary radioactive emissions is provided in the design; this can be part of the hazard controls or a separate design feature. Emissions that cannot be shielded are kept As Low As Reasonably Achievable (ALARA).

Additional rationale for this requirement can be found in Appendix D.4.7.2.3.

4.7.2.3.1 VERIFICATION– RADIOACTIVE MATERIALS RELEASE

Verification is considered successful when the following are completed: A and (B and/or C) and D (and E if applicable)

- A. Listing of end item radioactive materials is submitted for NASA SME assessment via JSC Form 44 (I)
- B. DFMR approach for controlling release; verifications are described in detail in the topic-specific safety requirements in Section 4.0. (A, I, T)

SSP 51721

Baseline

- C. Failure tolerance approach for radioactive material (LoC and/or appropriate controls), all of the following are provided: (1, 2, 3, 4, and 5):
 - 1. End item design is confirmed to provide three LoC or controls to prevent release by qualification and acceptance testing, including independent testing of each LoC/C. (A, I, and T)
 - 2. End item design is confirmed to provide primary and secondary emission absorption either as part of the controls to prevent release or through the design features by qualification and acceptance testing. (A, I, and T)
 - 3. End Item materials and material processing are reviewed and approved by NASA Materials Group. (A)
 - 4. End item flight hardware is built in accordance with approved drawings and assembled per approved procedures. (I)
 - 5. End item materials compatibility testing or analysis has been performed for both preparatory cleaning materials and radioactive materials. (T or A)
- D. The end item's radioactive materials have been properly loaded per pre-flight procedures/processing. (A, I)
- E. (If applicable) For end items that can release radiation during operations or hardware use, both of the following are provided: (1 and 2)
 - 1. Control(s) should be identified and proven effective in preventing/minimizing (ALARA) the release of radiation during operations or use. (A or T)
 - 2. Inspection of procedures shows that operational controls are in place to prevent/minimize (ALARA) release. (I)

4.7.2.4 BIOLOGICAL MATERIAL RELEASE

End item biological materials **shall** be controlled to prevent release.

Rationale

This requirement does not apply to crew food or crew personal preference items.

This requirement applies to all biological materials that are located in or may be introduced into the pressurized habitable environment. It is established to protect the crew and environment from immediate or latent biohazards, including contamination of food and water supplies. Biohazards are biological materials or biological agents that may be harmful to the crew and/or to the environment. This requirement encompasses live and cultured biological materials used in end items and/or collected as samples from ISS. This requirement also applies to vectors of biological materials such as animals and plants, non-biological materials such as soil or dust, and environmental conditions such as warm, moist air that may harbor or promote the growth of biological materials.

Controls to prevent release of biological materials are provided through failure tolerance or DFMR based on the hazard severity, reference Section 4.7.2, Hazardous Materials, for details. The preferred method to prevent release of biological materials is through LoC. Documentation of biological materials usage, along with the controls containment

SSP 51721
Baseline

methods for all phases and conditions of use, is supplied for review and approval by the ISRP.

Due to the typically nonvolatile nature, biological materials do not impact the ECLSS impact hazard ratings.

Additional rationale for this requirement can be found in Appendix D.4.7.2.4.

4.7.2.4.1 VERIFICATION - RELEASE OF BIOLOGICALS

Verification is considered successful when the following are completed: A and (B and/or C) and D (and E if applicable)

- A. Biological materials have been assessed and assigned hazard severity rating through both of the following:(1 and 2)
 - 1. Listing of end item biological materials as identified in the above rationale are submitted for BRB assessment via electronic submittal spreadsheet. (I)
 - 2. HMST is reviewed and V1 form signed by end item provider. (I) (V1 process)
- B. DFMR approach for controlling release; verifications are described in detail in the topic-specific safety requirements in Section 4.0. (A, I, T)
- C. Failure tolerance approach for controlling release (LoC and/or appropriate controls), all of the following are provided: (1, 2 ,3 ,4, and 5):
 - 1. Review of end items design for LoC and/or controls are commensurate with the hazard severity. (I)
 - 2. End item LoC/control design is confirmed by qualification and acceptance testing, including independent testing of each LoC/C. (T)
 - 3. End item materials and material processing are reviewed and approved by NASA Materials Group. (A)
 - 4. End item flight hardware is built in accordance with approved drawings and assembled per approved procedures. (I)
 - 5. End item materials compatibility testing or analysis has been performed for both preparatory cleaning materials and biological materials.(T or A)
- D. Flight sample loading:
 - 1. (If applicable) SPF certified rodents are used. (I)
 - 2. The end item's biological materials have been properly loaded per pre-flight procedures/processing. (I) (V2 process)
- E. (If applicable) For end items manipulating samples on orbit and/or using LoC or appropriate controls involving operations to prevent biological material release, both of the following are provided: (1 and 2)
 - 1. The hazard control is identified and proven to be effective in preventing biological material release. (A or T)
 - 2. Inspection of procedures shows that operational controls are in place, including inspection for leakage/loss of containment/control before

removing containment/control and cleaning after operations for common use hardware. (I)

4.7.2.5 PHYSICAL AGENTS

The term physical agents is used here to specify the response of materials in microgravity and their use in spaceflight and spacecraft. Physical agents are materials or substances that become hazardous or more hazardous based on how they act and respond in microgravity. The differences in the way particles and fluids respond in environments where the gravitational force is different than on the Earth's surface (for example lower force (microgravity) on ISS or increased force during launch and landing) may create hazards. Some physical agents (for examples some particles and THL-0 fluid) are nominally considered non- or marginally hazardous and become more hazardous when released in appreciable concentrations or large mass due to how they act and respond in microgravity. Requirements for end item physical agents are addressed based on the prevention of release of physical agents (Section 4.7.2.5.1, Physical Agents Release) and based on the prevention of release of shatterable materials, a unique set of physical agents (Section 4.7.2.5.2, Shatterable Materials).

4.7.2.5.1 PHYSICAL AGENTS RELEASE

End item physical agents whose release would create hazards **shall** be controlled to prevent release.

Rationale

This requirement encompasses particles and fluids that are located in or may be introduced into the pressurized habitable environment and act as physical agents when released. It is established to protect the crew from physiological hazards and/or to protect the environment and VV/ISS equipment from hazards resulting from contamination.

Requirements for materials or substances that are chemically reactive, toxic, and/or significantly soluble in water are covered in Section 4.7.2.2, Chemicals, and biological material, including allergens are covered in Section 4.7.2.4, Biological Material Release.

Control to prevent release of physical agents is provided through failure tolerance or DFMR based on the hazard severity, reference Section 4.7.2, Hazardous Materials and Table D.4.7.2.5.1-1 below for details. Documentation of physical agent usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP.

Additional rationale for this requirement can be found in Appendix D.4.7.2.5.1.

4.7.2.5.1.1 VERIFICATION– RELEASE OF PHYSICAL AGENTS

Verification is considered successful when the following are completed: A and (B and/or C) and D (and E if applicable)

- A. Physical agents have been assessed and assigned hazard severity ratings through the following:

SSP 51721

Baseline

1. Listing of end items physical agents is submitted for NASA SME assessment via electronic submittal spreadsheet. (I)
 2. HMST is reviewed and V1 form signed by end item provider. (I) (V1 process)
- B. DFMR approach for controlling release; verifications are described in the topic-specific safety requirements in Section 4.0. (A, I, T)
- C. Failure tolerance approach for controlling release (LoC and/or appropriate controls):
1. Review of end items design for LoC and/or controls are commensurate with the hazard severity. (I)
 2. End item LoC/control design is confirmed by qualification and acceptance testing, including independent testing of each LoC/C. (T)
 3. End item materials and material processing are reviewed and approved by NASA Materials Group. (A)
 4. End item flight hardware is built in accordance with approved drawings and assembled per approved procedures. (I)
 5. End item materials compatibility testing or analysis has been performed for both preparatory cleaning materials and hazardous materials. (T or A)
- D. End item's physical agents have been properly loaded per pre-flight procedures/processing. (I) (V2 process)
- E. (If applicable) For end items manipulating physical agents (or other hardware that produces physical agents) on orbit and/or using LoC/C involving operations, to prevent release of physical agents, both of the following are provided:
1. The hazard control is identified and proven effective in preventing physical agent release. (A and/or T)
 2. Inspection of procedures shows that operational controls are in place, including inspection for leakage/loss of containment/control before removing containment/control and cleaning after operations for common use hardware. (I)

4.7.2.5.2 SHATTERABLE MATERIALS

Shatterable materials are unique physical agents. A shatterable material is any material that can fracture under a load or impact and produce fragments that are potentially hazardous to the crew and/or vehicle. Common shatterable materials on the ISS include glass, ceramics, LCD monitors, certain metallic alloys, optical equipment, and any other frangible materials that can fracture and produce fragments. Shatterable material requirements are addressed based on preventing release of fragments (Section 4.7.2.5.2.1, Shatterable Material Release) and based on protecting optical glass from fracture (Section 4.7.2.5.2.2, Optical Glass Protection).

SSP 51721
Baseline

This section addresses potential IVA release of shatterable materials. Shatterable materials that do not fit into the requirements below should meet structural requirements as addressed in Section 4.2, Structures.

4.7.2.5.2.1 SHATTERABLE MATERIALS RELEASE

End items with shatterable materials **shall** prevent the release of fragments larger than 50 micrometers (μm) into the ISS habitable volume.

Rationale

This requirement encompasses shatterable materials that are located in or may be introduced into the pressurized habitable environment. It is established to protect the crew from physiological hazards and/or to protect the environment and VV/ISS equipment from hazards resulting from contamination.

Additional rationale for this requirement can be found in Appendix D.4.7.2.5.2.1.

4.7.2.5.2.1.1 VERIFICATION– SHATTERABLE MATERIALS RELEASE

Verification is considered successful when one of the following is completed: A or B

- A. The end item design is shown to fully and permanently contain the shatterable material, based on both of the following.
 - 1. The contained covering is identified and proven effective in preventing shatterable material release. (A or T)
 - 2. Review of the end item design and review of the as-built hardware shows containment of the shatterable material. (I)
- B. When containment is not practical, the following are provided:
 - 1. For non-operational phases (launch or when hardware is not operational), both of the following are provided: (1 and 2)
 - a. The contained covering is identified and proven effective in preventing shatterable material release. (A or T)
 - b. Review of the end item design and review of the as-built hardware shows containment of the shatterable material. (I)
 - 2. For the operational phase, the following is provided:
 - a. Inspection of procedures shows that operational controls are in place to inspect for breakage prior to removing the protective covering, restoring the protective cover when not in use, and identification of any limitations in the use of the end item that prevent damage to the shatterable material. (I)

4.7.2.5.2.2 OPTICAL GLASS PROTECTION

Camera lenses, filters, and any other optical glass **shall** be non-stressed (no delta pressure), and protected.

SSP 51721

Baseline

Rationale

Optical glass is typically thicker than regular glass (e.g., Digital Single-Lens Reflex (DSLR) camera lenses), and less susceptible to damage from contact loads. Optical glass should not protrude beyond the plane of the outer rim of the lens casing (i.e., it should be recessed to provide protection when in use). Protection of the optical glass can be provided via lens caps when not in use.

Use of optical glass typically involves the crew when the protective cap or covering is removed from the glass to prevent contact loading. When not in use, the end item should be stowed or the shatterable components protected. The intent of this is to prevent inadvertent impacts from the crew or other equipment that might result in glass fragments.

Additional rationale for this requirement can be found in Appendix D.4.7.2.5.2.1.

4.7.2.5.2.2.1 VERIFICATION– OPTICAL GLASS PROTECTION

Verification is considered successful when the following are completed: A, B, C, and D

- A. An inspection of the end item design or vendor data to verify that the end item glass or frangible material is non-stressed (no delta pressure from within the optical glass (camera) to ambient). (I)
- B. An inspection of the end item design to verify that protection for the optical glass is provided. (I)
- C. An inspection of drawing shows the launch configuration includes a transparent bag with warning label requesting inspection prior to removal. (I)
- D. Inspection of procedures shows that operational controls are in place to inspect for breakage prior to opening the bag and restoring the protective cover (lens cap or other cover) when not in use. (I)

4.8 FIRE PROTECTION

Fire protection includes three factors: fire prevention, fire detection and fire suppression. Safety relies on fire prevention to mitigate a fire event. Fire detection and suppression are considered responses to a fire event rather than controls to preventing a fire.

Fire Prevention

Fire prevention on ISS is accomplished primarily by controlling flammable materials and ignition sources. Flammable materials are controlled per Section 4.7.1.1 and ignition sources are minimized via adherence to electrical design requirements such as proper bonding, grounding, wire and fuse sizing, and circuit protection. An ignition source is a source of heat sufficiently intense and localized to induce combustion. For flammability considerations, any high-power electrical wire is a potential ignition source. Any item that could cause sparks, such as a brush motor, is also considered a potential ignition source. [Solid materials (other than materials with a finely divided flock on the surface, such as moleskin and some medical dressings) are not ignited in ISS environments by

SSP 51721

Baseline

electrical powers of less than 25 watts; small alkaline and lithium-ion batteries are incapable of delivering such energy.] Material flammability and electrical requirements and circumstances when the requirements cannot be met are discussed during the safety review process.

Fire Detection and Fire Suppression

Any end item with a potential fire source should consider fire detection and suppression. Detection and suppression design requirements are levied and verified via IRDs (e.g., SSP 57000, SSP 50835), ISS vehicle specification, end item specifications, or other equivalent system specifications. Detailed information for smoke detection design, parameter monitoring and formatting of C&W signals can be found in SSP 57000, Sections N.3.10.1 and I.3.4.1.4. Detailed information for portable fire extinguisher access port design can be found in SSP 57000, Section N.3.10.2 and SSP 50835, Section 3.10.4.

4.9 HUMAN FACTORS SAFETY

This section covers topics with a direct effect on the crew. The topics include acoustics, touch temperature, contact hazards, lasers and broadband light (Radio Frequency (RF), emergency lighting and emergency response.

For crew-related RF hazards, see Section 4.3.8, Radio Frequency Transmitter Compatibility.

4.9.1 ACOUSTICS

Acoustics requirements are intended to protect crew hearing and allow them to hear audible alarms and perform critical communication. A source that emits noise for a cumulative total of more than eight hours in any 24-hour period is considered a continuous noise source. A source that emits noise for a cumulative total of eight hours or less in any 24-hour period is considered an intermittent noise source. A source that emits noise with a sound level of 37 dBA or less, measured 2 feet (ft) (60 cm) from its loudest point is considered an insignificant noise source.

Noise levels are measured either as an A-weighted Sound Level as a single decibel (dBA), overall sound pressure level (dB), value or using a family of Noise Criterion (NC) curves which describe the relative loudness of an area or noise source. Each NC curve defines the values at each sound pressure level values at each octave band frequency from 60 to 8000 Hz that must not be exceeded. The NC level (e.g., NC-40) is a single value which represents a complete sound spectrum. For more information on NC curves, refer to ANSI/ASA S12.2-2008.

An NC-40 requirement is levied on all integrated rack and GFE/CFE continuous noise sources via applicable IRD or equivalent system specification. Continuous noise source sub-rack and non-rack payloads must meet an NC-34 requirement based on the applicable IRD. Intermittent noise sources must meet the IRD intermittent noise requirements. These intermittent sources are managed to ensure the sound level and time limits are not exceeded. These continuous and intermittent noise requirements are verified via the IRD process. End items must identify to the ISRP those noise sources

SSP 51721
Baseline

that do not meet the limits established in the IRD or equivalent specifications. ISRP review may be required to determine whether implementation of hazard controls is necessary. If the ISRP determines that any IRD exception creates a critical or catastrophic hazard, the end item provider may be required to present a HR to the ISRP to define controls and verifications to mitigate the hazard. Noise sources above 80 dBA are not allowed per the IRD requirement and must be discussed during the phased safety review process if the potential exists for exceeding the limit.

Acoustic requirements are applicable to any end item with a noise producing component – fan, motor, etc.

The source document for acoustics requirements in Sections 4.9.1.2 through 4.9.1.5 is SSP 50005.

4.9.1.1 IMPULSE NOISE HAZARD LIMIT

End item impulse noise **shall** be less than 140 dB peak overall sound pressure level at the crewmember's head location.

Rationale

This requirement is applicable to all individual noise sources. Impulse noise higher than this value could result in temporary to permanent hearing loss. Impulse noise is defined as a change in Sound Pressure Level (SPL) of more than 10 dB in one second or less.

Additional rationale for this requirement can be found in Appendix D 4.9.1.1.

4.9.1.1.1 VERIFICATION– IMPULSE NOISE HAZARD LIMIT

Verification is considered successful when acoustic testing performed using methodologies from JSC 28322 confirms that the criteria is met. (T)

4.9.1.2 CLASS 1 AND CLASS 2 ALARM AUDIBILITY

To ensure alarm audibility, the SPL of Class I and II alarms at the operating position of the intended receiver **shall** meet at least one of the following criteria:

- A. Using measurements of A-weighted sound levels [ISO 7731:2003(E), method a) in Section 5.2.2.1], the difference between the two A-weighted SPLs of the signal and the ambient noise is greater than 15 dBA ($LS_{A} - LN_{A} > 15$ dBA).
- B. Using measurements of octave-band SPL [according to ISO 7731:2003(E), method b) in Section 5.2.3.1], the SPL of the signal in one or more octave-bands exceeds the effective masked threshold by at least 10 dB in the frequency range from 250 Hz - 4000 Hz ($LS_{i,oct} - L_{ti,oct} > 10$ dB).
- C. Using measurements of 1/3 octave-band SPL [according to ISO 7731:2003(E), method c) in Section 5.2.3.2], the SPL of the signal in one or more 1/3 octave-bands exceeds the effective masked threshold by 13 dB in the frequency range from 250 Hz - 4000 Hz ($LS_{i,1/3oct} - L_{Ti,1/3oct} > 13$ dB).

SSP 51721
Baseline

Rationale

This requirement is applicable to emergency and warning tones and ensures they are audible over the continuous noise in the habitable areas. Acoustic measurements are periodically taken on-orbit and are used as a basis to quantify the ambient noise.

Additional rationale for this requirement can be found in Appendix D 4.9.1.2.

4.9.1.2.1 VERIFICATION- CLASS 1 AND CLASS 2 ALARM AUDIBILITY

Verification is considered successful when one of the following is completed:

- A. Test or analysis of alarm signal versus ambient noise confirms alarms will be audible. (T or A)

The method to calculate the effective masked threshold to verify option 2 and 3 are given in ISO 7731:2003E Annex B.

- B. If an exceedance to NC~52 is found during the ISS integrated increment analysis for requirement in Section 4.9.1.5, further analysis is performed to ensure alarm audibility. (A)

4.9.1.3 ALARM HAZARD LIMIT

Alarm signal's A-weighted Sound Level **shall** be 95 dBA or less at the location of the intended receiver.

Rationale

Alarms are allowed to produce sound levels up to 95 dBA in order to provide adequate design space for audibility. This is considered safe since alarms can be silenced.

4.9.1.3.1 VERIFICATION - ALARM HAZARD LIMIT

Verification is considered successful when acoustic testing or analysis performed using methodologies from JSC 28322 confirms that the criteria is met. (T or A)

4.9.1.4 REVERBERATION TIME

In areas where the crew must communicate by voice, the reverberation time **shall** be at or below 0.6 seconds at 1000 Hertz.

Rationale

This requirement applies to the ISS internal environment to prevent interference with critical crew communication. This requirement also applies to VVs while docked to ISS per SSP 50808. Any modules designed for ISS must meet this requirement.

4.9.1.4.1 VERIFICATION - REVERBERATION TIME

Verification is considered successful when test or analysis show the reverberation time meets this criteria. (T or A)

SSP 51721
Baseline

4.9.1.5 COMPOSITE CONTINUOUS ACOUSTIC EMISSIONS – ISS LEVEL REQUIREMENT (USOS)

The composite continuous SPLs for the complement of pressurized payloads along with the integrated vehicle system level acoustic emissions in habitable areas **shall** not exceed the requirement shown in Table 4.9.1.5-1 during normal operating conditions when averaged over a minimum of 10-second time intervals and for a spatial average across the vehicle centerline.

TABLE 4.9.1.5-1 NC~52

Frequency, Hz	Sound Pressure Level, dB
63	73
125	66
250	60
500	56
1000	53
2000	51
4000	50
8000	49

Rationale

Excessive noise in the ISS exceeding NC~52 could impact crew hearing and communication. This requirement is applicable to the overall ISS environment, including VVs, and is verified at the integrated level. This requirement is not applicable to individual end items but data from the individual end items may be used in the integrated analysis.

Additional rationale for this requirement can be found in Appendix D.4.9.1.5.

4.9.1.5.1 VERIFICATION – COMPOSITE CONTINUOUS ACOUSTIC EMISSIONS

Verification is considered successful when the SPLs of the total pressurized payload complement and vehicle are shown not to exceed NC~52, for each octave band frequency from 63 to 8000 Hz, for a spatial average across the module. Acoustical analysis is performed according to SSP 57011 EN-02 using continuous SPL data or Sound Power Level data (if available) for integrated racks, non-rack pressurized payloads, and continuous vehicle noise sources, including non-integrated GFE. (A)

4.9.2 IVA TOUCH TEMPERATURE

Touch temperature requirements for end item exposed surfaces are established to protect crew from skin damage. Touch temperature is addressed here based on the acceptable touch temperature limits for bare skin contact (Section 4.9.2.1, Touch Temperature Limits) and based on end item functional design (Section 4.9.2.2, Touch Temperature Based on End Item Functionality).

SSP 51721

Baseline

NOTE: Touch Temperature requirements for EVA hardware are captured uniquely in Section 4.10.1, EVA Temperature Extremes.

4.9.2.1 TOUCH TEMPERATURE LIMITS

For end item exposed surface temperature (T_{ES}) greater than 45° Celsius (C) (113° Fahrenheit (F)) or less than 0°C (32°F), bare skin contact **shall** be controlled based on permissible material temperature (T_{PM}) and skin contact time (incidental and intentional contact).

This requirement is based on SSP 50005.

Refer to rationale for term definitions and calculating T_{PM} .

Rationale

This requirement applies to end items inside and/or connected to the ISS internal pressurized environment.

The end item exposed surface touch temperature range from 0°C (32°F) to 45°C (113°F) is considered non-hazardous and is acceptable for bare skin contact. Contact with exposed surfaces outside of this temperature range are either prevented through failure tolerance or DFMR based on the hazard severity or shown by analysis to meet the T_{PM} based on end item material properties and skin contact time. Anything outside of the T_{PM} is considered a critical or catastrophic hazard (reference Section 4.1.1) as determined by the Flight Activities Control Board (FACB) and ISRP based on potential skin damage.

Additional guidance on touch temperature hazard severity is provided in Table/Figure for touch temperature hazard severity <TBR 4-11>.

To verify this requirement, end item exposed surface temperature (T_{ES}) are assessed based on the worst case temperature the end item can reach. This should take into account the appropriate number of failures based on potential hazard severity. For end items with worst case T_{ES} that fall within the non-hazardous range, no additional analyses/calculations are needed. For end items with worst case T_{ES} that is at or outside the non-hazardous range, the end item T_{PM} should be calculated.

Touch temperature limits depend on contact thermal conductance, which is a function of an end item's material properties and initial temperature, and skin contact time. Additional information on the derivation of hot and cold temperature limits can be found in NASA/SP-2010-3407, Human Integration Design Handbook (HIDH).

Additional rationale for this requirement can be found in Appendix D.4.9.2.1.

4.9.2.1.1 VERIFICATION - TOUCH TEMPERATURE LIMITS

Verification is considered successful when the following are completed: A or ((B or C) and (D and/or E))

- A. End item exposed surfaces (based on worst case T_{ES}) are within non-hazardous temperature range. (A or T)

SSP 51721

Baseline

- B. For end item exposed surfaces above the hot touch temperature hazard (where $T_{ES} > 45^{\circ}\text{C}$ (113°F)), material analysis shows that the minimum ($T_{ES} \leq T_{PM}$). (A)
- C. For end item exposed surfaces below the cold touch temperature hazards (where $T_{ES} < 0^{\circ}\text{C}$ (32°F)) material analysis shows that the minimum ($T_{ES} \geq T_{PM}$). (A)
- D. For end items using active thermal management, the design is shown to provide hazard controls in alignment with hazard severity to exceeding hazardous surface temperatures. (A or T)
- E. For end items using alternate means (such as delayed access to end item surfaces) to prevent crew exposure to touch temperature hazards, the following is provided:
 - 1. The control should be identified and proven to be effective in protecting bare skin and (A or T)
 - 2. Inspection of procedures shows that operational controls are in place to prevent contact with hazardous touch temperatures. (I)

4.9.2.2 TOUCH TEMPERATURE BASED ON END ITEM FUNCTIONALITY

For end items with exposed surface temperature (T_{ES}) that is outside the acceptable permissible material temperature (T_{PM}) due to end item functionality, bare skin contact **shall** be prevented through the use of controls.

Rationale

This requirement applies to end items that are intentionally designed to be outside of the acceptable, non-hazardous temperature range of 0°C (32°F) to 45°C (113°F) due to the purpose of the end item. This includes end items that are specifically designed to function as freezers or heaters.

Anything outside of the T_{PM} is considered hazardous. Incidental and intentional contact with exposed surfaces should be prevented through failure tolerance or DFMR based on the hazard severity (reference Section 4.1.1) as determined by the FACB and ISRP based on potential skin damage.

*Additional guidance on touch temperature hazard severity is provided in Table/Figure for touch temperature hazard severity **<TBR 4-11>**.*

To verify this requirement, end item exposed surface temperature (T_{ES}) should be assessed based on the worst case temperature the end item can reach. This should take into account the appropriate number of failures based on potential hazard severity. Refer to Section 4.9.2.1 rationale for information on T_{ES} and additional details.

Touch temperature limits depend on contact thermal conductance, which is a function of an end item's material properties and initial temperature, and skin contact time. Additional information on the derivation of hot and cold temperature limits can be found in NASA/SP-2010-3407, Human Integration Design Handbook (HIDH).

Operational Controls

The end items that fall into this requirement often necessitate intentional contact from the crew as samples and/or materials are added, moved, and/or removed from the end item. Incidental contact should be controlled by design. The use of operational controls such as PPE should be coordinated with the operations community and approved by the ISRP. PPE such as gloves or mittens suitable for the worst case temperature extremes should be provided. The PPE should appropriately cover and protect bare skin and be rated for the worst case time duration of the operations. The use of proven PPE in this application is considered to be an acceptable DFMR approach.

4.9.2.2.1 VERIFICATION - TOUCH TEMPERATURE BASED ON END ITEM FUNCTIONALITY

Verification is considered successful when the following are completed: A and B

- A. End item exposed surfaces (based on worst case T_{ES}) are defined based on the functionality of the hardware and are outside the non-hazardous temperature range. (A or T)
- B. For end items using alternate means (such as thermal gloves or delayed access to end item surfaces) to prevent crew exposure to touch temperature hazards, the following is provided:
 1. The control should be identified and proven to be effective in protecting bare skin for one of the following:
 - a. For delayed access time, the worst case T_{ES} is used to define the minimum wait time for T_{ES} to reach the non-hazardous touch temperature range (A or T)
 - b. For PPE, the appropriate thermal protection has been selected and proven to protect bare skin for the planned use (timeframe). (A or T)
 2. Inspection of procedures shows that operational controls are in place to prevent contact with hazardous touch temperatures. (I)

4.9.3 IVA CREW CONTACT HAZARDS

Crew exposure to hazards associated with sharp edges, latches, levers, cranks, hooks, controls, and holes located within the end item, must not pinch, snag, cut, entrap, or abrade the crew. Resulting injuries can range from a minor nuisance to potentially catastrophic.

Mitigating these hazards may be accomplished by making potential hazards inaccessible to the crew and/or providing guards to reduce or eliminate the potential to cause injury. Equipment (e.g., cables, fluid lines, air ducts) should also be protected because damage to the equipment may indirectly harm the crew (e.g., fluid leaks, restricted flow to critical systems, etc.).

SSP 51721

Baseline

The parent sharp edge design requirements are located in SSP 50005, Section 6.3 and are verified and validated via IRDs, end item specifications, or other equivalent system specifications (e.g., SSP 57000, Section 3.12.8; SSP 50835, Section 3.12.9.2). IRDs will identify which IRD requirement is also a safety requirement.

In the event that sharp edge requirements cannot be verified per the IRD, including functional sharp edges (scalpels, scissors, hypodermics, etc.), COTS products, on-orbit manufactured (3D-printed) parts, and any other hardware that do not meet these requirements, it is the responsibility of the end item provider to disclose the discrepancy to the ISRP. In most cases, a HR will be required to describe the control philosophy for the discrepancy. Discussions between the ISRP, Engineering, or the Safety Panel Engineer can help determine the necessity and control strategy of the HR.

NOTE: Sharp edge requirements for unpressurized hardware are captured uniquely in the EVA section.

4.9.3.1 USE OF SAFETY WIRE

For end items utilizing safety wire (lock wire) the crew **shall** be protected from the cut end.

Rationale

The use of safety wire is prohibited via SSP 57000, SSP 50835, or equivalent specification, for fasteners that could be manipulated on orbit, including maintenance and contingency operations. The on-orbit crew will not be expected to remove or reinstall safety wire. Physical protections for inadvertent contact of the cut end of safety wire used in proximity of crew operations can include folding the wire over and wrapping with Kapton tape, shrink tubing, RTV, etc. Physical barriers must be certified for the life of the end item. On-orbit manipulated fasteners must utilize other locking features. The use of safety wire must be documented in a UHR.

4.9.3.1.1 VERIFICATION - USE OF SAFETY WIRE

Verification is considered successful when the following are completed:

- A. Inspection of drawings to confirm that protections are in place. (I)
- B. Inspection of as-built hardware to approved drawings. (I)
- C. Material certification for service life of protective materials. (A)

4.9.4 LASERS AND BROADBAND LIGHT

Crew exposure to high-intensity laser and/or broadband light emissions could result in biological damage to the eye or skin. Sustained damage to the eye could lead to crew incapacitation or blindness. Skin tissue destruction can also occur. Hazards from crew exposure to high-intensity laser and/or broadband light emissions are controlled by making the source inaccessible to the crew (e.g., containment of the source) or by providing the appropriate number of controls to prevent exposure (e.g. power inhibits) based on hazard severity (reference Section 4.1.1).

SSP 51721
Baseline

Direct or indirect exposure to high-intensity laser emissions could also result in damage to end items, including vehicles and vehicle systems (i.e., VVs or the EMU). The ISSP is assessing potential hazards to end item hardware and as a result of end item damage due to exposure. **<TBR 4-12>** Potential hazards from end item exposure to high-intensity laser emissions will be addressed on a case by case basis with the ISRP; controls should be based on hazard severity.

Lasers and broadband light sources are considered to be sources of nonionizing radiation. The requirements here are focused on concern from crew exposure to lasers. Requirements related to RF are addressed in Section, 4.3.7, Electromagnetic Capability and Section 4.3, Electrical.

The requirements in this section are based on SSP 50005. Additional details (reference tables and calculations) can be found in SSP 50005.

4.9.4.1 LASERS - GENERAL

Lasers **shall** be designed and controlled in accordance with ANSI Z-136.1, American National Standard for Safe Use of Lasers.

Rationale

This requirement is applicable for all end items with lasers.

The ANSI standard provides for the safe use of lasers and laser systems by providing classifications according to their relative hazards and then specifying appropriate controls. The basis of the hazard classification is the ability of the laser beam to cause biological damage to the eye or skin during use. This standard is used to protect the crew as well as ground-based general public with and without optical aid consideration. The ANSI standard also provides the Maximum Permissible Exposure (MPE) for each classification. Use of ANSI Z-136.1 2007 or newer is acceptable and should be specified when providing data to the NASA SME, the JSC/Non-Ionizing Radiation (NIR)Group.

Additional rationale for this requirement can be found in Appendix D.4.9.4.1.

4.9.4.1.1 VERIFICATION- –LASERS - GENERAL

Verification is considered successful when one of the following is completed: A or B (and C if applicable)

- A. Laser classification is determined based on one of the following:
 - 1. Review of vendor-provided data and concurrence by the JSC/NIR Group. (I)
 - 2. Test of the laser at the source (based on max output or energy the laser could receive with no inhibits) and concurrence by the JSC/NIR Group. (T and I)
- B. For modified lasers, laser classification is determined based on one of the following:

SSP 51721

Baseline

1. Review of vendor-provided and modifications to confirm no change in laser output and concurrence by the JSC/NIR Group. (A and I)
 2. Test of the modified laser of the source (based on max output or energy the laser could receive with no inhibits) and concurrence by the JSC/NIR Group. (T and I)
- C. For contained lasers, one of the following is provided: (1 and 2)
1. A review of design and review of final configuration for contained lasers, confirms containment. (I)
 2. If access to a contained laser is possible, controls (e.g safety interlocks) are identified, proven acceptable, and provided as part of the final configuration. (A and I)

4.9.4.2 MAGNIFICATION OF LASERS

For exposed lasers of Class 1M, 2M and above, exposure resulting from magnification by ISS optical equipment **shall** be below the MPE.

Rationale

Class 1M and 2M and higher lasers are potentially hazardous if viewed with certain optical aids. An ocular hazard assessment ensures optical magnification by equipment on board ISS (cameras, binoculars, etc.) that could be used to view a laser source or its specular reflection does not result in exposure above the MPE. Information on worst case ISS optical equipment can be obtained from the JSC/NIR Group. Additional controls, such as operational controls, are required to prevent viewing a laser with optical magnification equipment if the analysis shows exposure would be above the MPE. (e.g., a flight rule preventing use of certain optical equipment during certain operational times, such as docking).

4.9.4.2.1 VERIFICATION- MAGNIFICATION OF LASERS

Verification is considered successful when the following are completed: A and/or B

- A. An optical assessment/ocular hazard analysis performed per ANSI Z-136.1 confirms that the MPE as specified in ANSI Z-136.1 is not exceeded. (A)
- B. Inspection of procedures shows that operational controls are in place to limit the use of optical instruments in the sightline of the laser. (I)

4.9.4.3 CLASS 3R, 3B, AND 4 LASERS

Class 3R, 3B or 4 lasers **shall** be inaccessible to the crew or provided with three controls to prevent exposure.

Rationale

Class 3R, 3B, or 4 lasers can be hazardous to the eye or skin from direct beam or specular reflection viewing conditions. Class 4 lasers could also pose a diffuse reflection or fire hazard. Crew exposure to Class 3R, 3B, or 4 lasers is considered a catastrophic

SSP 51721

Baseline

hazard so and the design is required to provide two failure tolerance to prevent exposure.

If access to a contained laser is possible, safety interlocks or other controls should be provided. Other controls could include filters, laser only points away from ISS, laser turned off during EVA, etc.

4.9.4.3.1 VERIFICATION - CLASS 3R, 3B, AND 4 LASERS

Verification is considered successful when one of the following is completed: A or B

- A. Review of design and review of final configuration confirms that the laser is contained and inaccessible to the crew. (I)
- B. Three controls against crew exposure are provided. (I)

4.9.4.4 VISIBLE LIGHT EXPOSURE FROM ARTIFICIAL SOURCES

Visible light sources whose intensity exceeds 10,000 nits **shall** be designed to limit crew exposure to below the Threshold Limit Values (TLV) as calculated per ACGIH (2014 or newer).

Rationale

This requirement is intended to prevent ocular injury and skin damage caused by overexposure to visible light from artificial sources. Examples of artificial light sources include LEDs, illumination lamps and display screens. Artificial visible light sources with an average output of 10,000 nits (1 nit = Candela per meter squared or Cd/m²) or less are not considered hazardous. The value of 10,000 nits is a commonly utilized specification in commercial hardware and is established based on guidance from the ACGIH (2014 or newer).

Additional rationale for this requirement can be found in Appendix D.4.9.4.4.

4.9.4.4.1 VERIFICATION- VISIBLE LIGHT EXPOSURE FROM ARTIFICIAL SOURCES

Verification is considered successful when one of the following is completed: A or B

- A. Vendor data or test data showing $\leq 10,000$ nits of luminance output from the source of the artificial light. (T or I)
- B. Calculations per ACGIH showing crew exposure does not exceed the TLV. (A)

4.9.4.5 INFRARED RADIATION (IR) LIGHT EXPOSURE FROM ARTIFICIAL SOURCES

Infrared light sources **shall** be controlled to prevent crew exposure that exceeds the TLV as calculated per ACGIH (2014 or newer).

Rationale

This requirement is intended to prevent ocular injury and skin damage caused by overexposure to infrared radiation (IR) from artificial sources. The end item should prevent exposure through controls or containment. Infrared radiation (IR) sources are

SSP 51721

Baseline

not necessarily required to be contained at the source, but should be obstructed by applicable means (e.g. shields, filters) before reaching the crew.

4.9.4.5.1 VERIFICATION – INFRARED RADIATION (IR) LIGHT EXPOSURE FROM ARTIFICIAL SOURCES

Verification is considered successful when both of the following are completed: A and B

- A. Calculations per ACGIH showing crew exposure does not exceed the TLV. (A)
- B. Test or inspection of as-built hardware confirms the end item IR source is controlled or contained. (T or I)

4.9.4.6 ULTRAVIOLET (UV) RADIATION LIGHT EXPOSURE FROM ARTIFICIAL SOURCES

Ultraviolet light sources **shall** be contained.

Rationale

This requirement is intended to prevent ocular injury and skin damage caused by overexposure to UV radiation from artificial sources. This requirement does not apply to ambient cabin lighting because the UV levels are minimal.

4.9.4.6.1 VERIFICATION – ULTRAVIOLET (UV) RADIATION LIGHT EXPOSURE FROM ARTIFICIAL SOURCES

Verification is considered successful when both of the following are completed: A and B

- A. Review of end item design confirms containment. (I)
- B. Test or inspection of as-built hardware confirms containment. (T or I)

4.9.5 LIGHTING

Lighting levels must provide enough illumination for the crew to perform their tasks (including emergency/backup/secondary lighting) while also maintaining an intensity below the MPE as to not injure the crew (Section 4.9.4).

The parent lighting requirements are located in SSP 50005, Section 8.13, and are verified and validated via IRDs, end item specifications, or other equivalent system specifications (e.g., SSP 57000, section 3.12.3; SSP 50835, Section 3.12.3.4; SSP 50808, Section 3.3.2.2). IRDs will identify which IRD requirement is also a safety requirement. In the event end items do not show successful compliance with the IRD or equivalent requirements, it is the responsibility of the end item provider to disclose the exception to the ISRP. If the ISRP determines that the exception creates a hazard, the end item will be required to present a HR to the ISRP to define controls and verifications.

4.9.5.1 EMERGENCY EGRESS PATH INDICATION

ISS Emergency Egress Indicators **shall** have a minimum American Society for Testing and Materials (ASTM) rating of 600/90 mcd/m² for illuminating material (glow in the dark material), and produce a minimum of 2 lux (2.0 millicandela (mcd)/m²).

SSP 51721
Baseline

Rationale

The ISS will visually indicate emergency egress hatches in the absence of power to general area lighting by using glow in the dark indicators for the ISS Emergency Egress Guidance Systems (EEGS). In order to provide emergency path marking, the indicators must produce a minimum of 2 lux (2.0 millicandela (mcd) / m²), which is the industry safety standard for minimum luminance visibility (ISO 16069, Graphical Symbols – Safety Signs – Safety Way Guidance Systems (SWGS), Section 7.3.2).

Additional rationale for this requirement can be found in Appendix D.4.9.5.1.

4.9.5.1.1 VERIFICATION - EMERGENCY EGRESS PATH INDICATION

Verification is considered successful when inspection of vendor data shows compliance to requirement.

Verification submittal: Inspection of vendor data. (I)

4.9.6 EMERGENCY RESPONSE

In an emergency situation, the crew must be able to remove themselves from any end item apparatus, migrate via the translation paths and isolate volumes, if required, in a timely manner. Additional requirements related to the integrated ISS internal configuration for maintaining translation paths and access to critical emergency response equipment can be found in the Generic Groundrules, Requirements, and Constraints (GGR&C), Section 13.

4.9.6.1 EGRESS FROM END ITEM APPARATUS

The design **shall** enable crew egress from end item apparatus in less than 30 seconds.

Rationale

The crew must be able to free themselves from any apparatus such that they can evacuate/relocate if necessary.

Additional rationale for this requirement can be found in Appendix D.4.9.6.1.

4.9.6.1.1 VERIFICATION – EGRESS FROM END ITEM APPARATUS

Verification is considered successful when one of the following is completed:

- A. Review of design and on-orbit configuration show the crew can egress the end item apparatus in less than 30 seconds. (I)
- B. Demonstration that egress can be accomplished in less than 30 seconds (D).

4.9.6.2 INTRAMODULE EMERGENCY EGRESS

The end item design **shall** not impede emergency IVA egress to the remaining contiguous pressurized volumes.

SSP 51721

Baseline

Rationale

A minimum emergency translation corridor of 32 X 45 inches (81 X 114 cm) is maintained within the USOS modules and 32 x 32 inches (81 x 81 cm) within the Russian Segment. A 32 X 45 in (81 X 114 cm) corridor allows for a crewmember to reverse direction at any point along the corridor during emergency situations. Temporary intrusions or items that can be quickly relocated or reconfigured will be assessed by the ISRP on a case by case basis. Rack rotation due to maintenance and rack translation are acceptable protrusions into the emergency translation corridor. Cables, hoses, and wires in the translation corridor must be restrained to prevent entanglement during emergency egress. Cable/hose restraint requirements are levied via the associated IRD and detailed cable management is left up to crew discretion.

Additional rationale for this requirement can be found in Appendix D.4.9.6.2.

4.9.6.2.1 VERIFICATION – INTRAMODULE EMERGENCY EGRESS

Verification is successful when the following is completed: A or (B and C)

- A. Review of design and on-orbit configuration show the end item does not impede egress. (I)
- B. End item information provided to the International Volume Configuration Working Group (IVCWG) for inclusion in the integrated assessment as necessary. (I)
- C. ISSP integrated assessment of on-orbit configuration for translation path per GGR&C. (A)

4.9.6.3 VOLUME ISOLATION

The ability to isolate a volume within three minutes by closing a module hatch **shall** be preserved.

Rationale

In emergency situations (i.e., fire, depress, or toxic atmosphere), the crew must be able to isolate themselves or the affected module within three minutes. The volume to be isolated could be more than one module but closing one hatch would isolate the crew from the hazard.

Additional rationale for this requirement can be found in Appendix D.4.9.6.3.

4.9.6.3.1 VERIFICATION – VOLUME ISOLATION

Verification is considered successful when each of the following are completed:

- A. End item information provided to the appropriate ISS Program integration function/team for integrated assessment. (I)
- B. ISSP integrated assessment performed per HR ISS-STO-0801, Injury of Crew or Damage to ISS during Transfer and Stowage of Loose Hardware, for each stage to ensure stowage complies with SSP 50621. (A)

SSP 51721

Baseline

- C. ISSP integrated hatch closure assessment performed per HR ISS-NTN-001 for each stage to evaluate drag-throughs and ensure each hatch can be closed within 3 minutes. (A)

4.9.6.4 HATCH DRAG-THROUGHES

Hatchways **shall** be clear of drag-throughs.

Rationale

Cables, lines, hoses, and ducts, in addition to anything which could pose interference with hatch closure, are considered drag-throughs. Any proposed drag through, including portable equipment, must be approved by the ISSP via an NCR. Node 3 and Cupola are considered as one volume for the purposes of drag-through evaluation; therefore, these drag-throughs do not require an NCR but would still be tracked as part of the hatch closure assessment.

4.9.6.4.1 VERIFICATION – HATCH DRAG-THROUGHES

Verification is considered successful when review of design shows no drag-throughs exist. (I)

4.10 EXTRAVEHICULAR ACTIVITY

Regardless of whether EVAs are planned, contingency or not required by an end item, all hardware in EVA accessible areas must be compliant with these EVA safety requirements. Only the ISRP supported by the EVA Analysis and Integration Team (AIT) can determine if an item is outside EVA accessible areas. If that determination is made, no assessment for EVA is required. Any agreed to EVA task used to satisfy the failure tolerance criteria can be used only as a third level of control to safe an end item if the ISRP and ISSP approve. The EVA task must also be negotiated by the operations team.

Generic EVA hazards are those introduced by being exposed to the EVA environment i.e., hazards independent of what is to be performed while EVA. Operational hazards (e.g., fatigue, tether management, distance from airlock) are those relating to the specific EVA operation to be performed. The requirements listed here address the generic hazards. Hazards related to EVA should be captured on the UHR. The EVA operations community ensures the operational hazards are addressed during the planning phase for each specific EVA.

Detailed design guidelines for EVA hardware can be found in SSP 41162, Segment Specification for the USOS, SSP 30256-001, EVA Standard Interface Control Document, SSP 57003, Appendix G, Attached Payload Interface Requirements Document and JSC 26626A, EVA Hardware Generic Design Requirement Document (GDRD) (for GFE). Requirements for the ISS to provide the capability for successful EVA is covered in SSP 41000 , System Specification for the ISS.

EVA on-orbit induced load requirements (including tool impact) are levied and verified via the associated IRD, such as SSP 57003 and SSP 30256. However, if failure to meet

SSP 51721 Baseline

these loads creates a hazard to the EVA crew or to ISS, the failed load requirement(s) are dealt with as safety requirements and address in Hazard Reports and/or NCRs.

Radio Frequency (RF) requirements are defined in SSP 51721, Sections 4.3.7.2, Protecting against Hazardous RF Irradiation and Section 4.3.7.3, Deployable End Item Radio Frequency Transmitters.

Keep Out Zones (KOZ), No Touch Areas (NTA) and Load Sensitive Areas (LSA) are warning categories that define certain areas of exterior hardware that may require special attention during an EVA. KOZ and NTA are used to draw attention to areas that pose a risk to the crew (sharp edges, RF emitters, etc). LSA are areas that are non-compliant with the EVA kickload requirement. Detailed definitions are provided in the glossary.

4.10.1 EVA TEMPERATURE EXTREMES

The EMU is protected from damage caused by high and low temperature extremes based on the following requirements. A burn through of EMU material can result in a loss of breathable atmosphere and potential loss of crew. All external hardware in an EVA accessible area must meet the incidental contact requirement. Incidental contact is considered brush and bump contact of up to 30 seconds at 0.1 psi or 3 seconds at 1 psi.

4.10.1.1 INCIDENTAL CONTACT

For incidental contact, end item temperatures **shall** be maintained within -180 to +235 degrees F, or limit heat transfer rates as listed in Table 4.10.1.1-1, Heat Transfer Rates.

TABLE 4.10.1.1-1 HEAT TRANSFER RATES

Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (°F)	Linear Conductor (BTU/hr °F)	Maximum Average Heat Rate ⁽¹⁾ (BTU/hr)
Hot Object	Incidental (0.5 max)	113	1.444	176.2 ⁽²⁾
Cold Object	Incidental (0.5 max)	40	1.478	-325.2 ⁽²⁾

NOTES:

1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for 12 second intervals are allowable).

Rationale

The values in this table assumes the skin temperature as the boundary (from medical limits and testing), with a linear conductor to account for the contact resistances and material thermal resistances of the glove (based on testing), and the maximum allowable heat rate (based on testing). The end item provider must apply these values to the object to be contacted by the skin boundary through the prescribed linear conductor. The objects initial temperature and material properties must be considered.

SSP 51721
Baseline

The EMU gloves can withstand contact temperatures of -180 to 235 degrees F (-118 to 113 degrees C) with a contact pressure of 0.1 psi (0.7 kPa) without discomfort to the hand for nearly 5 minutes. The Thermal Micrometeoroid Garment (TMG) can withstand these contact temperatures under any operational scenario.

Additional rationale for this requirement can be found in Appendix D.4.10.1.1.

4.10.1.1.1 VERIFICATION- INCIDENTAL CONTACT

Verification is considered successful when the following are completed:

- A. End item is confirmed by one of the following to be within the acceptable thermal range:
 - 1. Thermal Analysis (A)
 - 2. Thermal Test (T)
- B. If passive controls are implemented, verification must also include an inspection of drawings and hardware for passive hardware features. (I)
- C. If active controls are implemented, verification must also include a test of these active thermal controls. (T)

4.10.1.2 UNLIMITED CONTACT

For unlimited contact, end item temperatures **shall** be maintained within -45 to +145 degrees F, or for designated EVA crew interfaces listed in Table 4.10.1.2-2, limit heat transfer rates as listed in Table 4.10.1.2-1.

TABLE 4.10.1.2-1 HEAT TRANSFER RATES

Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (°F)	Linear Conductor (BTU/hr °F)	Maximum Average Heat Rate ⁽¹⁾ (BTU/hr)
Hot Object	Unlimited	113	1.149	42.52 ⁽²⁾
Cold Object	Unlimited	40	1.062	-132.7 ⁽²⁾

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 minute intervals are allowable.)

TABLE 4.10.1.2-2 DESIGNATED EVA INTERFACES

EVA Tools and Support Equipment
EVA Translation Aids (e.g., Crew and Equipment Translation Aid (CETA) Cart, handrails, handholds, etc.)
EVA Restraints (e.g., foot restraints, tethers, tether points, etc.)
All EVA translation paths (e.g., 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 (e.g., handholds, Articulating Portable Foot Restraint (APFR) ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

SSP 51721

Baseline

Rationale

For contact typical for designated EVA crew interfaces, the EMU gloves and TMG withstand contact temperatures of -45 to 145 degrees F (-43 to 63 degrees C).

Analysis is the preferred approach to verify this requirement because recreating the environment can be too costly or impractical.

End item temperature can be controlled passively or actively. Passive controls include the choice of material, coatings or insulation while active controls include items such as heaters or cold plates.

4.10.1.2.1 VERIFICATION- UNLIMITED CONTACT

Verification is considered successful when the following are completed:

- A. End item is confirmed by one of the following to be within the acceptable thermal range:
 - 1. Thermal Analysis (A)
 - 2. Thermal Test (T)
- B. If passive controls are implemented, verification must also include an inspection of drawings and hardware for passive hardware features. (I)
- C. If active controls are implemented, verification must also include a test of these active thermal controls. (T)

4.10.2 EXTERNAL CORNER AND EDGE

The EMU must be protected from cuts, tears and snags by adhering to the following requirements. These requirements apply to any protrusion, burr, or exposed sharp edge that has the potential to cut an EVA glove or puncture the EMU. All hardware in EVA accessible areas must meet these requirements.

4.10.2.1 SHARP EDGES AND PROTRUSIONS

End item edges and protrusions **shall** meet the criteria provided in Table 4.10.2.1-1, Table 4.10.2.1-2, and Figure 4.10.2.1-1.

SSP 51721
Baseline

TABLE 4.10.2.1-1 EDGE, CORNER, AND PROTRUSION CRITERIA – EDGE AND IN-PLANE CORNER RADII*

Application	Radius				Remarks	Figure 4.10.2-1 Referenced
	Outer in.	mm	Inner in.	mm		
(a) Openings, panels, covers (corner radii in plane of panel)	0.25 0.12	6.4 3.0	0.12 0.06	3.0 1.5	Preferred Minimum	
(b) Exposed corners:	0.50	13.0	–	–	Minimum	(a)
(c) Exposed edges: (1) 0.08 in. (2.0 mm) thick or greater (2) 0.02 to 0.08 in. (0.5 to 2.0 mm) thick (3) less than 0.02 in. (0.5 mm) thick	0.04	1.0	–	–	Full Radius Rolled or Curled	(b) (c) (d)
(d) Flanges, latches, controls, hinges, and other small hardware operated by the pressurized-gloved hand	0.04	1.0	–	–	Minimum required to prevent glove snagging	–
(e) Small protrusions (less than approximately 3/16 in. (4.8 mm)) on toggle switches, circuit breakers, connectors, latches, and other manipulative devices	0.04	1.0	–	–	Absolute minimum unless protruding corner is greater than 120°	

* A 45° chamfer by 0.06 in. (1.5 mm) (minimum) with smooth broken edges is also acceptable in place of a corner radius. The width of chamfer should be selected to approximate the radius corner described above.

SSP 51721
Baseline

TABLE 4.10.2.1-2 EDGE, CORNER, AND PROTRUSION CRITERIA – PROTRUSIONS AND OUTSIDE CORNERS

Application	Criteria/remarks
Latching devices	<p>All latching devices must be covered in a manner that does not allow gaps or overhangs that can catch fabrics or pressure suit appendages, or must be designed in a manner to preclude the catching of fabrics and pressure suit appendages.</p> <p>All surfaces and edges must be smooth, rounded, and free of burrs.</p>
Lap joints in sheet metal and mismatching of adjacent surfaces	<p>All surfaces must be mated within 0.03 in. (0.8 mm) of flat surface at edges, or must be butted or recessed. All exposed edges must be smooth and radiused 0.06 in. (1.5 mm) minimum, chamfered 45°, or must be covered with an appropriate material to protect EVA gloves.</p>
Sheet metal structure, box and cabinet three-plane intersecting corners	<p>Spherical welded or formed radii must be required unless corners are protected with covers.</p>
Screwheads, bolts, nuts, and nut plates, excess threads and rivets that can be contacted by crewmember	<p>All screwheads and boltheads must face the outside of the structure, if possible. Where nuts, nut plates, and threads are exposed, the nuts, nut plates and threads must be covered in a secure manner. Recessed heads or the use of recessed washers is recommended. Overall height of heads must be within 0.125 in. (3.2 mm) or covered unless more than 7 head diameters apart from center to center. Height of roundhead or ovalhead screws is not limited. Screwheads or boltheads more than 0.25 in. (6.4 mm) deep must be recessed or be covered with a fairing, except those intended to be EVA crew interfaces.</p> <p>Rivet heads must face out on all areas accessible to crewmember and must protrude no more than 0.06 in. (1.5 mm) unless spaced more than 3.5 head diameters from center to center. In all exposed areas where unset ends of rivets extend more than 0.12 in. (3.0 mm), or 0.50 in. (12.7 mm) of unset and diameter if more than 0.12 in. (3.1 mm), a fairing must be installed over them. This applies to explosive, blind, or pull rivets, etc. Unset ends of rivets must have edges chamfered 45° or ground off to a minimum radius of 0.06 in. (1.5 mm).</p> <p>A maximum gap of 0.02 in. (0.5 mm) must be allowed only between one side of a fastener head and it's mating surface.</p> <p>Burrs must be prevented or eliminated. Use of Allen heads is preferred. Torque-set, slotted, or Phillips head screws must be covered with tape or other protective materials or be individually deburred before flight.</p> <p>Screws or bolts with exposed threads protruding greater than 0.12 inches in length, must have protective features that do not prevent installation or removal of the fastener.</p>
Safety Wire	<p>Safety wire (lock wire) and cotter pins must not be used on exposed surfaces.</p>
Thin Materials	<p>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, must have edge radii greater than 0.003 inches.</p>

SSP 51721
Baseline

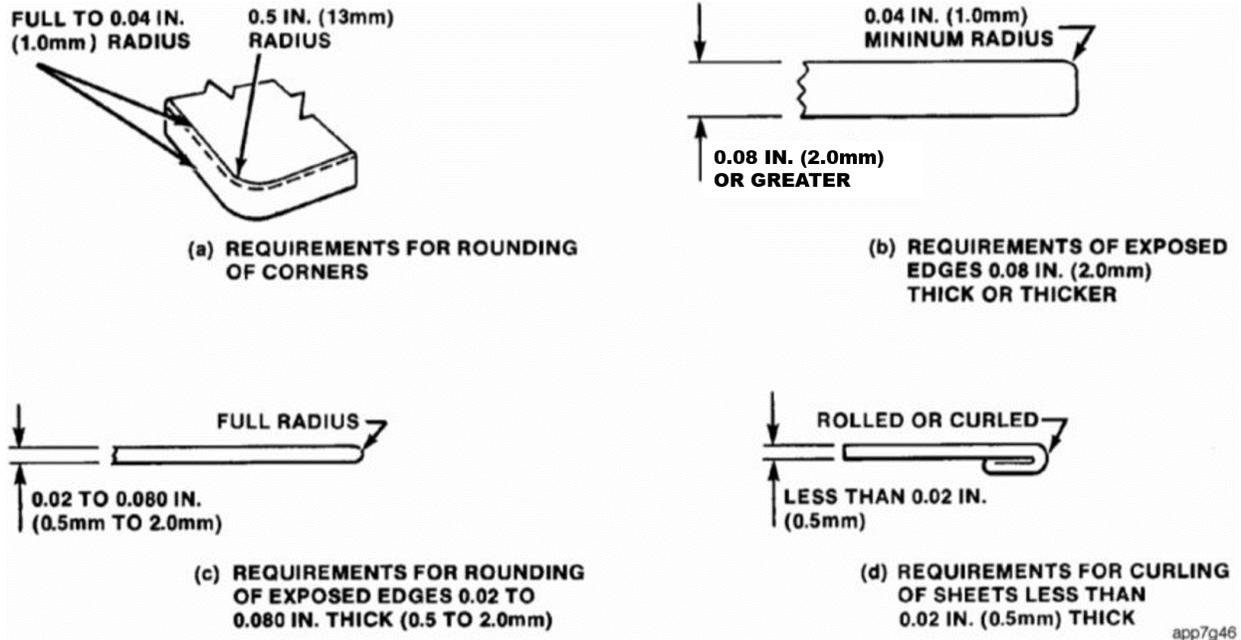


FIGURE 4.10.2.1-1 EXPOSED CORNER AND EDGE REQUIREMENTS

Rationale

End items in EVA accessible areas must be designed to preclude sharp edges and protrusions or must be covered in such a manner as to protect the crew and critical support equipment.

Additional rationale for this requirement can be found in Appendix D.4.10.2.1.

4.10.2.1.1 VERIFICATION – SHARP EDGES AND PROTRUSIONS

Verification is considered successful when one of the following is completed: (A and B) or C

- A. Inspection of the design drawings to show compliance to Tables 4.10.2.1-1 and 4.10.2.1-2 and Figure 4.10.2.1-1. (I)
- B. Inspection of hardware to drawing or equivalent dimensional inspection to show compliance to Tables 4.10.2.1-1 and 4.10.2.1-2 and Figure 4.10.2.1-1. (I)
- C. Inspection of operational control designating the non-compliant areas as NTA. (I)

4.10.2.2 EVA BURRS

All accessible exposed surfaces **shall** be free of burrs.

Rationale

Regardless of the end item design being in compliance with sharp edge requirements, burrs (ragged edges) can occur during manufacturing/assembly and must be screened and removed.

SSP 51721
Baseline

4.10.2.2.1 VERIFICATION – EVA BURRS

Verification is considered successful when the end items successfully passes an inspection to check for burrs and manufacturing defects. (I)

4.10.3 EQUIPMENT CLEARANCE FOR ENTRAPMENT HAZARD

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard. Entrapment hazards are caused by insufficient clearance, either statically or during movement or rotation of a hardware end item, that results in not meeting any or all of the following requirement:

- A. EVA Holes (entrapment of crew fingers)
- B. Gloved Operation (entrapment of crew hand)
- C. Translation Paths (entrapment of crew body)

4.10.3.1 EVA HOLES

Accessible holes (round, slotted, polygonal), other than tether points in the range of 0.5 to 1.4 inch (12.70 to 35.56 mm) **shall** be covered.

Rationale

A crewmember's gloved finger can become entrapped in holes of this range. Existing EVA tether point requirements call for tether points to have an internal opening of between 0.75 to 1.0 inches. Handrails/holds also have holes in this range, but the crew is trained to avoid these areas.

4.10.3.1.1 VERIFICATION – EVA HOLES

Verification is considered successful when the following are completed:

- A. A review of design shows that holes in this range are covered. (I)
- B. A review of as built hardware shows that holes in this range are covered. (I)

4.10.3.2 GLOVED OPERATION

For operations requiring EVA crewmember hand actuation, clearance **shall** be provided for an EVA gloved hand work envelope in accordance with Figure 4.10.3.2-1, Work Envelope for Gloved Hand.

Rationale

A crewmember's gloved hand can become entrapped in areas of this range.

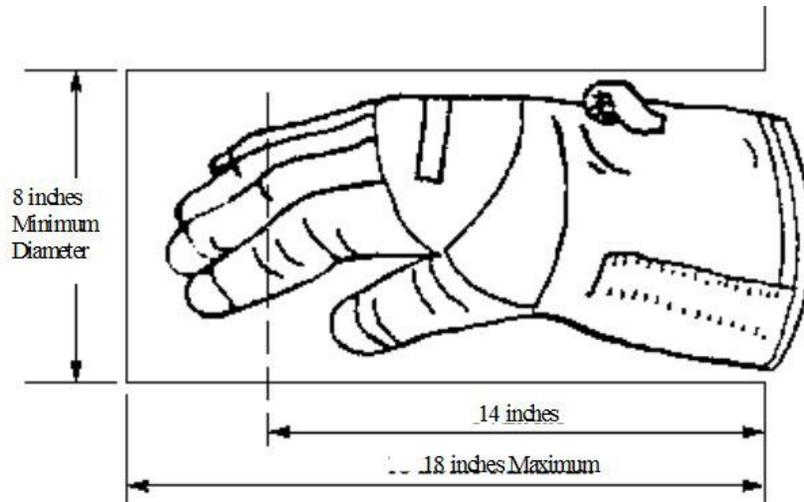


FIGURE 4.10.3.2-1 WORK ENVELOPE FOR GLOVED HAND

4.10.3.2.1 VERIFICATION – GLOVED OPERATION

Verification is considered successful when the analysis shows that glove clearance is provided as specified for EVA hand actuation operations. (A)

4.10.3.3 TRANSLATION PATHS

End items, except for translation aids identified in Table 4.10.1.2-2, **shall** not protrude into a 43 inch diameter translation path.

Rationale

Translation corridors have a minimum diameter of 43 in. (1.09 m) and must have no obstructions or intrusions into the path to allow for hand-over-hand translation of an EVA crewmember. End item design must take the expected location into consideration and assess for potential protrusions. An overall assessment of the specific translation path needed for each EVA is performed at an integrated level.

4.10.3.3.1 VERIFICATION – TRANSLATION PATHS

Verification is considered successful when the following are completed:

- A. Review of the planned on orbit configuration shows the end item does not protrude into the 43” translation path. (I)
- B. ISSP EVA analysis of the integrated configuration prior to each EVA shows there are no violations of the translation paths, or violations are approved by the EVA AIT (Analysis and Integration Team). (A)

SSP 51721

Baseline

4.10.4 PINCH POINTS

End items which pivot, retract, latch or flex such that a gap greater than 0.5 inches but less than 1.4 inches exists **shall** be designed or operated to prevent EVA crew entrapment.

Rationale

This requirement applies to end items that include a motive force such as a motor or spring and that operate with a gap greater than 0.5 inches but less than 1.4 inches. Openings in this range either within the hardware item itself or between the item and adjacent structure could trap crew appendages or pinch the EMU fabric causing damage.

4.10.4.1 VERIFICATION - PINCH POINTS

Verification is considered successful when one of the following is completed:

- A. A review of design drawings and on-orbit configuration shows that pinch points in this range are not crew accessible. (I)
- B. An Operational Control is formally accepted by the operations community to prevent movement during EVA or to establish a KOZ or NTA. (I)

4.10.5 CREW IMPACT FROM MOVING OR ROTATING EQUIPMENT

Moving or rotating equipment in EVA accessible areas **shall** be designed or operated to prevent injury due to EVA crew contact.

Rationale

This requirement is applicable to end items with moving parts that could impact the EVA crew. Controls for this hazard include covering the moving part, showing the movement is too slow or too weak to be a hazard, or implementing an operational control. Operational controls, such as removing power from the moving item when an EVA crewmember is in the area, would only be permitted if design solutions are not possible. The determination of whether an end item is in an EVA accessible areas is made by the ISRP and EVA AIT.

4.10.5.1 VERIFICATION - CREW IMPACT FROM MOVING OR ROTATING EQUIPMENT

Verification is considered successful when one of the following is completed:

- A. Analysis of moving part to verify it is low power/force. (A) – Engineering judgment with ISRP concurrence.
- B. Review of design to verify cover or inhibits. (I)
 - 1. If inhibits are implemented, a test of these inhibits is necessary. (T)
- C. Operational Control agreement to prevent movement during EVA or to establish a KOZ (I)

SSP 51721
Baseline

4.10.6 UNCONTROLLED MOTION OF FLEX HOSES

Flex hoses and lines with delta pressure **shall** be restrained to prevent uncontrolled motion.

Rationale

This requirement is necessary to prevent injury to crew and/or damage to adjacent hardware. Flex hoses and lines can be tethered or connected to prevent whipping.

4.10.6.1 VERIFICATION – UNCONTROLLED MOTION OF FLEX HOSES

Verification is considered successful when review of design and on orbit configuration shows flex hoses and lines are restrained. (I)

4.10.7 ENTANGLEMENT

Cables, conductors, bundles and hoses within EVA accessible areas **shall** be secured.

Rationale

To prevent crew entanglement, cable clamps, ducts, or retractors can be used to secure or enclose cables, conductors, bundles and hoses. The determination of whether an end item is in an EVA accessible area is made by the ISRP and EVA AIT.

4.10.7.1 VERIFICATION – ENTANGLEMENT

Verification is considered successful when review of design and on orbit configuration shows these items are restrained or contained. (I)

4.10.8 COMPONENT HAZARDOUS ENERGY – STORED ENERGY

Components which retain hazardous energy potential **shall** be designed or operated to prevent a crewmember from coming into contact with the stored energy.

Rationale

This applies to mechanical, chemical and electrical sources of stored energy. End items with the potential to release stored energy could inadvertently release this energy in the presence of the EVA crew and cause injury to the crew or damage the EMU which could result in loss of a crewmember. Examples include springs that can release or propel a mass, or cold propellants that can be released creating a pushing force, or chemicals mixing and creating explosive forces or high temperatures (e.g., hot firing propellants). End items must either be designed to prevent a crewmember from releasing the stored energy potential or be designed to allow safing of the potential energy when the crew is in the vicinity. Indicators must confirm that the safing was successful.

4.10.8.1 VERIFICATION – COMPONENT HAZARDOUS ENERGY – STORED ENERGY

Verification is considered successful when the following is completed: A or B or (B and C).

SSP 51721

Baseline

- A. Analysis to show stored energy component has insufficient energy to damage EMU. (A)
- B. Functional test of verifiable inhibits to releasing stored energy. (T)
- C. Operational control to ensure inhibits are in place when EVA is performed. (I)

4.10.9 TOXIC/CORROSIVE MATERIALS

EMU exposure to toxic or corrosive materials **shall** be controlled.

Rationale

Exposure to toxic or corrosive materials can cause damage to the EMU or contaminate the air lock and/or IVA environment. Materials and material processing for hardware that contain or condition fluids, which interface with the EMU are assessed per JSC 66695 and approved by the NASA Materials Group.

Toxic or corrosive materials should be completely contained whenever possible. Self-Sealing QDs (e.g., 1F45541, 1F00799) should be used on components of fluid systems which would create a hazardous condition during on-orbit maintenance. Detection and decontamination capabilities must be provided for hazardous materials that cannot be contained, such as propellants, or have the potential to leak and contaminate the EMU, such as ammonia. Detection and decontamination capability is not a control for the hazard, rather a response to a contingency situation after all fault tolerance is exhausted. Materials that could cause discoloration of the EMU should not be considered since they can affect the thermal properties of the suit.

The most common toxic or corrosive materials outside the ISS and visiting vehicles are monomethyl hydrazine (MMH), nitrogen tetroxide, unsymmetrical dimethyl hydrazine (UDHM) and partial reaction products from engine firings (fuel-oxidizer reaction products (FORP)) plus ammonia.

4.10.9.1 VERIFICATION – TOXIC/CORROSIVE MATERIALS

Verification are considered successful when (A, B, C, D, E, F and G) or (G and H) are completed:

- A. End item materials and material processing including capability with EMU are submitted for review and approved by NASA Materials Group. (A)
- B. Analysis and testing show flow control devices provide insulation to prevent fluid release onto the EMU. (A and T)
- C. Analysis and testing show electrical inhibits are independent and do not open more than one flow control device. (A and T)
- D. Analysis and testing shows monitoring of the appropriate electrical inhibits. (A and T)
- E. Inspection of procedures shows operational controls are in place to ensure the inhibit(s) are inserted or/and confirmed prior to EVA activity. (I)
- F. Inspection of operational controls include NTA or KOZ prior to EVA. (I)

SSP 51721

Baseline

- G. Inspection shows as built hardware is as designed per drawings. (I)
- H. Testing show that venting does not contact the EMU. (A and T)

4.11 MICROMETEOROID AND ORBITAL DEBRIS

Meteoroids occur naturally in space and usually originate from comets or asteroids. Orbital debris is manmade materials that remain in orbit around the earth. Both types of objects travel at extremely high velocities and pose a risk to all hardware mounted externally on the ISS. Hardware items, such as pressure vessels, cryogenic carriers, and other stored energy devices require Micrometeoroid and Orbital Debris (MMOD) protection since they could create a catastrophic hazard if impacted or penetrated by a meteoroid or orbital debris particle. Other resulting hazards of MMOD strikes can include fluid leakage, glass fragments, or other debris.

4.11.1 MICROMETEOROID AND ORBITAL DEBRIS

Payload and Systems end items with the potential to create a catastrophic hazard if impacted or punctured by MMOD (excluding cargo and crew transport vehicles) **shall** be designed in accordance with SSP 52005, Payload Flight Equipment Requirement and Guidelines for Safety Critical Structures with an assessed Probability of No Penetration (PNP) to be \geq required minimum PNP (the lesser of 0.9999 or $0.99999^{(A*Y)}$) MMOD protection for cargo and crew transport vehicles **shall** be designed in accordance with SSP 50808, International Space Station (ISS) to Commercial Orbital Transportation Services (COTS) Interface Requirements Document (IRD), with an assessed PNP to be greater than or equal to the required minimum PNP as determined by $0.99998^{(A*Y)}$.

A = Total hazardous impact surface area of the end item or cargo/crew vehicle in square meters (surface area should not include elements of the end item that do not represent catastrophic hazard to crew or station survivability if failed due to impact such as radiators and solar arrays), while Y = Exposure time in years.

NOTE: Requirements defined here and in SSP 52005 and SSP 50808 do not alter or define the existing ISS process for evaluation of MMOD contribution to ORU failure rates or ORU procurement decisions. ORU procurement decisions based on predicted MMOD failure events are evaluated on a case-by-case basis and procurement decisions made by appropriate ISS boards.

Rationale

MMOD strikes to externally mounted end items with catastrophic hazard potential can result in loss of the ISS or endanger the crew.

Additional rationale for this requirement can be found in Appendix D.4.11.1.

4.11.1.1 VERIFICATION – MICROMETEOROID AND ORBITAL DEBRIS

Verification is considered successful when either A or B are completed:

- A. Analysis shows that assessed PNP is \geq the required PNP with the assessed PNP determined using the Bumper 3 (or approved equivalent) analysis code with the

SSP 51721

Baseline

meteoroid and orbital debris environments per SSP 52005 (payloads and systems end items) or SSP 50808 (crew and cargo vehicles). (A)

- B. Test and analysis show end item design provides protection from MMOD per SSP 52005 (payloads and systems end items) or SSP 50808 (crew and cargo vehicles). (A, T)

Verification B is required if no applicable hypervelocity impact test data is available for the proposed end item or cargo/crew vehicle MMOD protection.

4.12 PROPULSION SYSTEMS

Premature firing of a solid propellant rocket motor or liquid propulsion system, while the end item is closer to the ISS than the minimum safe distance, is a catastrophic hazard. This includes, but is not limited to, considerations of plume effects, contamination, and collision or recontact with ISS. Refer to Section 4.2 (or IRDs) for plume effects such as shock, vibration, etc. Refer to Section 4.7.2.1, Hazardous Materials External Release, for contamination protection. To prevent this situation from occurring, it is necessary for end items to maintain failure tolerance and have the ability to monitor inhibits and health of the propulsion system. This section provides requirements for both solid and liquid propellants for all thrusters. It is necessary for hybrid systems to meet both solid and liquid requirements until proven the solid will not sustain a burn without the liquid propellant. Liquid propellant systems include all forms of fluids (e.g., gas, gel, liquid).

All crewed or un-crewed vehicles that are berthed or docked to the ISS and end items adhere to this section.

Safe Distance

The safe distance is determined using Figure 12.1-1. The hazard of engine firing close enough to inflict damage to the ISS due to heat flux, contamination, and/or perturbation of the ISS, is in proportion to the total thrust imparted by the engine in any axis and is controlled by establishing a safe distance for the event. For the collision hazard with the ISS, it is necessary to consider with consideration of many variables such as deployment method, appendage orientation, and control authority.

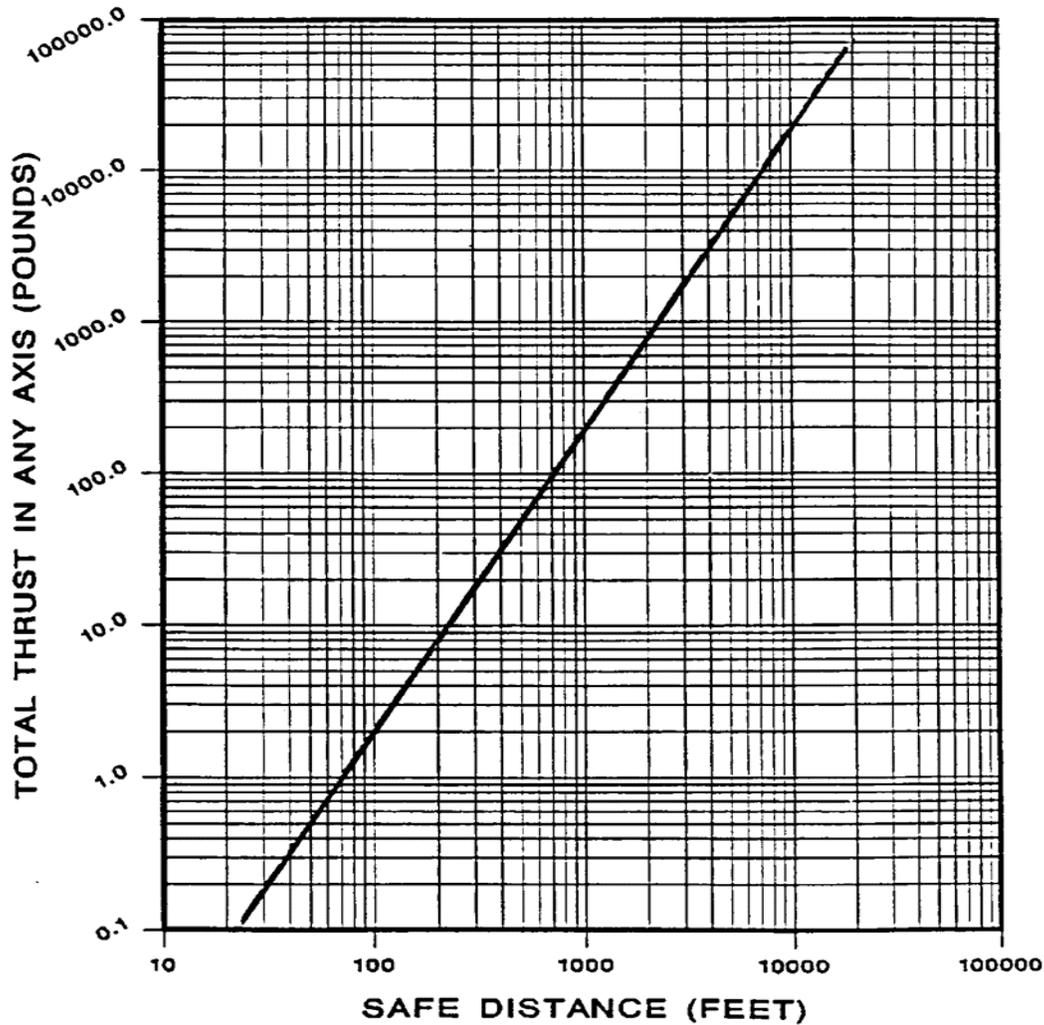


FIGURE 4.12-1 SAFE DISTANCE FOR FIRING THRUSTERS

4.12.1 SOLID PROPELLANT ROCKET MOTORS

End items with solid propellant rocket motors **shall** only be fired when outside the ISS safe distance and in an adequately fault tolerant orientation that precludes short term or long term re-contact with the ISS.

Rationale

Premature firing of a solid propellant rocket motor, while the end item is closer to the ISS than the minimum safe distance, is a catastrophic hazard.

Additional rationale for this requirement can be found in Appendix D.4.12.1.

4.12.1.1 VERIFICATION – SOLID PROPELLANT ROCKET MOTORS

Verification is considered successful when the following are completed:

- A. End items with a positive separation will show in the design that fire initiation does not start until the spacecraft has reached a minimum ISS safe distance. For

SSP 51721
Baseline

end items deployed with the SSRMS or JEM Arm sequencing is initiated by a real-time RF command. (T).

- B. Design includes the appropriate number of independent electrical inhibits. (I)
- C. Approval by ISSP of planned orientation at deployment. (I)
- D. Design includes S&A device and appropriate electrical inhibits. (I)
- E. If applicable, end items equipped with S&A device:
 - 1. S&A device is designed and tested in accordance with provisions of MIL-STD-1576, Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems. (T)
 - 2. If the S&A device is to be rotated to the arm position prior to the end item achieving a safe distance from the ISS:
 - a. Operational Control to include rotation performed as part of the final deployment activities. (I)
 - b. Initiator meets the requirements of Section 4.13. (I)
 - 3. Includes capability to resafe the S&A device. (I)

4.12.2 LIQUID PROPELLANT PROPULSION SYSTEMS

End items **shall** prevent catastrophic consequences due to uncontrolled thrusting of liquid propellant rocket motors.

Rationale

The premature firing of a liquid propellant propulsion system can cause a catastrophic hazard.

Additional rationale for this requirement can be found in Appendix D.4.12.2.

4.12.2.1 VERIFICATION- LIQUID PROPELLANT PROPULSION SYSTEMS

Verification is considered successful when the following are completed:

- A. Propellant flow control devices:
 - 1. The design of the propellant delivery system in end item liquid propellant thruster systems contains a minimum of two (three if in a primary EVA translation path or if using monopropellant) 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). If the end item is a bi-propellant system, the minimum number of devices apply to both the oxidizer and fuel sides. (I and T)
 - 2. The design shows that one of the flow control devices isolates the propellant tank(s) from the remainder of the distribution system. (I and T)

SSP 51721

Baseline

3. The thruster valves in End Item liquid propellant thruster system are designed to return to the closed position in the absence of an opening signal with appropriate force margin. (I and A)
- B. Design is such that the failure of one of the electrical inhibits does not open more than one flow control device. (I)
- C. Design includes monitoring of the appropriate electrical inhibits. (I)
- D. Analysis shows end item thrusters do not impinge on the ISS and cause a hazard. (A)

4.12.3 ADIABATIC/RAPID COMPRESSION DETONATION

The end item propulsion system **shall** be insensitive to Adiabatic, or rapid, Compression Detonation (ACD).

Rationale

This phenomenon is possible for propellants that can decompose exothermically. Hydrazines are the most commonly used propellant of this type, but it is necessary for other propellants and fluids (e.g., Nitrous Oxide, and Hydrogen Peroxide (H₂O₂)) to be assessed for sensitivity to ACD and similarly addressed.

Additional rationale for this requirement can be found in Appendix D.4.12.3.

4.12.3.1 VERIFICATION - ADIABATIC/RAPID COMPRESSION DETONATION

Verification is considered successful when the following are completed:

- A. System analysis of the transient pressure during all operational environments on the ground and in flight. (A)
- B. Test plans are approved by JSC Propulsion Branch. (I)
- C. Test results are accepted by JSC Propulsion Branch. (I)
- D. Pressure monitor on downstream lines is in place. (I)

4.12.4 PROPELLANT OVERHEATING

Components in propellant systems that are capable of heating the system **shall** prevent heating the propellant above the material/fluid compatibility limits of the system.

Rationale

Components capable of heating the system are heaters, valve coils, etc. Raising the temperature of a propellant above the fluid compatibility limit for the materials of the system is a catastrophic hazard.

Additional rationale for this requirement can be found in Appendix D.4.12.4.

SSP 51721

Baseline

4.12.4.1 VERIFICATION- PROPELLANT OVERHEATING

Verification is considered successful when thermal analysis of the capabilities, including failure scenarios, of the system shows that the material/fluid remains below the compatibility limit. (A)

4.12.5 PROPELLANT LEAKAGE

Leakage of propellant whose release would create a hazard **shall** be prevented.

Rationale

It is necessary for an end item to be two failure tolerant to prevent leakage of propellant past seals, seats, etc., if the leak has a flow path to the storage vessel. If the leak is in an isolated segment of the distribution system, failure tolerance to prevent the leak will depend on the type and quantity of propellant that could be released. As a minimum, the design is to be one failure tolerant to such a leak. Leakage of non-hazardous fluids may be acceptable, based on considerations of effects and quantities, with ISRP review and approval.

4.12.5.1 VERIFICATION - PROPELLANT LEAKAGE

Verification is considered successful when:

- A. The design includes appropriate failure tolerance to prevent leakage. (I)
- B. Leak test done in accordance with SSP 41172 or equivalent specification shows that the maximum allowable leakage rate requirement has met the design that includes appropriate failure tolerance to prevent leakage. (T)

4.12.6 MONITORING PROPULSION SYSTEM STATUS

The end item **shall** provide real-time propulsion system health and status telemetry.

Rationale

It is necessary for the end item to provide real-time data related to pressure, temperature, and quantity gauging of propulsion system tanks, components, and lines to ISS. Monitoring gives the ISS insight into the health of the propulsion system and provides notice of any developing issues.

Additional rationale for this requirement can be found in Appendix D.4.12.6.

4.12.6.1 VERIFICATION- MONITORING PROPULSION SYSTEM STATUS

Verification is considered successful when review of design shows health and status data is provided to the ISS or ground controllers per Sections 4.5.1 and 4.5.2. (I)

4.13 PYROTECHNIC SYSTEMS

Pyrotechnic systems (explosive-loaded and explosively-actuated, non-loaded devices) can create a hazard due to failure to fire and/or inadvertent firing, including explosion debris and collision of released materials with ISS. Hazard causes associated with

**SSP 51721
Baseline**

ground processing, natural and induced environments, hardware/software failure modes, and operator error must be considered.

Malfunction and inadvertent operation of control circuits caused by extremes of ground and flight environments must be avoided by protective design features.

All pyrotechnic device electrical and containment safety requirements are stated in the following paragraphs. This is dictated by the following figure and can be used for guidance.

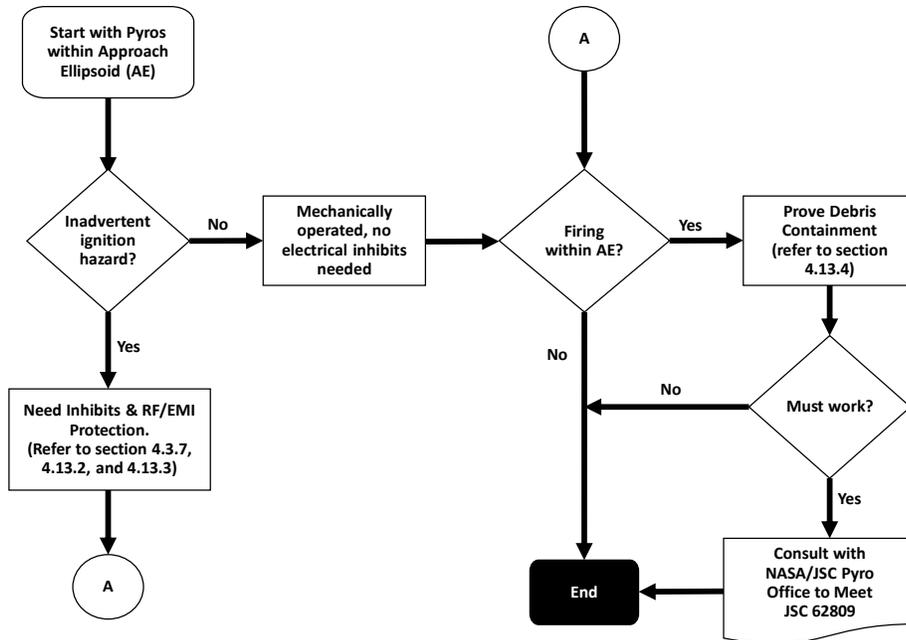


FIGURE 4.13-1 PYROTECHNIC DEVICE ELECTRICAL AND CONTAINMENT SAFETY REQUIREMENTS

4.13.1 PYROTECHNIC LOSS OF FUNCTION (MUST WORK)

If failure to function is catastrophic, the design of the pyrotechnic subsystem shall be in accordance with JSC 62809, Human Rated Spacecraft Pyrotechnic Specification.

Rationale

Where failure to operate causes a catastrophic hazard, pyrotechnic operated devices are designed, controlled, inspected, and certified to criteria equivalent to those specified in JSC 62809. End Item hardware provider should consult the NASA JSC Pyrotechnics Office for guidance as early as possible.

Additional rationale for this requirement can be found in Appendix D.4.13.1.

4.13.1.1 VERIFICATION - PYROTECHNIC LOSS OF FUNCTION (MUST WORK)

Verification is considered successful when the design of the pyrotechnic subsystem device shows compliance to JSC 62809.

SSP 51721
Baseline

4.13.2 ELECTRICAL EXPLOSIVE DEVICES

Electrical Explosive Devices (EED) **shall** meet the requirements of MIL-STD-1576.

Rationale

Over the years it has been NASA and Department of Defense's (DoD's) experience that the most reliable and preferred initiators are the NASA Standard Initiators (NSI). If other initiators are used, the hardware provider needs to perform an extensive qualification and acceptance test program. NSI's have undergone extensive testing to show that they will function as intended when used as designed. By selecting these type of devices the end item provider can avoid costly qualification and acceptance testing.

Additional rationale for this requirement can be found in Appendix D.4.13.2.

4.13.2.1 VERIFICATION- ELECTRICAL EXPLOSIVE DEVICES

Verification is considered successful when one of the following is completed:

- A. NSI selected for use:
 - 1. List of all pyrotechnic initiators installed or to be installed on the end item, including the function to be performed, the part number, the lot number, and the serial number. (I)
- B. Non-NSI EED selected for use:
 - 1. Design of the EED meets MIL-STD-1576 or NASA approved equivalent. (I)
 - 2. The qualification and acceptance test program is approved by the NASA JSC Pyrotechnic Group. (I)
 - 3. The test data has been approved and accepted by the NASA JSC Pyrotechnic Group. (I)
 - 4. List of all EED installed or to be installed on the end item, including the function to be performed, the part number, the lot number, and the serial number. (I)

SSP 51721
Baseline

4.13.3 PYROTECHNIC ELECTRICAL CIRCUITS

The firing circuits associated with pyrotechnic functions **shall** be designed to preclude inadvertent firing or failure to fire.

- A. Connectors and pins have no short circuit paths.
- B. Firing circuits are isolated and capable of carrying the initiator firing current.
- C. Monitor circuits and test equipment that doesn't compromise the safety of the firing circuit.
- D. Separate and dedicated power distribution points.
- E. Firing source circuit return side is isolated.
- F. Firing circuit is grounded at one point only and not a structural ground.
- G. Wiring uses shielded twisted pairs.
- H. Cables fabricated will use no splicing and connectors provided for mating and demating.
- I. Cable shielding provides a minimum of 90 percent of optical coverage with 360 degree continuous shields that are grounded to structure.
- J. All current-carrying components and conductors are electrically insulated from each other and system ground.
- K. Three inhibits shall be in place to make a two fault tolerant configuration for inadvertent firing.
- L. All firing circuit elements meet JSC 62809 section 8.4 for Electromagnetic Compatibility (EMC).
- M. Firing circuit is completely shielded.
- N. Firing circuit switching devices are protected to prevent inadvertent operation or degradation.
- O. Circuit elements have low DC bonding resistance to connection points.
- P. EEDs withstand up to one Amp and one Watt constant DC firing pulse.
- Q. EEDs are protected from electrostatic hazards.
- R. EEDs withstand electrostatic discharge and do not fire, dud, or deteriorate.

Rationale

If designed incorrectly, the firing circuit could cause a hazard by firing prematurely or not firing as expected.

Additional rationale for this requirement can be found in Appendix D.4.13.3.

4.13.3.1 VERIFICATION – PYROTECHNIC CONNECTORS AND PINS

Verification is considered successful when the following are completed:

SSP 51721

Baseline

- A. Connectors are approved by NASA. (I)
 - 1. Shell is stainless steel or other suitable electrically conductive finish.
 - 2. Shell-to-shell connection is before the pins connect.
 - 3. Shell provides 360 degree shield continuity.
- B. Circuit design does not share pins in multi-pin connectors with other load carrying circuits. (I)
- C. Any single short circuit occurring as a result of a bent pin or contamination does not result in more than 50 mA or one-tenth of the no fire current whichever is less applied to any EED. (A and T)
- D. One wire is used per pin. (I)
- E. No connector pins are used as a terminal or tie-point for multiple connections. (I)
- F. No spare pins are in connectors which are part of firing output circuitry. (I)
- G. Source circuits are terminated in a connector with socket contacts. (I)

4.13.3.2 VERIFICATION – FIRING CIRCUITS

Verification is considered successful when the following are completed:

- A. Circuit design includes a separate firing circuit for each EED. (I)
- B. The EED's firing circuit is isolated. (I or T)
- C. The EED's firing circuit has the capability to carry the initiator firing current. (A)
- D. Safing of firing circuits is accomplished by removal of the arm command. (T)
- E. Arming power dissipates within 30 seconds. (T)
- F. Arm/disarm indicator circuits are hardwired for mission critical functions, or the indicator circuits are at least as reliable as the operational firing circuits. (A or I)
- G. Arm/disarm indicator circuits are isolated from firing circuits. (I and T)
- H. Independent timing circuits used as logic for firing pyrotechnic devices are fail-safe. (A)
- I. The primary failure mode of the independent timing circuit does not result in an unsafe condition. (A)

4.13.3.3 VERIFICATION – PYROTECHNIC MONITOR CIRCUITS

Verification is considered successful when the following is completed:

- A. Application of operational voltage to the monitor circuit does not compromise the safety of the firing circuit nor cause the electroexplosive subsystem to be armed. (A)
- B. Monitoring currents are limited to one-tenth of the no-fire current level of the EED or 50 mA whichever is less. (T)

SSP 51721

Baseline

- C. Design of the monitor circuits and test equipment that applies current to the bridgewire limits the open circuit output voltage to 1 V. (T)
- D. The design utilizes best practices to preclude sneak circuits and unintentional electrical paths. (A)

4.13.3.4 VERIFICATION – SEPARATE FIRING SOURCE POWER DISTRIBUTION POINTS

Verification is considered successful when separate and dedicated power distribution points are used for the electro-explosive subsystem firing sources. (I)

4.13.3.5 VERIFICATION – FIRING SOURCE CIRCUIT RETURN SIDE ISOLATION

Verification is considered successful when one of the following is completed:

- A. The return side of the firing source circuit is isolated from structure by at least 10k Ω measured at 1.5 times the bus voltage or greater, or equivalent isolation. (T)
- B. The firing source circuit design contains isolation transformers that provide at least 10k Ω isolation between the end item return circuit and the vehicle return circuit when measured at 1.5 times the bus voltage or greater. (T)

4.13.3.6 VERIFICATION – PYROTECHNIC CIRCUIT GROUNDING

Verification is considered successful when the following are completed:

- A. Design of the firing circuits shows that any grounding is completed at one point only. (I)
- B. Analysis of the return path, on all circuits, minimizes voltage buildup and transients on the firing circuit return with respect to the single point ground. (A)
- C. Ungrounded firing output circuits are connected to structure by static bleed resistors. (I)
- D. There are no structural grounds used as return for pyrotechnic circuitry. (I)
- E. Electroexplosive subsystems include positive protection for line-to-line and line-to-ground shorts which may develop within a fired EED. (A)

4.13.3.7 VERIFICATION – PYROTECHNIC WIRING

Verification is considered successful when the following are completed:

- A. Shielded twisted pairs are used for all pyrotechnic circuitry wiring. (I)
- B. Shielded twisted pairs are not connected directly to vehicle structure and are isolated from vehicle direct current returns through a minimum of 100k Ω resistance. (I and T)
- C. Firing output circuits are physically separated from all other types of circuits. (I)
- D. Firing circuit wiring are routed separately (in separate trays or conduit) from all other current carrying circuits including electrical power, electrical control, RF transmission lines, and monitoring circuitry. (I)

SSP 51721

Baseline

- E. Firing circuits that do not share a common fire command are electrically isolated from one another such that current in one firing circuit does not induce a current greater than 16.5 dB below the no-fire current level in any firing output circuit. (I and T)
- F. Control circuits are electrically isolated so that a stimulus in one circuit does not induce a stimulus greater than 16.5 dB of the actuation level in any firing circuit. (T)

4.13.3.8 VERIFICATION – CABLE AND HARNESS DETAILS

Verification is considered successful when the following are completed:

- A. No splices are used to join elements of ordnance cables. (I)
- B. A connector is provided wherever a mating or demating circuit is required. (I)
- C. All cable runs are routed at a separation from structure not to exceed 5 cm for metal, 2.5 cm for conductive composite material (e.g., epoxy graphite). (I)

4.13.3.9 VERIFICATION – CABLE SHIELDING

Verification is considered successful when the following are completed:

- A. Cable shielding provides a minimum of 90 percent of optical coverage. (I)
- B. Cable shields terminated at a connector provide 360 degree continuous shield continuity without gaps. (I)
- C. Cable shields are grounded to vehicle structure through the EED connector and body. (I)
- D. Cable shields are not used as intentional current-carrying conductors. (I)

4.13.3.10 VERIFICATION – INSULATION RESISTANCE

Verification is considered successful when the following are completed:

- A. All current-carrying components and conductors are electrically insulated from each other and system ground. (I or T)
- B. The insulation resistance value between all insulated parts, is greater than 2 M Ω after exposure to the specified operational environment. Use the following potentials depending on the component: (T)
 - 1. 500V, minimum, dc
 - 2. \leq 250Vdc for the NSI (only one 250Vdc test is permitted)
 - 3. 50Vdc for all other testing on NSIs after the initial 250Vdc test
- C. Voltage breakdown from the balanced two-wire line to vehicle structure or direct current return is greater than 1050 Vac rms at a frequency of 60 Hertz or 1500 Vdc. (T)

SSP 51721
Baseline

4.13.3.11 VERIFICATION – TWO FAULT TOLERANT CONDITION

Verification is considered successful when the following are completed: A and (B or C)

- A. For those applications where premature firing may result in a catastrophic event, the pyrotechnic system need to be two fault tolerant against inadvertent firing. Control circuits will include an arming circuit which is energized by a separate signal or action prior to initiation of the firing signal.(I)
- B. Inhibits will be independent. Signals activating the inhibits will be independent.(I)
- C. Inhibits will be on both high voltage and return side of the circuit.(I)

4.13.3.12 VERIFICATION – PYROTECHNIC ELECTROMAGNETIC COMPATIBILITY

Verification is considered successful when the following are completed:

- A. The electroexplosive subsystem meets the requirements of Sections 4.3.7. (A or T)
- B. In the event that NSIs are selected, external operating frequencies are identified that have not previously been used for NSI certification and to which the NSIs could be exposed, MIL-STD-1576 Test Methods 2204 and 2207 were performed at those frequencies only. (T)
- C. In the event that NSIs are not selected, MIL-STD-1576 Test Methods 2204 and 2207 were performed to identify the RF impedance and sensitivity of the selected devices. (T)
- D. If the electroexplosive subsystem is non-compliant with any of the requirements in MIL-STD-1576 that could have an impact on electromagnetic environmental susceptibility, or if the electroexplosive subsystem utilizes an EED which NASA considers abnormally susceptible to the electromagnetic environment, then a worst-case analysis in accordance with Test Method 4303 was performed on all firing circuits for all storage, transportation, handheld, checkout and fully assembled configurations of the firing systems that can be exposed to the radiated electromagnetic environment. (A and T)

4.13.3.13 VERIFICATION – FIRING CIRCUIT SHIELDING

Verification is considered successful when the following are completed:

- A. The firing circuit including the EED is completely shielded or shielded from the EED back to a point in the firing circuit at which isolators eliminate RF entry into the shielded portion of the system. (I)
- B. EEDs do not fire in either the pin-to-pin or the pin-to-case mode due to direct coupling of the specified electromagnetic environment into the EED. (T)
- C. Command and control interfaces with the host vehicle used for any arming or firing functions are not activated or triggered by return currents flowing in the host vehicle or end item structure. (T)

SSP 51721

Baseline

- D. RF susceptibility protection for the EEDs is provided by a metallic enclosure which provides 360 degrees of coverage. (I)
- E. With the exception of cable shielding, there are no gaps or discontinuities in the shielding, including the termination at the back faces of the connectors, nor apertures in any container which houses elements of the firing circuit. (I)
- F. The electroexplosive subsystem is designed to limit the power produced at each EED by the electromagnetic environment acting on the subsystem to a level at least 16.5 dB below the maximum pin-to-pin DC no-fire power of the EED. (T)

4.13.3.14 VERIFICATION – PROTECTION OF FIRING CIRCUIT SWITCHING DEVICES

Verification is considered successful when the following are completed:

- A. Firing circuit switching devices are protected to prevent inadvertent operation. (A and I)
- B. Firing circuit switching devices are protected to prevent degradation by high voltage spikes or reverse voltages caused by transients due to load switching, RF interference, lightning, etc. (A or I or T)

4.13.3.15 VERIFICATION – PROTECTION OF DEVICES THAT CAN COMPLETE FIRING CIRCUIT

Verification is considered successful when the electro-explosive subsystem is designed to limit the power produced at each device in the firing circuit that can complete any portion of the firing circuit to a level at least 6dB below the minimum activation power for each of the safety devices. (A or T)

4.13.3.16 VERIFICATION – PYROTECHNIC ELECTRICAL BONDING

Verification is considered successful when the DC bonding resistance between electrical pyrotechnic circuit elements, and connection points of the shielded system, metallic enclosures, and structural ground is 2.5 mΩ or less. (T)

4.13.3.17 VERIFICATION – MINIMUM DEVICE WITHSTAND CAPABILITY

Verification is considered successful when the EEDs withstand a constant direct current firing pulse of up to 1 ampere and 1 watt power (minimum) for a period of five minutes (minimum) duration without initiation or deterioration of performance (dudding). (T)

4.13.3.18 VERIFICATION – USE OF BLEED RESISTORS

Verification is considered successful when the EEDs are protected from electrostatic hazards.

- A. Verification is considered successful the EEDs are protected from electrostatic hazards by the placement of resistors from line-to-line and from line-to-ground (Structure). (I)
- B. The parallel combination of these resistors are to be 10K ohms or more. (T)

4.13.3.19 VERIFICATION – ELECTROSTATIC DISCHARGE WITHSTAND

Verification is considered successful when the EEDs do not fire, dud, or deteriorate in performance as a result of being subjected to an electrostatic discharge of 25,000 Volts (V) from a 500 picofarad (pF) capacitor applied in the pin-to-case mode with no series resistor, and in the pin-to-pin mode with 5 K Ω resistor in series. (T)

4.13.4 PYROTECHNIC MECHANICAL CONTAINMENT

Pyrotechnic devices **shall** be designed to contain the effects of shock, debris, and hot gasses resulting from operation using these features:

- A. Tensile testing is performed on:
 - 1. Component parts that are heat treated after receiving from the mill.
 - 2. Component parts that have to withstand operating pressures or primary structural loads or both.
- B. Threaded parts are positively locked.
- C. The pyrotechnic blast is contained.
- D. Locked-shut firing test is conducted without fragmentation.
- E. Design yield FOS is a minimum of 1.1.
- F. Design ultimate FOS is a minimum of 1.4.
- G. Cartridge assembly can withstand 1.5 times the specified maximum allowable installation torque.
- H. Pressure cartridges and propellant actuated devices meet the proof pressure.

Rationale

This pyrotechnic containment section covers requirements for debris containment from pyrotechnics use, including design, development, and qualification.

Additional rationale for this requirement can be found in Appendix D.4.13.4.

4.13.4.1 VERIFICATION – TENSILE TESTING OF METALLIC PARTS

Verification is considered successful when the following are completed:

- A. A tensile test was performed for component parts that are heat treated after receiving from the mill. (T)
- B. A tensile test was performed for component parts that are required to withstand operating pressures or primary structural loads or both. (T)
- C. A test of the standard mechanical properties with the raw material was performed and all test data required by the material specification are included in the report. (T)

4.13.4.2 VERIFICATION – RETENTION OF THREADED PARTS

Verification is considered successful when all threaded parts are positively locked. (I)

4.13.4.3 VERIFICATION – BLAST CONTAINMENT

Verification is considered successful when a test is performed to demonstrate that the output of all pyrotechnic devices, except destruct charges, pose no hazard to crew or vehicle. (T)

4.13.4.4 VERIFICATION – LOCKED-SHUT TEST

Verification is considered successful when the following are completed:

- A. A locked-shut firing test, without fragmentation, is conducted at nominal pyrotechnic load to demonstrate this capability for pyrotechnic devices. (T)
- B. Pressure-actuated devices withstand internal pressures generated in operation with the movable part restrained in its initial position and without rupture or the release of shrapnel, debris, or hot gases that could compromise crew safety. (T)
- C. If a failed locked-shut capability results in loss of crew or vehicle, the locked-shut capability is confirmed with redundant charges operating simultaneously. (T)

4.13.4.5 VERIFICATION – DESIGN YIELD FACTOR OF SAFETY

Verification is considered successful when the following are completed:

- A. The design yield FOS is a minimum of 1.1 applied to the limit load. (A)
- B. Components have adequate strength to withstand limit loads without loss of operational capability for the life of the component. (A)

4.13.4.6 VERIFICATION – DESIGN ULTIMATE FACTOR OF SAFETY

Verification is considered successful when the following are completed:

- A. The design ultimate FOS is a minimum of 1.4 applied to the limit load. (A)
- B. Components have adequate strength to withstand ultimate loads without failure. (A)

4.13.4.7 VERIFICATION – CARTRIDGE TORQUE

Verification is considered successful when each cartridge assembly is capable of withstanding 1.5 times the specified maximum allowable installation torque without physical damage. (A)

4.13.4.8 VERIFICATION - PROOF PRESSURE OF PRESSURE CARTRIDGES AND PROPELLANT ACTUATED DEVICES

Verification is considered successful when the following are completed:

- A. Analysis of proof pressure of pressure cartridge and propellant actuated devices are approved by the cognizant NASA fracture control representative. (A and I)
- B. All components exposed to operating pressure are capable of withstanding an internal static proof pressure of 1.2 times the maximum operating pressure without permanent deformation or leakage. (T)

SSP 51721

Baseline

- C. All components exposed to operating pressure are capable of withstanding an internal pressure of 1.5 times the maximum operating pressure without structural failure (burst). (A, I, T)

4.13.5 AUTO-IGNITION

Explosive materials **shall** be able to withstand 50°F above the maximum expected thermal exposure without auto-igniting.

Rationale

The auto-ignition temperature of a pyrotechnic device is the lowest temperature at which it spontaneously ignites in normal atmosphere without an external source of ignition, such as a flame or spark.

Additional rationale for this requirement can be found in Appendix D.4.13.5.

4.13.5.1 VERIFICATION - AUTO-IGNITION

Verification is considered successful when the device does not ignite after being exposed to 50°F above maximum expected temperature for a minimum of one hour. (T)

4.13.6 MAXIMUM ENERGY TEST

Each pyrotechnically-loaded device **shall** be capable of performing its function with 115 percent of the maximum allowable charge weight.

Rationale

Other suitable methods, such as adding powder into the firing cavity, may be applied. This requirement will be satisfied during qualification testing. Devices should not be fabricated specifically to permit 115 percent overload if internal dimensions of the device do not permit overloading.

Additional rationale for this requirement can be found in Appendix D.4.13.6.

4.13.6.1 VERIFICATION - MAXIMUM ENERGY TEST

Verification is considered successful when the following are completed:

- A. The device functioned with 115 percent of the maximum allowable charge weight. (T)
- B. Pyrotechnic devices that provide containment of debris meet the first verification without structural failure. (T)

4.14 DEPLOYMENT, SEPARATION AND JETTISON FUNCTIONS

End items deployed, separated, or jettisoned from the ISS or VVs have the potential to collide with ISS and/or VVs, create orbital debris that can impact ISS, or result in ground impact risks. In this section deploy refers to intentional release of end items. These requirements are intended for deployed, separated or jettisoned end items that are not intended to come back to ISS vicinity.

SSP 51721
Baseline

The primary means for end item disposal or return is via VV reentry/return.

End item inadvertent deployment, separation or jettison is a catastrophic hazard unless it is shown otherwise, and the general inhibit and monitoring requirements of Section 4.5 apply.

When assessing relative motion of a deployed end item the ballistic characteristics of both the ISS and end item will be varied by examining the minimum, average and maximum frontal areas. In general, the worst-case relative motion is obtained by comparing relative motion with the maximum frontal area of the ISS to the end item with the minimum frontal area. The equations in Table 4.14-2, Frontal Area, provide the computation for average area of several geometric shapes.

End items should meet the criteria in Table 4.14-1 Ballistic Number for Deploy Delta Velocity. BN (Ballistic Number) is computed assuming a coefficient of drag (C_d) of two using end item dimensions with appendages in stowed configuration. IP specific ballistic number equations are seen in Table 4.14-3 below. BN calculation will be based on an average of the smallest and second smallest orthogonal frontal areas of the candidate.

TABLE 4.14-1 BALLISTIC NUMBER FOR DEPLOY DELTA VELOCITY

Deploy dV (m/s)	BN (kg/m ²)
< 0.5	≤100
≥ 0.5	≤120

TABLE 4.14-2 AVERAGE FRONTAL AREA

End Item Shape	Equation
Rectangular Box	$A_{ave} = \frac{(l \times w) + (w \times h) + (h \times l)}{3}$
Tumbling	$A_{ave} = \text{Surface area}/4$
Cylinder	$A_{ave} = \frac{2\pi r^2 + 2\pi r l}{4}$
Flat Plate	$A_{ave} = \frac{l \times w}{2}$
Sphere	$A_{ave} = \pi r^2$

TABLE 4.14-3 BALLISTIC NUMBER CALCULATIONS

Name	ID	Equation	Relations	Notes
Ballistic Number	BN	$BN = \frac{M}{C_d A_f}$ <p><i>M = Mass (kg)</i> <i>C_d = Coefficient of Drag</i> <i>A_f = Frontal Area(m²)</i></p>	$BN = \frac{4.905}{Sb}$ $BN = \frac{1}{B^*}$	NASA ballistic characteristic representation
Ballistic Coefficient	Sb	$Sb = \frac{4.905 C_d A}{M}$	$Sb = \frac{4.905}{BN}$ $Sb = 4.905 B^*$	Russian ballistic characteristic representation

SSP 51721
Baseline

B-Term	B*	$B^* = \frac{C_d A_f}{M}$	$B^* = \frac{1}{BN}$ $B^* = \frac{Sb}{4.905}$	USSTRATCOM ballistic characteristic representation
--------	----	---------------------------	--	--

4.14.1 RE-ENTRY HUMAN RISK

End items **shall** limit the risk of human casualty on the ground per the sponsoring IPs re-entry laws and regulations.

Rationale

Each IP has a responsibility for re-entry human risk based on IP's law. For NASA sponsored end items the risk of human casualty on the ground is limited to less than 1 in 10,000 as required per NASA-STD-8719.14A, Process for Limiting Orbital Debris. Note that for NASA sponsored end items there could be additional applicable requirements in NASA-STD-8719.14A that must be met. In 1995, NASA established a policy of limiting the risk of world-wide human casualty from a single, uncontrolled re-entering space structure to 1 in 10,000. For ESA sponsored end items the human casualty risk on ground is found in ESSB-ST-U-004. ESA sponsored end items also have additional requirements in ECSS-U-AS-10C - Adoption note of ISO 24113.

Additional rationale for this requirement can be found in Appendix D.4.14.1.

4.14.1.1 VERIFICATION – RE-ENTRY HUMAN RISK

Verification is considered successful when **one** of the following is completed:

- A. Debris Assessment Software (DAS) re-entry risk assessment reflects less than the United States (US)/IP's re-entry laws and regulations chance of ground fatality. (A)
- B. ORSAT assessment reflects less than the US/IP's re-entry laws and regulations chance of ground fatality. (A)
- C. Comparable analysis to DAS or ORSAT as determined by NASA ODPO reflects less than the US/IP's re-entry laws and regulations chance of ground fatality. (A)

4.14.2 TRACKABILITY

End items and all deployable subcomponents **shall** be trackable by the Space Surveillance Network (SSN).

Rationale

The ability of the SSN to track end items is a function of its radar reflectivity and optical properties. This allows NASA to monitor the item for potential collision with the ISS or

SSP 51721
Baseline

VVs. Data is acquired using ground-based radars, optical telescopes, and space-based telescopes.

Additional rationale for this requirement can be found in Appendix D.4.14.2.

4.14.2.1 VERIFICATION – TRACKABILITY

Verification is considered successful when review of design determines the end item is trackable by the SSN. (I)

4.14.3 FRAGMENTATION

End items **shall** maintain structural integrity following jettison until atmospheric re-entry. End items that deploy large numbers of sub-components are not considered to be fragmenting.

Rationale

Minimizing unintentional fragmentation decreases the number of items to track and the probability of collision (Pc) with ISS, VVs, and casualty on the ground.

Additional rationale for this requirement can be found in Appendix D.4.14.3.

4.14.3.1 VERIFICATION- FRAGMENTATION

Verification is considered successful when the following are completed:

- A. Structural analysis reflects no potential fragmentation. (A)
- B. Review of design and Inspection of as built hardware conforms to design drawings. (I)

4.14.4 EVA DEPLOY CLEARANCE

End items departing ISS via EVA **shall** have an unobstructed 30 degrees half angle cone around the planned velocity vector.

Rationale

This velocity vector will ensure there is initial clearance of all ISS/VV structures. The object must be under acceptable EVA control which is characterized by the responsible EVA Office.

Additional rationale for this requirement can be found in Appendix D.4.14.4.

4.14.4.1 VERIFICATION- EVA DEPLOY CLEARANCE

Verification is considered successful when the following are completed:

- A. Analysis of the trajectory design reflects the correct velocity vector in the unobstructed cone of a 30° half-angle. (A)
- B. Review of crew procedure documents correct deploy trajectory. (I)

4.14.5 ROBOTIC DEPLOY CLEARANCE

SSP 51721

Baseline

End items departing ISS via robotic deployment mechanism **shall** have a planned velocity vector in the axis of an unobstructed cone of the half angle greater than the worst-case half angle deploy mechanism accuracy.

Rationale

This velocity vector will ensure there is initial clearance of all ISS/VV structures.

Additional rationale for this requirement can be found in Appendix D.4.14.5.

4.14.5.1 VERIFICATION – ROBOTIC DEPLOY CLEARANCE

Verification is considered successful when the following are completed:

- A. Analysis of the trajectory design reflects the correct velocity vector of the unobstructed cone of the half angle greater than the worst-case half angle of accuracy. (A)
- B. Review of crew procedure documents correct deploy trajectory. (I)

4.14.6 CONTROLLABILITY

End items that are capable of modifying or adding energy in their orbit **shall** be two fault tolerant against creating a collision hazard.

Rationale

Examples of capabilities that can modify orbit energy are attitude control systems, propulsion systems, tethers, and deployable subcomponents.

Additional rationale for this requirement can be found in Appendix D.4.14.6.

4.14.6.1 VERIFICATION- CONTROLLABILITY

Verification is considered successful when analysis reflects that the end item does not create a collision hazard for nominal operation, nor creates a collision hazard within 10 days following a failure. (A)

Analysis includes the following:

- A. End items provide an operations and flight plan demonstrating that all systems will ensure that no part of the end item (including sub deployable end items) will enter a +/-2km radial by +/-25km down track by +/-25km cross track rectangular keep out zone centered about the ISS and does not follow a flight path which interferes with nominal ISS operations.
- B. End items demonstrate that within credible system failures as defined by the end item developer and ISRP, that that no part of the end item (including sub deployable end items) will enter a +/-2km radial by +/-25km down track by +/-25km cross track rectangular keep out zone centered about the ISS within 10 days of failure occurrence.

SSP 51721

Baseline

4.14.7 RECONTACT AVOIDANCE

Recontact avoidance for jettison includes requirements for keep-out sphere, range maintenance, V-Bar/R-Bar Crossing, Subcomponent Deploy, Low Orbit Non-ISS Deploy, and Higher Orbit Non-ISS Deploy.

4.14.7.1 KEEP-OUT SPHERE

End items **shall** clear a 200 m radius keep-out sphere (centered on the ISS center of gravity) within 1 orbit, and maintain a positive departing rate while in the keep out sphere.

Rationale

This helps to ensure safe relative motion with the ISS. There must be a velocity component in the $-V_{bar}$ direction from anywhere within the allowed jettison cone.

Additional rationale for this requirement can be found in Appendix D.4.14.7.1.

4.14.7.1.1 VERIFICATION– KEEP-OUT SPHERE

Verification is considered successful when end item relative motion analyses reflect clearance of ISS 200 m keep-out sphere within 1 orbit and end item positive clearance during the entire first orbit. (A)

4.14.7.2 RESERVED

4.14.7.2.1 RESERVED

4.14.7.3 R-BAR CROSSING

End items shall not return to ISS vicinity (i.e., crossing the ISS R-bar from in front of ISS) in the first 30 days after departure from the keep-out sphere unless the end items have phased 360 degrees.

Rationale

Planned ISS reboosts are typically performed within a 30-day interval (on average). Requiring a minimum 30-day return makes it likely that the ISS will perform a planned reboost that would mitigate the return of a low drag end item. When considering a jettison/deploy date for an end item that has the potential to return to ISS vicinity, the actual ISS reboost schedule should be examined to ensure a reboost is expected to be performed at a time which mitigates return risk from that end item.

Additional rationale for this requirement can be found in Appendix D.4.14.7.3.

4.14.7.3.1 VERIFICATION– R-BAR CROSSING

Verification is considered successful when relative motion analyses (assuming no ISS reboost) reflect end item does not return to ISS vicinity in the first 30 days after departure unless the end items have phased 360 degrees. (A)

4.14.7.4 SUBCOMPONENT DEPLOY

If an end item includes a deployable subcomponent, the subcomponent **shall** only be deployed after the following conditions are met:

- The primary end item has achieved a downtrack range of ≥ 500 km.
- The primary end item's Semi-Major Axis (SMA) is less than the ISS SMA.
- The deployment velocity of the end item subcomponent does not result in the subcomponent's SMA, nor the primary end item's SMA, being greater than the ISS SMA.

Rationale

There are three aspects to the requirement to ensure both the primary end item and the subcomponent do not create a collision hazard for the ISS. The first is the end item being a safe distance from the ISS and the second and third being SMA constraints. The primary end item's SMA can be less than the ISS SMA; however, the deploy velocity of the subcomponent could still result in the subcomponent having a SMA greater than the ISS SMA. This analysis is typically completed by NASA Trajectory Operations and Planning Officer (TOPO) group.

4.14.7.4.1 VERIFICATION– SUBCOMPONENT DEPLOY INITIATION

Verification is considered successful when relative motion analyses reflect that:

- A. The end item achieves a downtrack range of ≥ 500 km,
- B. The primary end item's SMA is less than the ISS SMA, and
- C. The deployment velocity of the end item subcomponent does not result in the subcomponent's SMA (positive v -bar subcomponent deploy), nor the primary end item's SMA (negative v -bar subcomponent deploy), being greater than the ISS SMA. (A)

4.14.7.4.2 SUBCOMPONENT REQUIREMENTS

If an end item includes deployable subcomponents, each subcomponent shall also demonstrate that it meets requirements in Sections 4.14.1, 4.14.2, 4.14.3, 4.14.6, 4.14.7.2, 4.14.7.3, 4.14.7.5 and 4.14.7.6.

4.14.7.5 LOWER ORBIT NON-ISS DEPLOY

End items deployed from VVs to an orbit lower than ISS **shall** be deployed from an orbit with a relative apogee at least 15 kilometer below ISS.

Rationale

The altitude buffer prevents conjunction risk with the ISS in the short term before tracking and probability of collision with the candidate(s) can be established. 15 km provides adequate separation for posigrade payload deploy to maintain relative apogee

SSP 51721

Baseline

separation from the ISS considering typical deploy speeds from current deploy mechanisms. This analysis is typically completed by NASA TOPO group.

4.14.7.5.1 VERIFICATION– LOWER ORBIT NON-ISS DEPLOY

Verification is considered successful when relative motion analyses reflect end item pre-deploy (deploying visiting vehicle's orbit parameters) relative apogee is at least 15km below the ISS. (A)

4.14.7.6 HIGHER ORBIT NON-ISS DEPLOY

End items deployed from VVs to an orbit higher than ISS **shall** be deployed from an orbit coelliptic with the ISS with SMA at least 45km above the ISS SMA.

Rationale

At this altitude, natural orbital precession while decaying to the ISS' altitude range creates a sufficient difference between the ISS orbit plane and the jettison candidate's orbit plane for the crossing speed of the candidate with respect to ISS to be at least 200 m/s at the time of closest approach. This velocity allows TOPO to calculate Pc with the ISS and plan/execute an avoidance maneuver if necessary. This requirement assumes a conservatively low jettison candidate BN of 10 kg/m². Candidates with BN less than 10 kg/m² must be jettisoned at a higher coelliptic orbit, to be determined on a case by case basis. This analysis is typically completed by NASA TOPO group. If additional constraints indicate it is not feasible to deploy at an altitude higher than 45 km above ISS, additional analysis can be performed to confirm/deny that the 200 m/s requirement will be met for a given deploy.

4.14.7.6.1 VERIFICATION – HIGHER ORBIT NON-ISS DEPLOY

Verification is considered successful when relative motion analyses reflect end item pre-deploy (deploying visiting vehicle's orbit parameters) relative apogee is at least 15km below the ISS. (A)

4.15 HATCHES

In addition to the other requirements in this document, hatches designed for the ISS have some unique safety considerations. The following requirements were derived from SSP 50005 but are not all inclusive. Additional requirements are outlined in SSP 50005 which are not strictly safety such as strength required for operation, labeling, etc. Other unique requirements, such as the direction of opening, should be considered depending on the application of the hatch.

4.15.1 VISUAL INSPECTION OF ADJACENT VOLUME

Hatches **shall** allow a visual inspection of the adjacent volume.

Rationale

The crew must be able to verify safe conditions prior to opening a hatch and entering the volume. Visual inspection allows for an assessment of hazards such as debris or

SSP 51721
Baseline

unrestrained hardware. Visual inspection can be accomplished via cameras, windows or other means.

4.15.1.1 VERIFICATION – VISUAL INSPECTION OF ADJACENT VOLUME

Verification is considered successful when review of design and as-built hardware shows that the capability for visual inspection is provided. (I)

4.15.2 INDICATION OF PRESSURE AND TEMPERATURE PRIOR TO HATCH OPENING

Indication of pressure and temperature **shall** be provided to the crew prior to opening a hatch.

Rationale

The crew must be able to verify that the pressure and temperature in the adjacent volume are at a safe level.

4.15.2.1 VERIFICATION – INDICATION OF PRESSURE AND TEMPERATURE PRIOR TO HATCH OPENING

Verification is considered successful when review of design and test of the as-built hardware shows that pressure and temperature indications are provided for the volume to be entered. (I and T)

4.15.3 CAPABILITY TO OPERATE FROM BOTH SIDES

Hatches **shall** be capable of being operated from both sides.

Rationale

Hatches must operable from both sides to allow crew rescue in either direction. This includes being able to lock and unlock the hatch, if applicable, and the ability to open or close the hatch from either side.

4.15.3.1 VERIFICATION – CAPABILITY TO OPERATE FROM BOTH SIDES

Verification is considered successful when review of design and as-built hardware, test, or demonstration shows that the capability to operate the hatch from either side is provided. (I, T, D)

4.15.4 PREVENTION OF OPENING PRIOR TO COMPLETE PRESSURE EQUALIZATION

Hatches **shall** be designed to prevent opening prior to complete pressure equalization.

Rationale

Opening a hatch to a volume at a differential pressure could cause damage to the hatch or injury to the crew.

4.15.4.1 VERIFICATION – CAPABILITY TO OPERATE FROM BOTH SIDES

Verification is considered successful when review of design and as-built hardware shows that the capability to prevent opening is provided. (I)

SSP 51721
Baseline

4.15.5 OPERATION BY ONE CREWMEMBER

Hatches **shall** be capable of being operated by one crewmember.

Rationale

A single crewmember must be able to operate a hatch without relying on additional crew.

4.15.5.1 VERIFICATION – OPERATION BY ONE CREWMEMBER

Verification is considered successful when demonstration shows that the capability for the hatch to be operated by one crewmember is provided. (D)

4.15.6 CO-LOCATION OF TOOLS OR DEVICES NECESSARY FOR HATCH OPERATION

Tools or devices necessary for hatch operation **shall** be co-located with the hatch.

Rationale

A hatch must be operable during an emergency situation without having to retrieve tools that are located elsewhere. Any items necessary for hatch operation must be stowed within the hatch or within reach of the hatch.

4.15.6.1 VERIFICATION – CO-LOCATION OF TOOLS OR DEVICES NECESSARY FOR HATCH OPERATION

Verification is considered successful when review of design and as-built hardware shows that any tools necessary for operation are co-located with the hatch. (I)

APPENDIX A - ACRONYMS AND ABBREVIATIONS

A	Analysis
ACD	Adiabatic (or Rapid) Compression Detonation
ACGIH	American Conference of Governmental Industrial Hygienists
AIT	Analysis and Integration Team
ALARA	As Low As Reasonably Achievable
APFR	Articulating Portable Foot Restraint
ARED	Advanced Resistive Exercise Device
ASTM	American Society for Testing and Materials
AWG	American Wire Gauge
BN	Ballistic Number
BRB	Biosafety Review Board
BRC	Battery Risk Classification
BSL	Biosafety Level
C&W	Caution and Warning
CAMMP	Configuration Analysis Modeling & Mass Properties
CBCS	Computer Based Control System
CDC	Centers for Disease Control
CE	Conducted Emissions
CFE	Contractor Furnished Equipment
CID	Circuit Interrupt Device
cm	centimeter
CMRS	Crew Medical Restraint System
CoC	Certificate of Compliance
COTS	Commercial Orbital Transportation Services
CPSC	Consumer Product Safety Commission
CS	Conducted Susceptibility
CSA	Canadian Standards Association
D	Demonstration
DAS	Debris Assessment Software
dB	Decibel (unweighted sound pressure levels)
dBA	Decibel (weighted sound pressure levels)
DC	Direct Current
DFMR	Design for Minimum Risk
DoD	Department of Defense
DPA	Destructive Physical Analysis

SSP 51721**Baseline**

DRM	Design Reference Mission
EC	Electrochemical Capacitor
ECG	Electrocardiogram
ECLSS	Environmental Control and Life Support System
EED	Electronic Engine Display
EEGS	Emergency Egress Guidance System
EIRP	Effective Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EME	Electromagnetic Effects
EMEP	Electromagnetic Effects Panel
EMI	Electromagnetic Interference
EMU	Extravehicular Mobility Unit
EP	Exposed Pallet
EPCE	Electrical Power Consuming Equipment
EPS	Electrical Power System
ESA	European Space Agency
ESD	Electrostatic Discharge
EVA	Extravehicular Activity
EXPRESS	EXpedite the PProcessing of Experiments for Space Station
F	Fahrenheit
FACB	Flight Activities Control Board
FC	Fault Containment
FDIR	Fault Detection, Isolation, and Recovery
FHL	Flammability Hazard Level
FOD	Foreign Object Debris
FORP	Fuel Oxidizer Reaction Products
FOS	Factor(s) of Safety
FP	Floating Potential
ft-lbs	Foot-Pounds
GDRD	Generic Design Requirement Document
GFCI	Ground Fault Circuit Interrupts
GFE	Government Furnished Equipment
GGR&C	Generic Groundrules, Requirements, and Constraints
GSE	Ground Support Equipment
HEPA	High Efficiency Particulate Air
HHP	Human Health and Performance
HMST	Hazardous Materials Summary Table
HR	Hazard Report(s)
HRL	Hazard Response Level

SSP 51721**Baseline**

HTV	H-II Transfer Vehicle
I	Inspection
IBW	Bundled wire
IDD	Interface Definition Document
IEC	International Electrotechnical Commission
IHS	ISS Hazard System
IP&P	International Partners & Program
IPGB	ISS Portable Glove Bag
IR	Infrared Radiation
IRB	Institutional Review Board
IRD	Interface Requirements Document
ISRP	International Space Station Safety Review Panel
ISS	International Space Station
ISSP	International Space Station Program
ISW	Single Wire
IT	Information Technology
ITCS	ISS Thermal Control System
ITU	International Telecommunication Union
IVA	Intravehicular Activity
IVCWG	Internal Volume Configuration Working Group
J	Joules
JAXA	Japan Aerospace Exploration Agency
JSC	Johnson Space Center
km	kilometer
KOZ	Keep Out Zone
kPa	Kilopascal (unit of pressure)
KSC	Kennedy Space Center
KU	K-Band Frequency Sub-Band
KU/LAN	K-Under Local Area Network
LAN	Local Area Network
LBB	Leak Before Burst
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LoC/C	Levels of Containment/Control
LoC	Levels of Containment
LSA	Load Sensitive Area
LSG	Life Science Glovebox
LTL	Low Temperature Loop
m	meter

SSP 51721**Baseline**

M&P	Materials and Processes
mA	milliAmp
MAGIK	Manipulator Analysis, Graphics, and Interactive Kinematics
mAh	milliAmp
MAPTIS	Materials and Processes Technical Information System
MDP	Maximum Design Pressure
ml	Milliliter
MLI	Multi-Layer Insulation
mm	millimeter
MMOD	Micrometeoroid and Orbital Debris
MMR	Multiple Modular Redundancy
MNWF	Must Not Work Function
MOSFET	Metal Oxide Semi-conductor Field Effect Transistor
MPAC	Material Properties as Controls
MPE	Maximum Permissible Exposure
MSFC	Marshall Space Flight Center
MSG	Microgravity Science Glovebox
MTL	Moderate Temperature Loop
MUA	Material Usage Agreement
MWA	Maintenance Work Area
MWF	Must Work Function
MΩ	Megohm
NC	Noise Criterion
NCR	Non-compliance Report
NIR	Non-Ionizing Radiation
Nits	Candela per meter squared or Cd /m ²
NRTM	Near Real Time Monitoring
NSI	NASA Standard Initiator
NSTS	National Space Transportation System
OCA	Oxygen Compatibility Assessment
OCAD	Operational Control Agreement Database
OCV	Open Circuit Voltage
ODPO	Orbital Debris Program Office
OE	Operational Envelope
ORDEM	NASA Orbital Debris Engineering Model
ORSAT	Object Reentry Survival Analysis Tool
ORU	Orbital Replacement Unit
PCB	Printed Circuit Board
PCM	Pressurized Cargo Module
PCU	Plasma Contactor Units

SSP 51721**Baseline**

PHCM	Payload Hazard Control Matrix
PIP	Push in Pull
PNP	Probability of No Penetration
POIC	Payload Operations Integration Center
PPE	Personal Protective Equipment
psia	Pounds per square inch absolute
PTC	Positive Temperatures Coefficients
QD	Quick Disconnect
RE	Radiated Emissions
RF	Radio Frequency
rms	Root Mean Square
RPC	Remote Power Controller
RPCM	Remote Power Control Module
RSC-E	Rocket Space Corporation - Energia
RTM	Real-Time Monitoring
S&A	Safe and Arm
S&M	Structure and Mechanism
SAE	Standard Automotive Engineers
SDP	Safety Data Package
SEE	Single Event Effects
SMA	Semi-Major Axis
SMAC	Spacecraft Maximum Allowable Concentration
SME	Subject Matter Expert
SPF	Specific Pathogen Free
SPL	Sound Pressure Level
SPRT	Subsystem Problem Resolution Team
SRAG	Space Radiation Analysis Group
SSN	Space Surveillance Network
SSRMS	Space Station Remote Manipulator System
T	Test
TBD	To Be Determined
TBR	To Be Resolved
TDRS	Tracking and Data Relay Satellite
TES	Exposed Surface Temperature
THL	Toxicity Hazard Level
TIA	Tailoring/Interpretation Agreement
TID	Total Ionizing Dose
TLV	Threshold Limit Value
TM	Technical Memorandum
TMG	Thermal Micrometeriod Garment
TOPO	Trajectory Operations & Planning Officer

SSP 51721

Baseline

TPM	Permissible Material Temperature
TR	Thermal Runaway
TTE	Time To Effect
UHR	Unique Hazard Report
UL	Underwriters Laboratories
USB	Universal Serial Bus
USOS	United States On-orbit Segment
USSTRATCOM	United States Strategic Command
V	Volts
Vdc	Volts (direct current)
VIPER	Vehicle Integrated Performance Environments and Resources
VV	Visiting Vehicle
Wh	Watt-hours

APPENDIX B - GLOSSARY

ACTIVELY SAFED SYSTEMS

Only hazardous when system exceeds pre-defined limits.

ADIABATIC/RAPID COMPRESSION DETONATION (ACD)

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

AMBULATORY

A crewmember/patient is considered ambulatory if they are not restrained in any location during nominal or emergency operations (e.g., a patient restrained on the CMRS) and are free to move about the ISS IVA volume.

APPLIED PART

Part of the medical equipment which is designed to come into physical contact with the patient or parts that are likely to be brought into contact with the patient.

BIOHAZARD

Biological materials or agents that may be infectious to the crew or other organisms resulting in disease and/or to the environment resulting in environmental contamination.

CATASTROPHIC HAZARD

Any condition which may cause a disabling or fatal personnel injury or illness, or one of the following: loss of ISS, loss of a crew-carrying vehicle, or loss of a major ground facility.

COMMON CAUSE FAILURE

Failure of multiple items or systems due to a single event or common failure mode.

COMPOSITE OVERWRAPPED PRESSURE VESSEL (COPV)

A pressure vessel with a composite structure fully or partially encapsulating a metallic or plastic liner. The liner serves as a fluid (gas or liquid) permeation barrier and may or may not carry substantive pressure loads. The composite structure generally carries pressure and environmental loads.

CONTROL

Design or operational features that provide a verifiable method of preventing the hazardous event from occurring (e.g., a switch that interrupts the power to a hazardous function).

CREDIBLE

A condition that is reasonably likely to occur.

CRITICAL HAZARD

Any condition which may cause a non-disabling personnel injury or illness, loss of a major ISS end item, loss of redundancy (i.e., with only a single hazard control

SSP 51721

Baseline

remaining) for on-orbit life sustaining function, or loss of use of systems needed for essential logistics (e.g., the SSRMS).

CRITICAL SERVICES

ISS or transport vehicle services required to assist in the control of hazards.

DESIGN FOR MINIMUM RISK (DFMR)

An alternate approach to failure tolerance using the safety-related properties and characteristics of the design to reduce the associated risk to an acceptable level.

ELECTROMAGNETIC INTERFERENCE (EMI)

Any conducted or radiated electromagnetic energy that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronic or electrical equipment.

ELEMENT

End items transported, transferred, stowed, operated on and/or removed from the ISS.

END ITEM

A final combination of end products, component parts, and/or materials that is ready for its intended use. (e.g., modules, visiting vehicles, scientific equipment, experiments, payloads, logistics, crew psychological support items, tools, spares, instruments and assemblies, including waste)

FACTOR OF SAFETY

The structural capacity of a system beyond the expected loads or actual loads.

FAIL SAFE

The ability to sustain a failure and retain the capability to safely terminate or control the operation. This terminology is used with the design of structure, pressure systems, and fasteners to ensure that after failure of any single structural component, the remaining structural components can withstand the resulting redistributed loads without failure. A fail safe approach can also be implemented with computer systems, but this typically results in end item inoperability after the first failure.

FAILURE

The inability of a system, subsystem component or part to perform its required function within specified limits.

FAILURE TOLERANCE

The ability to sustain a certain number of failures and still retain capability. Single failure tolerance would require a minimum of two failures for the hazard to occur. Two-failure tolerance would require a minimum of three failures for a hazard to occur. Fault tolerance is a subset of failure tolerance.

HAZARD

A state or a set of conditions, internal or external to a system, that poses a threat to life, health, vehicle, or environment. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent

SSP 51721

Baseline

characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

HAZARDOUS COMMAND

A command that can create an unsafe or hazardous condition which potentially endangers the crew or ISS. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard.

HAZARDOUS FUNCTIONS

Operational events whose inadvertent operations or loss may result in a hazard.

HAZARDOUS MATERIALS

Any item, substance, or agent (physical, chemical, biological, and/or radiological), which has the potential to cause harm to the crew, the ISS environment, or equipment either by itself or through interaction with other factors.

IGNITION SOURCE

A source of heat sufficiently intense and localized to induce combustion.

INDEPENDENT INHIBIT

Inhibits are independent if no single credible failure, event or environment removes more than one.

INHIBIT

- A. Hardware implementation: A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.).
- B. Software implementation: A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available.

INTRAVEHICULAR ACTIVITY (IVA) OPERATIONAL ENVELOPE (OE)

The boundary at which potentially hazardous IVA operations will cease if a crewmember approaches the boundary (e.g., a crewmember approaches another crewmember that is operating the ARED (Advanced Resistive Exercise Device), reduced LoC operations).

INTERLOCK

A design feature that ensures that any conditions prerequisite for a given function or event are met before the function or event can proceed.

KEEP OUT ZONE (KOZ)

A warning category that defines a volume in which a hazardous condition may be present and which poses a risk to crew. A KOZ should be used for hazards which exist in the 3 dimensional space away from the surface of hardware, such as radiation, plumes, or mechanical motion.

SSP 51721

Baseline

KU/LAN

Ku-band access for Local Area Network (LAN) - KU/LAN - The Ku band is the portion of the electromagnetic spectrum in the microwave range of frequencies from 12 to 18 gigahertz (GHz).

LEVELS OF CONTAINMENT (LOC)

The failure tolerant design approach applied to contain hazardous materials that requires concentric independent layers (physical barriers) in the end item design where each individual layer is of a design integrity able to contain the hazardous material. The required number of independent levels of physical barriers is based on the hazard severity.

LOAD SENSITIVE AREA (LSA)

A warning category that defines an area, which is non-compliant with 125 lb EVA Kickloads but can withstand a 45 lb handling load. LSAs allow the crew to apply a handling load of up to 45 lbs to the hardware in question. However, the hardware must still have positive margins of safety and use appropriate factors of safety for the 45 lb limit. The crew is trained to abide by a 45 lb handling limit. If an item cannot take the 45 lb handling load, it would be a NTA. These warning categories do not preclude the need for NCRs for exceptions.

MARGINAL HAZARD

Any condition which may cause damage to an ISS end item (the loss of which then itself does not constitute a critical or catastrophic hazard) and/or an injury that does not require medical intervention from a second crewmember nor consultation with a Flight Surgeon (including those injuries that might result in minor crew discomfort).

MARGIN OF SAFETY

Deviation of the actual (operating) factor of safety from the specified factor of safety. Can be expressed as a magnitude or percentage relative to the specified factor of safety.

MATERIAL PROPERTIES AS CONTROLS (MPAC)

Alternative to a physical barrier in containing hazardous materials that utilizes the physical properties of a particular hazardous material or the interaction of the hazardous material with other materials such as adhesive properties with surface tension.

MAXIMUM DESIGN PRESSURE

Pressure of a system under worst-case conditions as a result of two worst-case failures.

MODIFIED END ITEMS

End items of a similar design and operation of other previously-flown end items, but with modifications.

MONITOR

Safety status of end item functions, devices, inhibits, or parameters.

SSP 51721

Baseline

MUST-NOT-WORK-FUNCTION

A function, if performed inadvertently or at an inopportune time, results in a hazard.

MUST-WORK-FUNCTION

A redundant function, if not performed, can result in a catastrophic hazard if the function is not performed.

NEAR REAL TIME MONITORING (NRTM)

Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit).

NON-COMPLIANCE REPORT (NCR)

A report documenting a condition in which a requirement cannot be met.

NO TOUCH AREA (NTA)

A warning category that defines an area on which a hazardous condition may be present and which poses a risk to crew. A NTA should be used for hazards which exist on a surface, such as sharp edges, temperature extremes, pinch points, entrapment, crew loads, etc. NTAs can be applied to large areas in which multiple non-compliant areas exist in close proximity to one another.

OFFGASSING

The release of chemicals from materials into habitable areas.

OPERATOR ERROR

Any inadvertent action by either flight and/or ground crew that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features which control a hazard.

OUTGASSING

The release of chemicals from materials into the external (vacuum) environment leading to contamination of surfaces and/or degradation of materials.

OPERATIONAL CONTROL

The control of a hazard by the real-time activities of the on-orbit crew, issuance of a ground command or the implementation of a preplanned decision by the Flight Control Team.

OPERATIONAL MITIGATION

Operational activity or response that helps reduce the probability of realizing the hazardous event consequence but has limitations or uncertainties that do not constitute a full level of control of the hazard (e.g., cleanup following release of a hazardous substance).

PAYLOAD

A scientific or technology experiment that is flown to the ISS to be operated/conducted in the ISS microgravity environment. Payloads may be installed or deployed in the ISS internal pressurized volume, or attached external to the ISS pressurized volume.

SSP 51721

Baseline

PHYSICAL AGENTS

Materials or substances that, alone, are considered non-hazardous but become hazardous when released in large mass or concentrations due to how they act and respond in microgravity.

PREREQUISITE MONITORING

Monitoring required to confirm inhibits and controls are in place before a hazardous procedure is implemented. Prerequisite monitoring is defined as monitoring required to confirm inhibits and controls are in place before a hazardous procedure is implemented. Prerequisite monitoring is used for situations that are only hazardous for a short time in comparison to the duration of an ISS mission (e.g., prior to connector mate/demate). When prerequisite monitoring is used, once the inhibit is established and confirmed, it does not need to be continuously monitored since the inhibit is considered to be in a safe state. Prerequisite monitoring may also be used for most work systems that do not have a catastrophic hazard potential.

PRESSURE VESSEL

A container designed primarily for pressurized storage of gases or liquids and:

- A. Contains stored energy of 14,240 foot-pounds (19,307 joules) or greater based on adiabatic expansion of a perfect gas.

or

- B. Stores a gas that will experience an MDP greater 100 psia (690 kPa); or
- C. Contains a gas or liquid in excess of 15 psia (103.4 kPa) which will create a hazard if released.
- C. Contains a gas or liquid in excess of 15 psia (103.4 kPa) which will create a hazard if released.

REAL TIME MONITORING (RTM)

Immediate notification of changes in inhibit or safety status to the crew.

REDUNDANCY

Use of more than one means to accomplish a given function.

REFLIGHT END ITEM

End items that have previously flown (using the same part number and serial number) on a transportation vehicle or ISS, are unmodified, and are being re-manifested for flight.

RISK (SAFETY)

The potential for injury or loss. Risk is a function of the frequency of occurrence of an undesirable event, the potential severity of the resulting consequences, and the uncertainties associated with the frequency and severity.

SSP 51721

Baseline

SAFE

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

SAFE DESIGN LIFE

Period of time in which cargo can be retained at or restored to the specified operational condition via prescribed resources and procedures. Design life must include ground and on-orbit time, including passive stowage.

SAFE OPERATIONAL LIFE

Period of time in which cargo will fulfill its intended function within specified performance limits under stated conditions without any corrective maintenance, recalibration, or repair. Safe operating life should include both ground and on-orbit life.

SAFED

A configuration that will not cause a hazard.

SAFETY ANALYSIS

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

SAFETY CRITICAL

A condition, event, operation, process, function or feature with potential to create a critical or catastrophic hazard. A safety critical feature of a design is a feature whose failure or malfunction has the potential to create a critical or catastrophic hazard. This terminology is most often used with structures, circuits, fasteners, software, and mechanisms. An end item with a safety critical feature does not classify the entire end item as safety critical.

SAFING

Event or sequence of events necessary to place systems, subsystems or component parts into predetermined safe conditions.

SEALED CONTAINER

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

SERIES END ITEM

End items of the same design and operation as previously flown. Series items must be built to the same drawings, have the same part number, and use the same processes as the initial end item.

SMART SHORT

An electrical short that subjects wiring to currents at the highest value the source can provide without activating circuit protection devices. Sustained smart short currents are maximum current allowed for > 1 second by the upstream circuit protection device.

Safety critical circuits are:

SSP 51721

Baseline

- Circuits whose loss of function could result in a critical or catastrophic hazard or,
- Circuits whose malfunction or degradation of performance could result in a critical or catastrophic hazard or,
- Circuits that control inhibits whose loss could result in critical or catastrophic hazards.
- Circuits that are inhibited or not operational to prevent operation a critical or catastrophic hazard.
- No single failure can remove more than one inhibit or control to a critical or catastrophic hazard.
- Circuits that are insusceptable to EMI.

STRUCTURE

All components and assemblies designed to sustain loads or pressures, provide stiffness and stability, or provide support or containment.

TIME-TO-EFFECT

Time interval between loss of a control(s) and occurrence of the hazard. TTE of the hazard is the time between the loss of an inhibit and occurrence of the hazard.

TORTUOUS PATH

A path that is convoluted, indirect, involved, difficult to follow, and/or circuitous. Used as mitigation to the escape of hazardous fluids.

TOUCH/LEAKAGE CURRENTS

Unintentional currents to which a crewmember can be exposed.

TOXICITY HAZARDS

Chemicals that may be harmful to the crew (including physiological effects such as irritation to skin or eyes).

VERIFICATION

Proof of compliance with requirements. May be determined by test, analysis, demonstration, and/or inspection.

APPENDIX C - OPEN WORK

Table C-1 lists the specific To Be Determined (TBD) items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBD item is numbered based on the section where the first occurrence of the item is located as the first digit and a consecutive number as the second digit (i.e., <TBD 4-1> is the first undetermined item assigned in Section 4 of the document). As each TBD is solved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBDs will not be renumbered.

TABLE C-1 TO BE DETERMINED ITEMS

TBD	Section	Description

Table C-2 lists the specific To Be Resolved (TBR) issues in the document that are not yet known. The TBR is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBR issue is numbered based on the section where the first occurrence of the issue is located as the first digit and a consecutive number as the second digit (i.e., <TBR 4-1> is the first unresolved issue assigned in Section 4 of the document). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBRs will not be renumbered.

TABLE C-2 TO BE RESOLVED ISSUES

TBR	Section	Description
TBR-3-1	3.14	Updates required to SSP 30599, "Safety Review Process" as related to safety Non-Compliance Reports (NCRs).
TBR 4-2	Table 4.2.3-1	Engineering Review Board (ERB) to resolve Low Energy Fail Safe Pressure Systems definition/criteria.
TBR 4-3	Table 4.2.3-1, 4.2.3.1, 4.2.3.1.1, 4.2.3.2	Recommendation from engineering to remove Table 4.2.3-1, 4.2.3.1, 4.2.3.1.1, and 4.2.3.2. The pointers to engineering structures documents in 4.2.3.2.1 (payloads) and 4.2.3.2.2 (systems) capture all the information in the before mention table and sections.
TBR 4-4 TBR D-4	4.2.3.1 D.4.2.3.1	Engineering to determine how to document sealed containers with an MDP ranging from 45 to 100 psi. Currently, this range (45 to 100 psi) undefined. Historically, the ISS Safety Review Panel (ISRP) has considered MDP from 22 psi to 100 psi a sealed container assuming that all other criteria of a sealed container has been met.

**SSP 51721
Baseline**

TBR	Section	Description
TBR D-5	D.4.2.3.2	Factory of Safety (FOS) for Secondary Compartments/Volumes. Discrepancy in engineering documents. SSP 52005 Rev G does not identify FOS for Secondary Compartments. SSP 30558 and SSP 30559 identify FOS > 2.5 MDP for Secondary Compartments. Historically for payloads, secondary compartments were verified with a FOS > 1.5 MDP per SSP 51700. EA to resolve at Engineering Review Board.
TBR 4-6	4.3.1	Forward work is necessary to clarify rational related to EPS requirements for items not powered while on ISS.
TBR 4-7	4.3.2.1	May see updates to NASA-STD-3001 that can impact the current requirements. 32V rms may be replaced with unique AC and DC current limits (rather than voltage limits) to define threshold for catastrophic hazards.
TBR 4-8	4.3.6.2	JSC/EP capacitor testing needed to determine a safe energy level for electrochemical capacitors.
TBR 4-9	4.4.2.2	Hazardous commanding for additional systems, including Ka (frequency) and laser communication, will be addressed at a later time
TBR 4-10	Table 4.7.2-1	The difference in the safety requirements for designing end items with hazardous materials (LoC/C) and on-orbit hazardous response (HRL) is under review. On-orbit hazardous release is documented in Flight Rule B20-17. This is specific to hazardous materials that fall into the FHL 1-3 hazard ratings.
TBR-11 TBR D-11	4.9.2.1 4.9.2.2 D.4.9.2.1	The Flight Docs have an action to address/define the crew impacts from hot and cold touch temperatures. The ISRP is working with them to define the values/limitations for hot and cold touch temperatures as related to hazard severity.
TBR-12	4.9.4	The ISSP is assessing the potential hazards from or as a result of end item hardware, including vehicles and vehicle systems (i.e. VVs or the EMU) exposure to high-intensity laser emissions. Resolution will specifically define/address potential hazards to internal and external hardware as well as free flying visiting vehicles and provide information on how it is expected to be regulated/controlled.

APPENDIX D - RATIONALE

Appendix D is a continuation of requirement rationales from Section 4.

D.4.1.2 Rationale – Environmental Compatibility

The safety assessment must take into consideration the worst-case environment in which the end item is intended to reside and operate, inclusive of launch and return/disposal. An end item is considered safe when it does not create a hazard and when the identified hazard controls are verified to function in the worst-case natural and induced environments.

Worst-case environments consist of all the environments that the end item will be exposed to, including handling, exposure durations, appropriate combinations of thermal, vibration, pressure (including module depressurization), mechanical, cycle life, and others as appropriate. As an example, a pressure system Maximum Design Pressure (MDP) must be determined using the worst-case temperature. End items intending to be used in the United States On-orbit Segment (USOS) airlock during Extravehicular Activity (EVA) preparations would need to consider the worst-case oxygen environment per Section 4.7.1.1. Environments are defined in SSP 41000, SSP 57000, SSP 57003, and SSP 50835. Transport vehicle requirements from Section 3.5 must also be considered in determining the worst-case environment. Hazard controls, especially those of an electrical or electronic nature could be rendered inoperable when exposed to the natural and induced environments of ISS or visiting vehicles. In some cases, the suitability of those controls may require a test or demonstration above and beyond an analysis to show compatibility of the end item hazard controls with the environment. In these cases, the end item developer must inspect (and may be required to provide to the ISRP) these additional verification submittals, such as test and demonstration reports, to confirm the hazard is controlled throughout the life of the end item.

D.4.2.2.3 Rationale – Mechanisms Lubrication

Lubrication is one of the most important factors in successful mechanism design and operation. All contacting surfaces that are expected to move with respect to one another need to be lubricated in some way, regardless of material choices, load, or life requirements. Use of dissimilar metallic materials for the wear surfaces, though strongly encouraged, is not an equivalent to or substitute for lubrication and does not meet the intent of this requirement. A successfully complete life test per Section 4.2.1.15.1 also contributes to verification of this requirement.

The quantity of lubricant used and method of application can be almost as important as the presence of lubricant. Too much can impede mechanism performance or create contamination problems, and too little can result in reduced life or inadequate performance.

SSP 51721

Baseline

Lubricants must be compatible with interfacing materials, other lubricant used in the design and the natural and induced environment, including the EVA environment if applicable.

ISS Structures and Mechanism and Materials and Processes (M&P) personnel can provide a list of acceptable lubricants.

NOTE: A successfully complete life test per Section 4.2.2.15.1 also contributes to verification of this requirement.

D.4.2.2.4 Rationale – Mechanisms Springs

Springs are a common mechanism component as well as a common source of problems. Spring failure tolerance provides for increased mechanism reliability. Determining that a spring failure is not credible requires demonstrating that adequate life and stress margins exist on the part (similar to determining DFMR classification). This can be accomplished with a combination of stress analysis, fatigue analysis, fracture control methods, and testing. However, given the size of many springs used in mechanisms, fracture approaches are often not feasible and other steps have to be taken to demonstrate reliability. The strategy for any given spring must be developed with the ISS Structure & Mechanism (S&M) and M&P teams. “In rare cases, spring failures can be declared non-credible by showing compliance with a comprehensive set of structural, life and fracture control requirements, in which case this requirement is not applicable.”

D.4.2.2.6 Rationale – Mechanism Mechanical Stops

The impact against the mechanical stop can create elevated loads on other parts of the mechanism in addition to the stops themselves, and these loads have to be accounted for in the structural analysis. The contact of mechanical stops is often rapid enough that static analysis approaches can lack sufficient conservatism so a dynamic analysis is necessary. A bounding worst-case load would include impact at maximum speed combined with stall torque. Both the mechanism and the hard stop margins must be evaluated. Both the mechanism and the hard stop margins must be evaluated. This requirement applies to all types of mechanical stops including emergency stops, though in failure cases it may be appropriate to utilize less conservative applied loads consistent with existing program structural requirements.

D.4.2.2.8 Rationale – Mechanism Positive Indication of Status

The ability to verify that the mechanism is functioning in the proper state is critical to identifying and controlling failures. Without knowledge of status, a hazardous, failed condition may unknowingly exist. State indication can be accomplished in different ways including electrically or visually.

Indication redundancy may be required to meet higher-level failure tolerance requirements. Operational controls and/or training may be required to ensure inspection of on-orbit indicators.

SSP 51721
Baseline

D.4.2.2.9 Rationale – Mechanism Starting Torque /Force Margins

Torque and force margins are intended to ensure that the mechanism retains reserve torque or force capability that can be applied in the event of an unforeseen effect that reduces motive force from the mechanism. Therefore, as with any other capability of the mechanism, the minimum torque or force margin must be verified as intact prior to placement into service.

Starting torque margin is defined as:

Starting Torque Margin = (Available Driving Torque/Resisting Torque) – 1

For linear devices, “Force” replaces “Torque” in the above equation.

Worst-case environmental conditions include:

- *Frictional effects*
- *Possible changes in static and dynamic friction due to storage time*
- *Alignment effects*
- *Wire harness loads*
- *Damper drag*
- *Thermally induced distortions*
- *Load-induced distortions*
- *Variations in lubricity*
- *Fluid pressure on the elastomers in viscous dampers*
- *Supply voltage, motor, and controller parameters*
- *Acceleration due to vehicle motion or maneuvers that can hinder motion*
- *Loading due to vibroacoustic environment*

In practice, it can be difficult to test/verify the margin directly in accounting for worst-case parameters affects and inability to measure specific values. This often drives some portion of the verification to depend on analysis to derive the margin of safety. In these cases, the margin must be calculated by using the worst stack-ups of tested factors and adjusting for factors not present in the test. Operational controls and/or training may be required to ensure inspection of on-orbit indicators.

D.4.2.2.10 Rationale – Mechanism Dynamic Torque/Force Margins

Torque and force margins are intended to ensure that the mechanism retains reserve torque or force that can be applied in the event of an unforeseen effect that reduces mechanism dynamic motive force. Therefore, as with any other capability of the mechanism, the minimum torque or force margin must be verified as intact prior to placement into service.

Dynamic torque margin is defined as:

SSP 51721

Baseline

Dynamic Torque Margin = (Available Driving Torque-total resisting torque) / Torque Required for acceleration) – 1

For linear devices, “Force” replaces “Torque” in the above equation. Worst-case environmental conditions include:

Frictional effects

- Possible changes in static and dynamic friction due to storage time
- Alignment effects
- Wire harness loads
- Damper drag
- Thermally induced distortions
- Load-induced distortions
- Variations in lubricity
- Fluid pressure on the elastomers in viscous dampers
- Supply voltage, motor, and controller parameters
- Acceleration due to vehicle motion or maneuvers that can hinder motion
- Loading due to vibroacoustic environment

In practice, it can be difficult to test the margin directly in accounting for worst-case parameters and the inability to measure specific values. This often drives some portion of the verification to depend on analysis to derive the margin of safety. In these cases, the margin must be calculated by using the worst stack-ups of tested factors and adjusting for factors not present in the test.

D.4.2.2.11 Rationale – Mechanism Holding Force Margins

Torque and force margins ensure that the mechanism retains reserve torque or force capability that can be applied in the event of an unforeseen effect that reduces holding force from the mechanism. Therefore, as with any other capability of the mechanism, the minimum torque or force margin must be verified as intact prior to placement into service.

Dynamic torque margin is defined as:

Dynamic Torque Margin = ((Available Driving Torque-total resisting torque) / Torque Required for acceleration) – 1

For linear devices, “Force” replaces “Torque” in the above equation.

Worst-case environmental conditions include:

Frictional effects

- *Possible changes in static and dynamic friction due to storage time*

SSP 51721

Baseline

- *Alignment effects*
- *Wire harness loads*
- *Damper drag*
- *Thermally induced distortions*
- *Load-induced distortions*
- *Variations in lubricity*
- *Fluid pressure on the elastomers in viscous dampers*
- *Supply voltage, motor, and controller parameters*
- *Acceleration due to vehicle motion or maneuvers that can hinder motion*
- *Loading due to vibroacoustic environment*

In practice, it can be difficult to test the margin directly in accounting for worst-case parameters and the inability to measure specific values. This often drives some portion of the verification to depend on analysis to derive the margin of safety. In these cases, the margin must be calculated by using the worst stack-ups of tested factors and adjusting for factors not present in the test.

D.4.2.2.13 Rationale – Mechanism Function

End items with safety critical mechanism must ensure that mechanical function works as intended and does not impact ISS. Acceptance testing must incorporate run-in, functional, and environmental testing at worst-case environments. The run-in test conditions must be representative of the operational loads, speed, and environment. Inspection and functional tests must be performed before and after environmental testing. This testing will ensure there are no workmanship defects.

Qualification testing must include all worst-case environments and all mechanism configurations. Inspection and functional tests must be performed before and after qualification testing. The testing must be conducted with mounting interface boundary conditions that replicate the flight boundary conditions, including stiffness, mounting alignment and tolerances, thermal distortions and load-induced distortions. Qualification units must utilize flight-like electronics.

D.4.2.2.14 Rationale – Mechanism Life

All functions of the mechanism have to be life tested to verify life of the system, including back-up or redundant provisions; however, the appropriate number of cycles to be applied to the back-up or redundant provisions should be consistent with the possible failure scenario. Typical design life concerns include fatigue limits, deterioration of lubrication, excessive wear, and deterioration during extended quiescent periods. It is highly recommended that spare cycles be added to the total cycles required to allow troubleshooting or execution of extra cycles without exceeding the mechanism's certified life.

SSP 51721
Baseline

The service life in Table 4.2.2.14-1 includes operational cycles plus the total of all ground cycles (including test cycles, installation cycles, and maintenance cycles).

Life verification testing must include a number of cycles at the expected operating environmental extremes, loads, and speeds that are representative of the number of cycles at those conditions expected in the service life of the mechanism. Other life test considerations include ensuring representative bearing contact stresses and assessing hard stop contacts. Performance measurements must be taken on the first and last cycles of the test. However, the appropriate number of cycles to be applied to the back-up or redundant provisions should be consistent with the possible failure scenarios.

D.4.2.2.15 Rationale – Mechanism Load Redistribution

Whether a particular failure is considered credible will be determined by the ISRP, with input from the appropriate subject matter expert. This minimizes the number of structural configurations to be analyzed. Full factors of safety apply to these failure conditions, though it may be appropriate to utilize less conservative applied loads consistent with existing program structural requirements.

D.4.2.3 Rationale – Pressure Systems

A pressure vessel is a container designed primarily to sustain internal pressure, but which can also sustain some vehicle-induced loads. More specifically, a container that stores pressurized fluids or gases and: (1) Contains stored energy of >14,240 ft-lbs (19,310 J) based on adiabatic expansion of a perfect gas; or (2) Contains a gas or liquid in excess of 15 psia which will create a hazard if released. Verification is based on the type of pressure vessel used.

Stored energy can be calculated using the Baker Equation which can be found in NASA-HDBK-5010, Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware, Appendix G or online. It is necessary for End items containing hazardous materials to provide appropriate levels of containment per Section 4.7.2. Structural and fracture control requirements are applicable for high pressure systems per Section 4.2. Maintaining system integrity during exposure to all applicable environments and for the entire service life of the pressure vessel.

D.4.2.3.1 Rationale – Pressure Systems – Sealed Container

A sealed container consists of only one pressurized compartment or vessel and has

- *MDP is ≤ 100 psia and > 22 psia <TBR D-4>*
- *Containing non-hazardous materials and*
- *Stored energy $\leq 14,240$ ft-lbs*

When sealed container has an MDP ≤ 22 psia, no additional testing or analysis is required. When the MDP is greater than 100 psia, it is considered a pressure component and high pressure system safety requirements are applicable. End items that are comprised of more than one pressurized component are considered a pressure

SSP 51721
Baseline

system. In order to determine if an end item qualifies as a low energy pressure system, apply the following criteria to pressurized lines, fittings and components.

- Bottle or pressure vessels built to commercial Department of Transportation (DOT) standards,
- Having < 100 psia internal pressure,
- Contents of the pressure system are non-hazardous, and
- Contains less than 1,000 foot-pounds of energy

This approach is consistent with Department of Energy PNNL-18696, Pressure Systems Stored-Energy Threshold Risk Analysis. <TBR D-4>

D.4.2.3.2 Rationale – Pressure Systems – Pressure Vessel Maximum Design Pressure (MDP) <TBR D-5>

Maximum Design Pressure (MDP)

MDP is the pressure of the system under worst-case conditions as a result of two worst-case failures. MDP derivations are necessary to understand the capabilities of the pressure systems to preclude rupture hazards. MDP takes into account maximum relief pressure, maximum regulator pressure, maximum temperature, and transient pressures. Two fault tolerance collectively in pressure regulators, relief devices, and/or a thermal control system (e.g., heaters) can be used to control pressure collectively to causing the pressure to exceed the MDP.

The FOS is a constant which has been defined for proof and ultimate pressure design criteria. Design FOS apply to MDP as shown in Table D.4.2.3.3-1. FOS has a historical basis and is necessary to ensure DFMR by not allowing failures due to uncertainties which result from the design process, manufacturing process, and the loading environment.

Ultimate Strength and Proof Pressure

Ultimate strength is the maximum pressure that a structure will withstand without incurring rupture, detrimental deformation, or collapse. The proof pressure gives evidence of satisfactory workmanship and material quality and/or establishes maximum initial flaw sizes for safe-life demonstration. Analysis of mechanical service life proof pressure factor is necessary when proof pressure is greater than the minimum factor.

Pressurized Lines, Fittings, and Components

Smaller pressurized lines, fittings and components of a pressure system generally have higher FOS because of the manufacturing limitations of making lines, fittings and components thinner than nominal thicknesses of materials.

TABLE D.4.2.3.3-1 MINIMUM FOS FOR PRESSURE SYSTEMS

	Proof Pressure	Ultimate
1. Design factors for windows, glass, and ceramic structure are defined in SSP 30560, Glass, Window and Ceramic Structural Design and Verification Requirements.	= 2.00 x MDP	= 3.00 x MDP
2. Hydraulic and Pneumatic Systems		
a. Lines and Fittings less than 1.5 inches (38 mm) dia. (OD)	= 1.50 x MDP	= 4.00 x MDP
b. Lines and fittings, 1.5 inches (38 mm) dia. or greater	= 1.50 x MDP	= 2.00 x MDP
c. Reservoirs/Pressure Vessels	= 1.50 x MDP	= 2.00 x MDP
d. Actuating cylinders, valves, filters, switches, line-installed alignment bellows and heat pipes	= 1.50 x MDP	= 2.50 x MDP
e. Flex hoses, all diameters	= 2.00 x MDP	= 4.00 x MDP

Notes:

- [1] Reference SSP 52005, Payload Flight Equipment Requirements and Guidelines for Safety-Critical Structures when pressure loads have a relieving or stabilizing effect on structural capability.
- [2] In a system with fluid lines and flex hoses, the individual flex hoses to be proof pressure tested to 2.00 X MDP individually if the assembly level is proof tested to 1.5 X MDP.
- [3] This table is based on SSP 30559 and Appendix B of SSP 30558, Fracture Control Requirements for Space Station

Pressure Vessel Leak Before Burst (LBB)

LBB describes a pressure vessel designed such that a crack in the vessel will grow through the wall, allowing the contained fluid to escape and reducing the pressure, prior to growing so large as to cause fracture at the operating pressure. SSP 52005, SSP 30558, and SSP 30559 describe verification activities that include flight unit testing proof pressure test (Proof = FOS x MDP), Inspection post-proof pressure test for induced leaks and/or detrimental deformation, Non-Destructive Evaluation (NDE) inspection of welds, LBB fracture mechanics analysis for tank wall stability (crack of length ten times the wall thickness at MDP. NASA-STD-5019, Fracture Control Requirements for Spaceflight Hardware also provides guidance related to LBB verification activities.

Metallic Pressure Vessels

SSP 52005 and SSP 30558, describe verification activities that include a fatigue analysis showing a minimum of 10 design lifetimes that may be used in lieu of testing a certification vessel to qualify a vessel design. ANSI/AIAA S-080, Space Systems – Metallic Pressure Vessels, Pressurized Structures, and Pressure Components can also be used as requirements references.

Composite Pressure Vessels

SSP 52005, SSP 30558, and SSP 30559 describe verification activities that include compliance with ANSI/AIAA S 081, Space Systems – Composite Overwrapped Pressure Vessels (COPVs), damage control plan assessment, and stress rupture life assessment.

Dewars and Cryostats

SSP 52005, SSP 30558, and SSP 30559 describe verification activities that include fracture mechanics safe life assessment for containers of hazardous fluids and all non-LBB designs, MDP analyses and testing, design review of outer shells (e.g., vacuum jackets) pressure relief full flow capability and redundancy, thermal expansion analyses

SSP 51721

Baseline

of cryogenic systems thermal expansion and contraction loads, automatic relief capability incorporated between valves in the system where cryogen can be trapped and converted to gaseous state, and material compatibility to show cryogenic systems are insulated with an oxygen compatible material or vacuum-jacketed to preclude liquefaction of air.

Pressure Stabilized Vessels

Pressure-stabilized vessels contain a minimum pressure to ensure structural integrity under launch and landing loads. Additional verifications may be required to test for the existence of the minimum required pressure prior to the application of loads into the system and/or test the 1FT pressure decay monitoring to ensure minimum design FOS exists at the time of subsequent structural load application.

Pressure Systems with Hazardous Fluids

Pressure system components are considered fracture critical if they contain hazardous fluids or if loss of pressurization would result in a catastrophic hazard. Hazardous materials are defined in Section 4.7.2.

Flow Induced Vibrations

Flow induced vibrations are structural and mechanical oscillations of structures immersed in or conveying fluid flow as a result of an interaction between the fluid-dynamic forces and the inertia, damping, and elastic forces in the structures. Evaluations of these vibrations is necessary when fluids are flowing through flexible hoses and bellows. Verification activity in SSP 52005, SSP 30558, and SSP 30559 include inspection of designed in accordance with MSFC-DWG-20M02540, Assessment of Flexible Bellows and 32L2 Flexible Hose, testing per MSFC-SPEC-626, Test Control, and certification in accordance with NSTS-08123, Certification of Flex Hoses and Bellows for Flow Induced Vibration.

Secondary Compartments/Volumes

It is necessary to assure secondary compartment/volumes integral/attached to pressure system components be designed consistent with structural requirements when pressurized as a result of a credible single barrier failure. For systems, SSP 30558 and SSP 30559 verification activities include design review that shows FOS >2.5 MDP, qualification testing to certify hardware for operating environments (including fatigue conditions), and/or venting/relief provisions when external leakage does not present a catastrophic hazard. For payloads, SSP 51700 verification activities include design review that shows FOS >1.5 MDP <TBR D-5>, qualification testing to certify hardware for operating environments (including fatigue conditions), and/or venting/relief provisions when external leakage does not present a catastrophic hazard.

Redundant Seals

It is necessary to assure redundant seals in series are independently qualified. If individual seals are used with single-barrier DFMR containers, their number should be consistent with the hazard level. Single, high quality, leak tested metallurgical welds are

SSP 51721

Baseline

acceptable barriers in DFMR designs. In general, single non-metallic adhesive or heat/chemical-fuse joints are not acceptable in DFMR designs.

Single Barrier Failures

Failures of structural parts such as pressure lines and tanks, properly designed and tested, welded, or brazed joints are not considered credible single barrier failures. Verification activities per SSP 52005, SSP 30558, and SSP 30559 are necessary when pressure system single barrier failures are controlled by design. These verifications include:

- *Fusion weld joints NDE method for cracks or any other type of flaw indication related to fracture critical components*
- *Established sampling procedure to ensure weld quality for items that cannot be inspected*
- *Proof testing for fracture critical pressurized lines, fittings and components to the FOS requirements*
- *Post proof testing of pressure integrity at the system level.*
- *Qualification test of individual seal*
- *Acceptance test of the pressure system*

Pressure Control

For pressurized system/vessels which are connected to a higher pressure source where pressure regulation is used to control the MDP of the lower pressure system, at least one pressure relief device is necessary.

The pressure relief device controls the MDP of the lower pressure system. The device may be a part of the two-failure tolerant design establishing MDP for the lower pressure system/vessel.

Pressure integrity is verified at the system level, i.e., after the pressure system is completely assembled (although component testing to higher proof pressure is sometimes necessary prior to assembly).

When planning overpressure protection, consider the following design features:

- *Provide overpressure protection that does not require periodic retest, such as a burst disk.*
- *Provide a relief valve with a threaded fitting and upstream pressure isolation that can easily be replaced.*
- *Provide overpressure protection that can be retested in-place.*
- *For pressure systems with a FOS of 4.0 or greater, provide overpressure protection that can be manually verified periodically in-place, such as a relief valve with a manually opening device.*
- *Provide overpressure protection for systems to be attached to the ISS cooling loops. This protection can be accomplished with an accumulator, convoluted stainless tubing, flex hose, or thermal expansion bubble.*

SSP 51721

Baseline

Verification activities per SSP 52005, SSP 30558, and SSP 30559 are necessary when pressure system single barrier failures are controlled by design. These verifications include review of design for two failure tolerance to exceeding MDP, pressure system is leak checked for complete containment integrity, pressure regulators function at the system level MDP, pressure relief devices function at the system level MDP, and thermal control systems maintain the pressure at or below the system level MDP.

Pressure Relief Valves

Relief valves may be used as components in a pressure system to provide overpressure protection to prevent exceeding the MDP. For most ground-based applications, a retest is performed annually to ensure that the relief valve set point is still within tolerances. Depending on the relief valve design, application and code certification, the retest requirement could be extended up to three years.

Failure of most pressure systems with relief valves results in a loss of functionality or mission without leading to a catastrophic hazard. If the failure of the relief valve does not cause a catastrophic failure, then extending the period of retest does not require engineering approval. The project should work with the valve manufacturer to understand the rate of degradation of the device and if that will affect the system reliability.

For spaceflight applications, retest of a relief valve may not be practical. Verification and periodic retest of relief valve functionality confirms that the valve provides overpressure protection, but the retest period is not specified in the NASA standards. Provider coordination with appropriate M&P Group is necessary to define a practical timeline for retesting or replacing relief valves based on the rating of the valve, the estimated drift of the set-point, system redundancy, consequence of failure and the ability to remove or replace the valve. Verification activity in SSP 52005, SSP 30558, and SSP 30559 include testing to demonstrate overpressure relief capability, maintenance for replacement of pressure relief valve at defined intervals, and/or operational controls for on-orbit testing or replacement is in place.

Burst Disks

Two-failure tolerance is necessary for hardware controlling pressure in pressurized systems to remain below MDP. A burst disk assembly with a robust design may be considered equivalent to two relief devices when verification activities per SSP 52005, SSP 30558, and SSP 30559 are completed related to:

- *Burst disk material compatible with the pressure system fluid*
- *Burst disk design employs a reversing membrane against a cutting edge to ensure rupture without debris generation. Historical use and experience indicate that a burst disk with cutting edge can be a highly reliable pressure relief device. The cutting edge ensures a repeatable unit-to-unit rupture pressure and this precision is especially important in systems with minimal margin on MDP.*
- *Design of burst disc does not employ sliding parts or surfaces subject to friction and/or galling.*

SSP 51721

Baseline

- *Design of burst disc includes stress corrosion resistant materials for all parts under continuous load.*
- *Qualification testing for the intended application at the intended use conditions including temperature and flow rate.*
- *Acceptance testing of membrane actuation pressure for each flight assembly using either special tooling or procedures to prevent cutting-edge contact during the test or demonstration of materials and process controls or rigorous lot testing program, and*
- *Acceptance testing to verify nominal operating pressure shows no leakage.*

Fluid Release from a Pressurized System Inside a Closed Volume

Whether in the ISS internal environment or internal compartment of a launch vehicle, a potential over pressure threat can be created with fluid release. It is important that the leakage does not induce a level of structural integrity loss for that environment. Being 2FT to fluid release helps to mitigate hazards of this nature. Per SSP 41000, release of fluid through controlled release devices do not require to complete additional analysis provided the pressurized system is 2FT to leakage.

D.4.3.1.2 Rationale – Wire Derating

Electrical Power System (EPS) analysis should be performed at the highest level of integration possible. In many cases end item hardware does not come in contact with its interface until installed on ISS. For this reason, achieving EPS compliance is heavily reliant on lower level verifications. EPS wiring and circuit protection is to be sized to protect the crew and ISS/vehicle electrical and control circuitry from injury/damage. Properly sized wiring and circuit protection is critical to the protection of safety critical circuits and/or inhibits. Electrical current passing through wire (if not controlled or limited for specific wire size) can generate excessive heat which could result in insulation pyrolyzation or safety critical circuit damage. This damage can cause crew toxicity hazards, crew touch temperature hazards, or propagation to other wires in a bundle resulting in loss of safety critical circuits.

Safety Critical Circuits

Safety critical circuits are:

- *Circuits whose loss of function could result in a critical or catastrophic hazard or,*
- *Circuits whose malfunction or degradation of performance could result in a critical or catastrophic hazard or,*
- *Circuits that control inhibits whose loss could result in critical or catastrophic hazards.*
- *Circuits that are inhibited or not operable to prevent operation a critical or catastrophic hazard*
- *No single failure can remove more than one inhibit or control to a critical or catastrophic hazard*
- *Circuits that are insusceptable to EMI*

SSP 51721 Baseline

Wire Selection

NASA recommends the use of Standard Automotive Engineers (SAE) AS22759 with silver or nickel plating, with a temperature rating of $\geq 200^{\circ}\text{C}$ for wire harnesses interfacing with ISS 120Vdc or 28Vdc power supplies. The listed wires are considered standard on NASA programs. Wiring with these specifications should be the first considerations when choosing wire for applying electrical power to devices for electrical items operating on ISS. In cases where other wire insulation is used coordination with EPS SMEs is required. The recommended wire types include AS22759/10, /11, /12, /20, /21, /22, /23, /28, /29, /30, /31, /81, /82, /83, /84, /86, /87, /89, /90, /91, /92, /181, /182, /183, /184, /186, /187, /189, /190, /191, and /192.

Circuit Protection Devices - Six Inch Criteria

When EPCEs contain less than the equivalent of six inches (power and return) of 18 American Wire Gauge (AWG) or smaller insulated wiring inside an avionics box, and the avionics box does not contain any safety critical circuitry, upstream circuit protection is not required. Circuit protection requirements are applicable to end items with any power source (i.e. ISS EPS, battery, Solar Arrays, etc.). Circuit protection requirements are also applicable to unpowered end items that can create a safety hazard if powered.

Wire Size Derating Hazards

Exceeding wire derating requirements can result in risks of exceeding maximum rated insulation temperatures based on the temperature differences experienced on orbit due to absence gravity (i.e., lack of convection cooling). This wire derating requirement applies to end item supplied harnesses which connect EPCE to the ISS interface. Derating is based upon maximum upstream current capability. Any deviation from section 4.3.1.2 will require end items to generate ISSP exception documentation to address:

- *Worst-case current environment*
- *Degradation of wire insulation materials*
- *Exceeding wire temperature rating (requirements in Table 4.3.1.2-1 and Telemetry (TM) 102179 Guidelines)*
- *Exceeding wire voltage rating*
- *Degradation of wire and wire insulation based on the upstream circuit protection switch gear trip characteristics*
- *Exceeding touch temperature limits (Table 4.3.1.2-1, column C and Technical Memorandum (TM) 102179 guidelines), and*
- *Impacts to adjacent safety critical circuitry*

Wire sizing is determined based on upstream circuit protection devices, not the planned downstream loads. In other words, the electrical distribution system is designed to protect itself not the EPCE. Wire sizing is based on the worst-case upstream available current (130% of EPCE upstream circuit protection unless higher sustained currents longer than one second are possible).

To control a catastrophic hazard, the equivalent of two fault tolerant is required. Proper wire sizing can be considered the equivalent of two levels of control (one fault tolerant)

SSP 51721
Baseline

based on DFMR criteria when Inspection of as built hardware is designed per drawings show insulation material properties (i.e. temperature, voltage, and abrasion resistance, etc. The proper selection of circuit protection can be considered the third control.

Wire Derating – General

Wire derating requirements are applicable to most wiring regardless of whether the end item is powered via battery, ISS provided power, or other power sources, including commercial off the shelf end items that interface with the ISS AC inverter. The only wiring not subject to derating requirements are Category 1 battery powered items as defined in ISS-OE-907 “Multilateral Category 1 Constraints”. The lack of convective cooling in micro-gravity requires the power wiring to be derated by a significant amount to prevent potential overheating of the wire insulation.

Wire derating provides the equivalent of two controls to prevent overheating of wiring. Appropriate wire type selection and wire derating coupled with sufficient circuit protection provides three levels of control to a catastrophic hazard.

Wire derating includes derating for wire and cables inside the EPCE and interfacing wires and cables with the EPCE power source. Wire derating selection depends upon:

- *Temperature rating of the insulation material*
- *Voltage rating of the wiring and insulation with respect to the operating and transient voltage with recommended voltage design margin*
- *Location of the wire use (IVA or EVA) which includes worst-case environment that allows for circuit protection device trips before reaching smart short current.*
- *Crew accessible wiring/cablings when powered (touch temperature hazard)*

Many circuits and electrical installations in a design will have more than one configuration that can fulfill all essential safety needs. EPCE is not considered part of the ISS electrical power distribution circuitry.

Wire Derating - Smart Short Currents

A smart short subjects wiring to currents at the highest value the source can provide without activating EPCE circuit protection devices. It is necessary to derate EPCE wire for smart short currents, or upstream circuit protection worst case limits (>1 second) per Table 4.3.1.2-1 column B.

Wire Derating – No Circuit Protection in the EPCE

When EPCE does not provide internal circuit protection, the EPCE wire size is to be compatible with upstream circuit protection devices. There are several ISS source loads including Remote Power Control Module (RPCM), PS120, utility outlet panel, PS28, standard utility panel, etc. Source loads circuit protection or current limiting for downstream EPCE are identified in interface or end item specifications, and should be referenced when completing EPCE wire sizing and circuit protection analysis.

D.4.3.1.3 Rationale – Circuit Protection

Circuit Protection - General

Circuit protection devices include fuses, circuit breakers (thermal or electronic), current limiting circuits, positive temperature coefficients (PTC) thermistors, and/or Remote Power Controllers (RPCs). Circuit protection can be provided by other upstream devices that are not in the EPCE, such as ISS EPS devices. Each type of circuit protection device provides specific characteristics that warrant its use in a particular circuit or location to prevent damage to the ISS EPS and/or its associated distribution wiring.

Circuit Protection - Thermal Protective Devices

Thermal protective devices (i.e., fuses and circuit breakers) may be capable of delivering full max blow capability on orbit when operated either in a temperature controlled environment or in a path of circulating cabin air. Reducing the fuse and circuit breaker size based on derating levels could result in a mission success concern, even though the reduced fuse size provides additional margin in the control of wire overheating.

Circuit Protection - Six Inch Criteria

When EPCEs contain less than the equivalent of six inches (power and return) of 18 AWG or smaller insulated wiring inside an avionics box, and the avionics box does not contain any safety critical circuitry, upstream circuit protection is not required. This is because such short lengths of wire cannot produce enough pyrolysis products to create a hazard.

In the event of a conflict between circuit protection device derating for mission success and circuit protection device sizing for safety, the safety circuit protection sizing requirement takes precedence. Although circuit protection compliance provides wire insulation protection, EPCEs are not relieved of meeting ISS flammability requirements.

Circuit Protection - Smart Short Currents

Properly implemented, circuit protection devices limit wire insulation temperatures below derated wiring limits to preclude crew and equipment hazards for any possible circuit load/fault condition. Sustained smart short currents are maximum current allowed for > 1 second by the upstream circuit protection device.

NASA requires wiring to be protected against smart shorts.

Circuit Protection – Fuses

Fuses are generally used in areas where no quick response time is necessary. Fuses can be used in Must Not Work safety critical circuits, do not require immediate circuit breaker reset capability to mitigate a safety concern, or rely on other circuits to provide power redundancy. When there is a fuse failure, the downstream circuit receives no electrical power. Derating of fuses could be necessary when operating on ISS since fuses can heat faster and open at lower level currents in the micro-g or vacuum environment.

Circuit Protection – Circuit Breakers

Circuit breakers (CBs) are used in circuits that require reset capability and are in locations that are accessible to the crew. Derating of thermal circuit breakers are necessary. Derating factors for magnetic type CBs are less than those of fuses since magnetic type CBs is less dependent on convection cooling than fuses. CBs should not be used as power switches (on/off switches) unless the CB is a three position CB with clear open, tripped, and closed positions and indications for crew verification. The preference is for a power switch combined with a CB for EPCE input power protection.

Circuit Protection – Last Wire Downsizing in Avionics Boxes

Circuit protection is not typically required for last wire downsizing inside habitable area avionics boxes that are designed and tested to standard aerospace practices, and do not contain safety critical circuitry. This is because:

Avionics boxes provide excellent physical protection of wire segments routed internal to the box since designs cannot dictate wire termination sizes on all components, circuit protective devices may not prevent failure of electrical components that draw small electrical currents, and use non-flammable materials to prevent fire propagation.

Circuit protective devices do not always prevent failure of electrical components that draw small electrical currents. When avionics boxes are not considered sealed containers, it is necessary to assess the power wiring inside when EPCEs contain more than six inches (power and return) of 18 AWG (American Wire Gauge) or smaller insulated wiring inside an avionics box. This is because lengths of wire greater than 6 inches can produce enough pyrolysis products to create a hazard venting into the crew environment.

The primary control for fire propagation is the use of non-flammable materials.

Circuit Protection - Protection Devices – Parallel Power Wires

When two parallel power wires originate from one source and are later joined together downstream prior to distributing power to an EPCE, each wire is to have its own circuit protection device.

When there are more than two parallel power wires originating from one source and are later joined together downstream prior to distributing power to an EPCE, each wire is to have circuit protection devices at both the source and load end of the wire, otherwise faults could be fed through the back end of the circuit. A common example of parallel power wiring is when the electrical components limit the wire sizing (i.e., connector sockets size limits wire sizing, Printed Circuit Board (PCB) connectors limit wire sizing, or wire bundles have size limitations for routing or bend radius limitations).

Circuit Protection - RPCs

RPCs are solid state resettable devices that provide current sensing, current limiting on certain types, and continuous monitoring. When there is an overload, the RPC could either go into current limit (RPCM Type I, II & V) and trip or simply trip once a threshold is reached (RPCM Type III, IV & VI). RPCs do not require derating since the devices are

SSP 51721
Baseline

not thermally sensitive. The most prevalent RPC in the ISS is the current limiting Type V.

D.4.3.1.4 Rationale – DC Circuit Electrical Inhibits Used to Prevent Catastrophic Hazards

Direct Current Circuit Electrical Inhibits

Electronics boxes could contain numerous “inadvertent” energized sources, loose wires, washers, and debris due to workmanship errors and improper routing of wires in boxes. Inadvertent motion of mechanical systems or activation of transmitters using DC circuits may have catastrophic consequences.

Direct Current Circuit Electrical Inhibits – Return Leg Inhibits

The return leg inhibit requirement was added to safety requirements after the Challenger accident. NASA determined that protection is necessary for inadvertent application of power since downstream (bypass) of all power side inhibits is a credible failure mode.

Direct Current Circuit Electrical Inhibits – When Ground Return Leg Inhibit Not Possible

Some end items by design can contain three independent inhibits, but a ground return inhibit is not possible in the design. Analysis is required to show that single events or failures do not bypass or remove more than one inhibit (e.g., RF and/or digital circuits).

One example is RF oscillators may not be designed with a return leg inhibit due to the ground plane design. However, the RF enabling circuitry requires two actions to cause the transmitter to activate (i.e., a command to activate the carrier oscillator and a transmit command to start the transmitter). Analysis and test verification is necessary for a design that requires two distinct controls/commands to activate the RF. When RF commands are routed through a computer or complex electronic device, the requirements in Section 4.4.1 (Computer Based Control Systems) are applicable. Another example is a stepper motor. Stepper motors may not be capable of being designed with a return leg inhibit. Although stepper motors may provide three independent inhibits to prevent inadvertent operation, motor operation is a pulse driven function. If no pulse signal can be sent, then there is no hazard. Therefore, control circuitry analysis and testing are necessary to show stepper motor is incapable of receiving commands (e.g., field programmable gate array to drive the stepper motor is off or unable to drive the motor). ISRP review on a case by case basis is necessary for DC circuits to prevent a catastrophic hazard without a return leg inhibit.

D.4.3.1.5 Rationale – Separation of Redundant Safety Critical Circuits

As a result of increased emphasis on the routing of redundant safety critical circuits, it is necessary to ensure separation of redundant paths to eliminate common cause failures. This ensures that an unexpected event damaging one circuit is not likely to prevent the other circuits from performing the function. All redundant functions required to prevent a catastrophic hazard cannot be routed through a single connector. A possible cause of the failure of redundant safety critical circuits in the HR is damage to electrical circuits.

SSP 51721

Baseline

Wire bundles are considered to be any group of wires that are spot-tied or clamped together. When safety critical circuits cannot be separated from a common wire bundle or connector, additional design feature (e.g., physical barrier that prevents failures in one safety critical circuit from propagating to adjacent safety critical circuits, or separated by the maximum possible distance in the connector to eliminate bent pins from bypassing inhibits or shorting power sources used for hazardous functions) can be considered on a case-by-case basis.

D.4.3.2 Rationale – Electric Shock

General

The ISS IVA environment poses similar shock hazard conditions as working with electrically powered devices in terrestrial wet/damp conditions. The ISS EVA environment also poses shock hazards to the crew in Extravehicular Activity Mobility Units (EMUs) (i.e. with electrically powered devices, etc.). There are also catastrophic hazards posed by the generation of any molten metal during electrical connector mating/demating that can either damage the EMU or result in IVA crew hazards. These environments require added diligence in ensuring electric shock and molten metal hazards are prevented.

End items planning to interface with the ISS inverter require compliance to JSC 66202, ISS Power Inverter to 120VAC 60Hz loads IDD and ISS-NCR-IPVR-001, to prevent integrated electric shock hazards.

Prevention

Electric Shock is prevented by providing two failure tolerance by design through isolating electric currents from EPCE crew accessible surfaces with voltages >32V DC/rms (input or internally converted), and for all voltages when directly connected to crew medical devices This can be accomplished in the following ways:

- *Limiting non-patient equipment enclosure and chassis leakage currents (Sections 4.3.2.1 and 4.3.2.2)*
- *Providing protective covers for electrical power conductors, terminations, and unterminated power connectors (Section 4.3.2.3)*
- *Electrical bonding and grounding with H class bond interfaces ($\leq 0.1 \Omega$). - 2 levels of control (Section 4.3.2.4)*
 - *2 ground wires (redundant grounding) from device chassis ground to power source ground for crew accessible surfaces or DFMR ground path with Class H bond interfaces ($\leq 0.1 \text{ Ohm}$) for all crew accessible interfaces and interfaces to ground path(s) back to power source ground – 2 levels of control*
- *EPCE isolation > 1M Ω (grounding isolation from EPCE electronics and also from power input [hot/return]) – 1 level of control (Section 4.3.2.4)*
- *EPCE isolation of secondary power [hot/return output] from primary power [hot/return input] >1M Ω for internally generated voltages >32V (High Voltage secondary power isolation) – 1 level of control (Section 4.3.2.4)*
- *Insulated wires and cables – (portable/non-rack equipment requirement) with double insulation (Section 4.3.2.3)*

SSP 51721
Baseline

D.4.3.2.1 Rationale – General EPCE with No Direct Interface to Medical Equipment

Leakage Currents

Leakage currents and touch currents can result in electrical shock to the crew. Leakage currents are measured on the ground (chassis) portion of the electrical circuitry while touch current is measured at the device enclosure.

<32V dc/rms

The ISRP in conjunction with Johnson Space Center (JSC) Human Health and Performance (HHP), determined that there are no credible shock hazards to the crew for voltages <32V dc/rms from non-patient electrical devices. Medical equipment includes crew bioinstrumentation (invasive and non-invasive) and patient devices. General EPCE is an EPCE that is not used in crew bioinstrumentation, or CMRS activities or is crew accessible when the crew is connected to Bioinstrumentation or Medical Devices.

Touch Currents

Touch current is leakage current flowing through a human body when it touches one or more accessible parts of equipment. Touch current was previously known as “enclosure leakage current” or “chassis leakage current”. All electrical equipment, when powered, has a touch current because there are no perfect insulators. All circuits provide some current through electrical circuitry either to equipment chassis (i.e., ground), or through imperfect enclosure insulators (e.g., plastics). This includes items that use a 120V dc/rms power source, regardless of any step-down converters in the electrical device.

IEC 60601

Per the IEC 60601, Class I devices are not double insulated. General equipment that is not double insulated is required to provide hazard controls consistent with bonding and isolation requirements of Section 4.3.2.4.

Per IEC 60601, double insulated devices typically have a non-conductive housing and thus touch current typically will not flow on robust non-metallic housings without a failure(s). When the enclosure is double insulated, touch current becomes the primary measure by which a leakage current failure through a non-conductive enclosure can create a shock hazard.

Touch Current \leq 0.5mA

When general EPCE or chassis touch/leakage currents are \leq 0.5mA, the crew is protected from excessive levels of current leakage from electrically powered equipment as a result of direct or incidental contact. Since reverse polarity can damage equipment, reverse polarity input testing is to be prohibited. The non-Medical EPCE is not crew accessible when the crew is connected to Bioinstrumentation or Medical Device such that leakage currents >0.1 mA are not introduced to the crew when instrumented or otherwise connected to a Medical Device. Section 4.3.2.1 can also be met when Class I devices provide controls consistent with bonding/grounding and isolation requirements of Section 4.3.2.4 for all crew accessible surfaces and power sources. Class III

SSP 51721

Baseline

equipment (internally powered) is not required to meet touch current requirements when the equipment is <32Vdc/rms.

D.4.3.2.2 Rationale – General EPCE with Direct Interfaces to Medical Equipment

Most general EPCE allows a much higher leakage or touch current than medical equipment. General equipment that has direct interfaces to medical equipment can introduce extraneous electrical currents to lower impedance paths. In this case, the lower impedance could result in heart fibrillation when the –crew is connected to medical equipment. Crew with general EPCE operating around the patient can create an electrical path between general EPCE and the patient or patient equipment.

Requirements Derivation

Requirements for touch or leakage currents are derived from IEC 60601-1 and UL 60601-1, Safety Standards for Medical Equipment. It is necessary to protect the crew from lethal or disabling leakage currents from patient and general devices. Crew is protected from shock hazards when touch currents from medical equipment are <0.1mA.

EPCE and $\leq 0.1\text{mA}$

General EPCE with direct interfaces to medical equipment that provide electrical isolation and bonding/grounding per Section 4.3.2.4 fulfills the $\leq 0.1\text{mA}$ requirement since touch currents are electrically isolated and the EPCE is bonded/grounded back to the source ground.

EPCE Current Redirection

The general EPCE leakage current can be redirected through the patient via contact with patient electrodes or through contact with an attending crewmember. For terrestrial applications, UL60601-1 suggests (as derived from the IEC 60601) maintaining a 7.5' radius separation distance between non-medical equipment and patient equipment. This is not feasible in the ISS environment, but other factors mitigate the risk. This radius is intended to protect patients during invasive procedures. The likelihood of this occurring on ISS is remote. Currently, no ISS medical equipment has an invasive connection and no planned invasive procedures documented. It is necessary for ISS equipment to meet more conservative design requirements than terrestrial equipment, i.e. bonding, grounding, and non-medical equipment touch current requirement of $\leq 0.5\text{mA}$.

D.4.3.2.4 Rationale – Bonding, Grounding and Electrical Isolation

Electrical shock is considered a catastrophic hazard. End items are required to provide three controls to protect the crew from shock hazards when voltages are > 32V dc/rms.

Hazard Control Methods

The general EPCE leakage current can be redirected through the patient via contact with patient electrodes or through contact with an attending crewmember. For terrestrial applications, UL60601-1 suggests (as derived from the IEC 60601) maintaining a 7.5'

SSP 51721

Baseline

radius separation distance between non-medical equipment and patient equipment. This is not feasible in the ISS environment, but other factors mitigate the risk. This radius is intended to protect patients during invasive procedures. The likelihood of this occurring on ISS is remote. Currently, no ISS medical equipment has an invasive connection and no planned invasive procedures documented. It is necessary for ISS equipment to meet more conservative design requirements than terrestrial equipment, i.e., bonding, grounding, and non-medical equipment touch current requirement of $\leq 0.5\text{mA}$.

Rack and Rack Mounted HW

For racks or rack-mounted hardware this typically involves two controls for electrical bonding (Class H) and grounding and one control for electrical isolation. A combination of ground continuity, properly bonded ground interfaces are required for electric shock controls, in addition to electrical isolation.

Portable and Non-Rack Equipment

Portable and non-rack equipment involves providing one control for electrical isolation and two controls for electrical bonding/grounding.

Cabling for Portable and Non-Rack Equipment

One control for electrical bonding/grounding (which complies with Class H bond interface requirements) and two controls for electrical insulation are necessary for portable and non-rack cabling. Cabling is not specifically isolated (electrical circuitry is), but cables can be shown to be electrically insulated (double insulation) and the shield bonded/grounded back to the power source ground.

Class H Bonding

bond. The primary method is a direct bond. The other is indirect bonding. Direct and some indirect bonds are considered DFMR since design implementation is highly reliable with low risk of failure. A DFMR bond is considered the equivalent of two independent controls. A DFMR bond is one with a faying surface $> 4X$ the equivalent cross-sectional area of derated copper wiring necessary to carry the fault bond current, washers provide proper contact area and pressure in the bond path (no star washers are to be used), the fasteners maintain proper contact with proper back-off prevention, and proper surface treatments are applied.

Alternate Bonding Methods

An alternate method is to use redundant electrical bonding and grounding paths such as two safety (ground) wires or a safety wire and cable shield, thus providing two hazard controls. Cable shields used as electrical bonding/grounding paths to prevent shock hazards are required to meet Class H bonding requirements and grounding continuity requirements, and terminated to the connector backshell per standard aerospace practices at each connector.

SSP 51721 Baseline

Unique Hazard Reports (UHR)

Many electrical bonding, grounding and isolation requirements for voltages < 32V are located in the applicable IRD or equivalent specifications along with the verification requirements and methodologies, and are also addressed in the Standard Hazard report Controls/Verifications. A UHR is required to define electrical shock hazard controls in the following situations:

- *The end item that uses or generates voltages greater than 32V dc/rms.*
- *Operational controls are necessary to preclude shock hazards.*
- *End item spacecraft charging or incompatibility with the plasma environment that may lead to shock hazards.*

Insulation

Electrical bonding/grounding is not a required control when all crew accessible surfaces constitute a double insulated electrical barrier or enclosure “with each level of insulation shown to withstand >4X the highest voltage: surfaces are non-metallic, non-conducting surfaces when it is shown the surfaces constitute a double insulated electrical barrier or enclosure”. This is equivalent to two hazard controls with a third control provided by electrical isolation >1M Ω from primary input power and chassis or from primary input power and internal secondary power output.

Cable Connectors

Cable connectors that contain voltages > 32V dc/rms require shock hazard controls. This may be in the form of a Class H bond interfaces and an acceptable ground path through equipment or bulkhead connector back shells to ISS structure, insulating sleeve, or covered with electrically insulating material per verifications in Section 4.3.2.1.A to prevent crew contact. Electrical connectors bonded through bulkhead connections are considered DFMR provided appropriate DFMR criteria is applied to all bonds for these connectors. Figures D.4.3.2.4-1 through D.4.3.2.4-5 provide examples of alternate bonding methods for cable connectors when DFMR methods are not used in order to provide a second hazard control. In Figures D.4.3.2.4-1 through D.4.3.2.4-5, the term “ground wire” is often includes an electrical bond interfaces.

Floating Power Connector Bonding

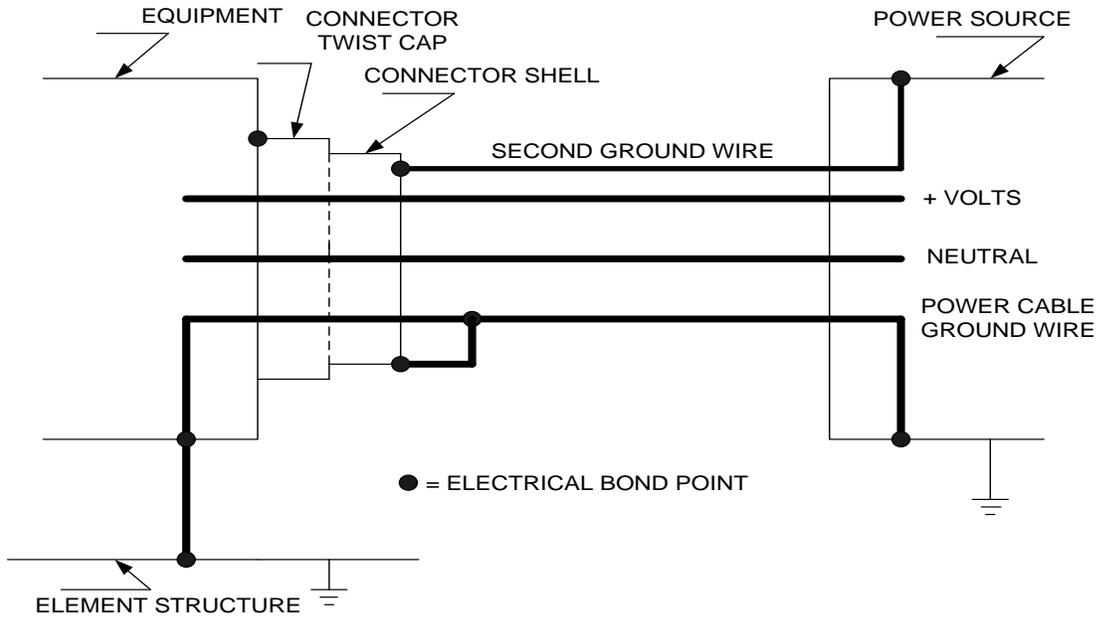
The connector shell is said to be floating when it is not connected (bonded/grounded) ISS structure. To prevent shock hazards associated with floating connectors, bond interfaces between the connector shell and structure are necessary to assure continuity of the ground path back to the power source ground. Figures D.4.3.2.4-4 (Power Cable Floating Connector Interface – Backshell to Groundwire) and Figure D.4.3.2.4-5 (Power Cable Floating Connector Interface Backshell to Backshell) provides guidance in the architecture of recommended floating connectors on ISS.

TABLE D.4.3.2.4-1 MEASURES TO PREVENT CREW ELECTRICAL SHOCK HAZARDS

Hazard Control Method	Implementation	# of Controls	Notes
Direct class H bond path	Direct bonding method (DFMR) ^{1,2,3} .	2	Metal-to-metal interfaces joined by processes that transform the mated surfaces into one piece of metal (e.g., welding or brazing) are considered permanent and are inherently bonded. Semi-permanent joints held together by screws, rivets, clamps, etc., are also considered direct bonds. This method provides confidence that conductive paths are sized to carry maximum faults currents. The bond path is considered reliable, having undergone materials and structural verifications as well as electrical. A DFMR bond is one with a faying surface > 4X the equivalent cross-sectional area of copper wiring necessary to carry the fault bond current, washers provide proper contact area and pressure in the bond path, fasteners maintain proper contact, and proper surface treatments are applied.
Indirect class H bond path	Indirect bond path classified as DFMR ^{1,2,3} .	2	Some indirect bonds may be considered DFMR. For example, the rack-to-ISS bond strap (683-56200), bond strap 683-13477-1 or military-grade bond straps such as MIL-DTL-83413/8C (excluding types D, E, and H) or MIL-DTL-24749, types III or IV are considered a DFMR bond paths. A DFMR bond is one with a faying surface > 4X the equivalent cross-sectional area of copper wiring necessary to carry the fault bond current, washers provide proper contact area and pressure in the bond path, fasteners maintain proper contact, and proper surface treatments are applied. These particular types of bond strap applications have undergone extensive life-cycle testing, and mechanical testing to show that use on ISS will not result in a damage or loss of bond path during the ISS planned lifetime.
Indirect class H bond path	Indirect bond path not classified as DFMR ^{2,3} .	1	Examples include ground or third wire in harness connected to both the end item and power source reference. The ISS structure for ISS-provided 120 Vdc power or overall cable shield is sized to carry fault current and terminated to end item and power source reference. Use of a second independent indirect bond path would provide a second control.
Isolation (primary or input isolation)	> 1MΩ isolation between end item hot and chassis and return and chassis	1	Provides a single independent control.
Isolation (secondary)	> 1MΩ isolation between hazardous voltages (>32V dc/rms) and crew accessible low voltages (e.g., 5 Vdc or 28 Vdc)	1	When low voltage is crew accessible and either generates or is generated from a voltage that exceeds 32V dc/rms, the isolation between low voltage and high voltage is required in addition to the input isolation requirement.
Double Insulation	All crew accessible surface are non-metallic, non-conducting surfaces.	2	UL and/or CSA and/or CE listing for COTS hardware provides two controls.
Electrical Isolation	Crew accessible surfaces are conductive, with internal double insulation	1	Requires conductive surface to be isolated by >1MΩ from electrical conductors.
GFCI	AC powered devices only	1	Only applicable for end items powered via the ISS AC Inverter.

Notes:

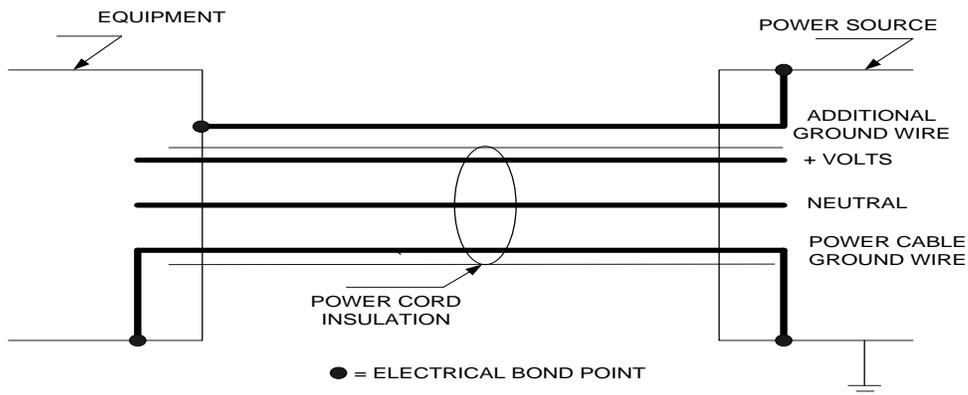
- 1) DFMR is considered the equivalent of two independent controls. It applies when the design implementation is highly reliable and considered low risk to failure.
- 2) MSFC-HDBK-3697, Electrical Bonding Design Guide Handbook can be used as a reference in designing electrical bonds.
- 3) This applies to all conducting surfaces accessible to crew that could be energized in a fault condition.



POWER CABLE CONNECTED TO EQUIPMENT EXAMPLE 1

- 1 – POWER CABLE GROUND WIRE
- 2- CONNECTOR BONDED TO EQUIPMENT THROUGH NORMAL CONNECTOR MECHANICAL ACTION
- 3 – IF POWER CAN BE APPLIED AFTER THE LOAD CONNECTOR IS DISCONNECTED THEN A SECOND GROUND WIRE IS REQUIRED

FIGURE D.4.3.2.4-1 POWER CABLE CONNECTED TO EQUIPMENT



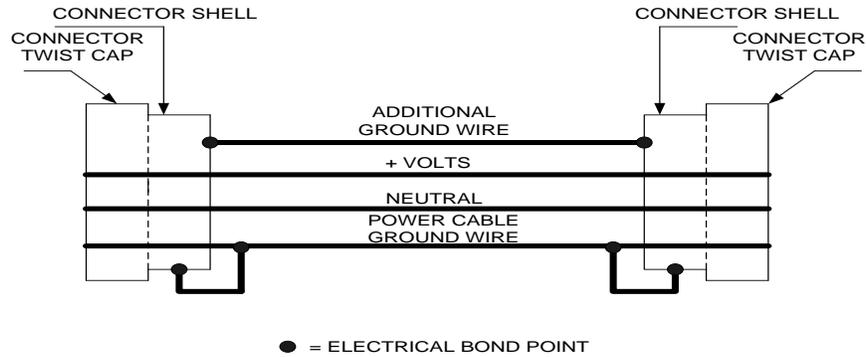
POWER CABLE CONNECTED TO PORTABLE EQUIPMENT EXAMPLE 2

- 1 – POWER CABLE GROUND WIRE
- 2 - ADDITIONAL GREEN WIRE
- 3 – ALTHOUGH NO CONDUCTIVE SHELL POWER CONNECTORS ARE INVOLVED, THREE GROUND FAULT CONTROLS ARE STILL REQUIRED

FIGURE D.4.3.2.4-2 POWER CABLE CONNECTED TO PORTABLE EQUIPMENT

SSP 51721
Baseline

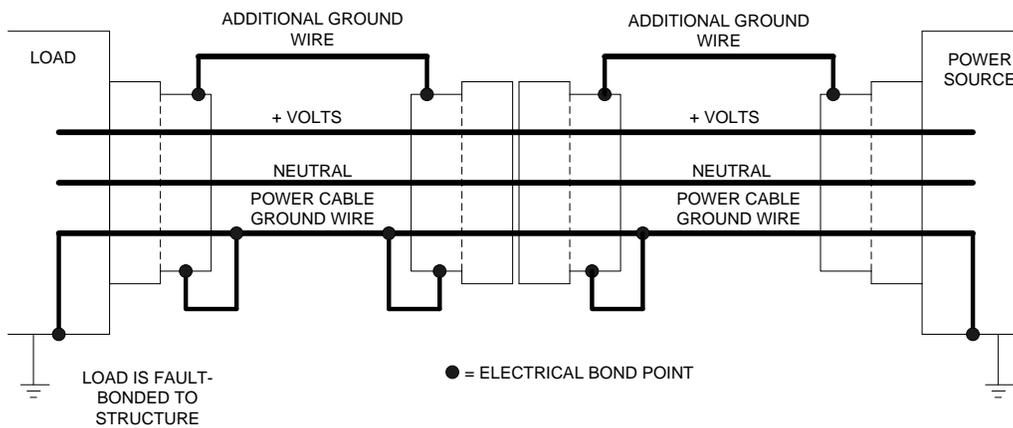
Power connections in example 2 represent a COTS power cord configuration with non-conductive connector shells that plugs into a standard wall outlet, power supply or an equipment directly wired to its power supply.



POWER CABLE USED AS EXTENSION/JUMPER EXAMPLE 3

- 1 - POWER CABLE GROUND WIRE BONDED TO CONNECTOR SHELLS
- 2 - ADDITIONAL GROUND WIRE
- 3 - POWER CABLE GROUND WIRE MUST BE GROUNDED AT THE POWER SOURCE

FIGURE D.4.3.2.4-3 POWER CABLE AS AN EXTENSION OR JUMPER



POWER CABLE FLOATING CONNECTOR INTERFACE EXAMPLE 4

- 1 - POWER CABLE GROUND WIRE BONDED TO CONNECTOR SHELLS
- 2 - ADDITIONAL GROUND WIRE
- 3 - POWER CABLE GROUND WIRE MUST BE GROUNDED AT THE POWER SOURCE

FIGURE D.4.3.2.4-4 POWER CABLE FLOATING CONNECTOR INTERFACE – BACKSHELL TO GROUND WIRE

SSP 51721 Baseline

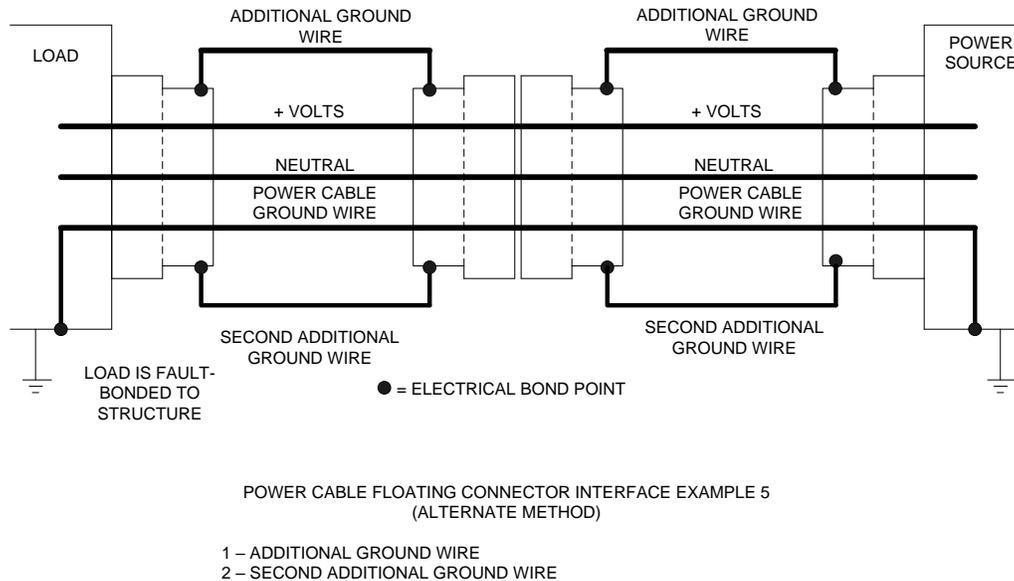


FIGURE D.4.3.2.4-5 POWER CABLE FLOATING CONNECTOR INTERFACE – BACKSHELL TO BACKSHELL

D.4.3.3.1 Rationale - Scoop-Proof Power Connectors

The use of mechanical design features are necessary to fully enclose or shroud the power connector pins and sockets during mate/demate activities. This minimizes the potential for molten metal caused by FOD or bent pins. Scoop Proof designs provide a longer shell design on the pin half of a connector. This requirement is applicable to EVA/IVA connectors.

This is the primary design feature that protects against production of molten metal. The longer shell allows the pin contacts to be recessed sufficiently so as not to be damaged if the mating shell is “scooped” into it, thus preventing pins from being bent or contacts from being electrically shorted during mating. The design of AC plugs does not meet this standard because it is not shrouded when partially de-mated. A bent pin analysis is recommended to ensure bent pins will not bypass safety critical circuits, remove more than one inhibit to a hazard, or cause molten metal hazards.

Inadvertent Connection Reversal

Per the IRD, end items with electrical connectors are required to design the electrical connectors to prevent inadvertently reversing a connection or mating the wrong connectors if a hazardous condition can be created.

Bonding and Isolation

Power connectors that contain voltages >32Vdc/rms also create additional hazard potential of crew electrical shock. As noted in Section 4.3.2.4 (Bonding and Isolation), additional cable and connector design features are necessary to protect from electric shock hazards.

SSP 51721
Baseline

D.4.3.3.2 Rationale – Power Connector Sockets

Exposed conductors and terminations can result in electrical shock to the crew as a result of direct or indirect contact. The powered side of the connectors are to be terminated in sockets (versus pins). This minimizes the risks of molten metal caused by FOD or bent pins, and precludes inadvertent shorting when the connector is unmated or exposed to the crew. This requirement is applicable to both EVA and IVA connectors.

Unmated Electrical Connectors

When powered side of connectors are left unmated, the connector is to be covered and powered off as per Section 4.3.2.3.

D.4.3.3.3 Rationale – Upstream Verifiable Inhibit for Power Connectors

Power connectors with upstream available current >3A can present shock or molten metal hazards to the crew and/or equipment during power connector mate/demate. A verifiable upstream inhibit provides one level of control to prevent shock and/or molten metal hazards to the crew.

This requirement is applicable to EVA/IVA connectors.

Other Controls

Other controls are provided via connector attributes (scoop proof connectors, and powered side of interface in pins), and connector electrical bonding, grounding, and isolation.

Inhibit Enabling

The upstream verifiable inhibit can be enabled by the crew or ground by removing power upstream of the power connector(s) prior to mate/demate activities. This upstream inhibit can be provided by the end item or other ISS resources and provides one level of control.

>200V dc/rms

An additional (2nd) verifiable upstream inhibit is necessary when the open circuit voltage is >200 V dc/rms, short-circuit current > 65A, power is >8.2Kw, or batteries are > 40Vdc OCV. For more information on connectors with >200 V dc/rms, short-circuit current > 65A, power is >8.2Kw, or batteries are > 40Vdc OCV, refer to Section 4.3.3.7.

Monitoring

Verifying the upstream inhibit has been established using Sections 4.5.1 and 4.5.2. Once an inhibit is confirmed, the inhibit does not need to be continuously monitored since is considered to be in a safe state for mechanical type inhibits such as manual switches, RPCs, etc. Other inhibit types that have commandable controls or controls not implemented by the crew require monitoring during the timeframe of the hazard. For more information on monitoring requirements, refer to Section 4.5.

SSP 51721

Baseline

Batteries <40V

Refer to Section 4.3.3.5 for batteries with voltages <40V when the battery or battery box is inserted directly into an enclosure.

D.4.3.3.4 Rationale – EVA 2nd Upstream Inhibit electrical Power Connectors <200V dc/rms, <65A, <8.2 KW, or a Battery OCV <40V dc

The second inhibit is required for EVA because arcing and molten metal can cause a hole in the Extravehicular Activity Mobility Unit (EMU) or potentially ignite the 100 percent Oxygen in the EMU. This requirement can only be applied to end items that have <200V OCV dc/rms, <65A short circuit current, <8.2Kw power capabilities, or <40V dc batteries. A second inhibit is not necessary for Extravehicular Activity Robotics since the crew is not mating or demating electrical connectors.

Monitoring

Monitoring of the second inhibit is not required when OCV is <200Vdc, short circuit current <65A, power availability is <8.2Kw, or batteries OCVs are <40V.

Minimizing Downstream Loads

A series of tests were managed by the JSC Engineering Directorate to evaluate molten metal hazards related to electrical connector mate/demate. The theory was potential to arc is a function of available power and the sharpness of pins. Testing showed contacts begin pitting at 1.5 amperes and 123 V for 22-AWG pins or 184.5 watts. Based on this data, the 180-watt limit was chosen as a conservative value for this interpretation. Test data associated with a 22-AWG connector (smallest pin size expected) also showed that minimal damage occurs from 1.5 ampere to 3.8 ampere (average is 3) at 33 volts. Therefore, for higher voltages (e.g. 120V), the limit is based on power (e.g., 188 W). For lower voltages (<32V), the limit is based on current (e.g. ≤3A). An adequate margin of safety is in place because the limits are set based on initiation of pitting or contact damage rather than the contact fail threshold. Additionally, the limits are also set based on the smallest pin size, which is rarely used in EVA applications. For more details on this testing, refer to EP5-T51-015.

EMI Input Filter Considerations

When there are input EMI filters upstream of the switching device which remove downstream loads to less than 180W or 3A, there can be transient exceedances of these values until the capacitors are charged in the EMI input filter. In the event end items do not show successful compliance with the IRD or equivalent requirements for inrush current caused by EMI filters, additional verification is necessary to show downstream loads are <180W or 3A. This type of design is acceptable when input filter energy storage capability is no greater than that allowed in Table 4.3.3.4-1 – Input EMI Filter Energy Storage Capability Calculation.

D.4.3.3.5 Rationale - Battery Connectors with OCV <40Vdc

When battery voltages are <40Vdc with >3A worst case current capabilities, there is a molten metal and shock hazard. Either providing one verifiable upstream inhibit of all

SSP 51721
Baseline

power sources or limiting short-circuit currents is necessary. The inhibits/controls for molten metal and /or shock hazard should provide safety features for both battery power inhibiting and other power sources on same buses (i.e., ISS powered with battery back-back or secondary power, or for battery chargers. This will address multiple power sources for a single mate/demate connection.

Limiting Short Circuit Current

Limiting the short circuit currents to < 20 A with the 0.5 seconds provides confidence that the shroud provides crew protection. The 0.5-second duration is based on engineering judgment that energy (heat) is limited when current is reduced within 20A limit within 0.5 second. The initial short duration current delivering properties of even small batteries is relatively high, but the current should decrease rapidly. This requirement encompasses most of the COTS batteries.

40Vdc Batteries

The ISRP and HHP extend the 32Vdc limit criteria to 40Vdc for batteries. Hand-to-hand resistance values are sufficiently high to reasonably reduce the risk of fibrillation at or below 40V when batteries are inserted into an enclosure. This is considered valid since battery installation results in hand-to-hand contact only. The 40Vdc is derived based on 1K hand-to-hand contact impedance with 40 mA let-go threshold current based on 99.5 percentile rank of adults.*

D.4.3.3.6 Rationale – Blind Mate or Remote Connectors >32V dc/rms

Electric shock can result when crew connects or disconnects remote connectors. This requirement is applicable to both EVA and IVA connectors. Molten metal is not considered a risk since the crew is removed from the local area of the connector.

Connectors are considered remote when they are inaccessible to the crew such as back-of-the-rack connectors. These connectors are also sometimes referred to as blind-mate connectors. Due to the nature of the connector being remote, it may not be practical to inhibit power to the connector (e.g., back-of-the-rack connectors could require inhibiting the entire rack to <3A).

Since one half of the connector remains mated to the rack (structure), it is necessary to ensure Class H bonds are in place prior to any mate, and remains bonded until power connectors fully demate to prevent electric shock hazards (<0.1Ω). The Class H Bond ensures that there are no potential differences between the interfaces during crew installation, maintenance, or other end item reconfiguration activities that make repeatable or DFMR bonds prior to any power connector mate activity >3A upstream available current, and remains bonded until full demate of the power connector(s).

End items that use electrical power >32V dc/rms are required for primary power to be isolated from chassis primary power from secondary (hot/return) by $\geq 1 \text{ M}\Omega$. This provides a single level of protection against electrical shock hazards.

When voltages > 32 V dc/rms are converted to voltages $\leq 32 \text{ V dc/rms}$, it is necessary to maintaining isolation between > 32 V dc/rms hardware and lower voltages of at $\geq 1 \text{ M}\Omega$.

SSP 51721
Baseline

This prevents potential differences that can be a shock concern while transitioning to low voltage circuits.

D.4.3.3.7 Rationale – 2nd Verifiable Upstream Inhibit for Power Connectors >200V dc/rms, >65A, >8.2Kw, and/or >40Vdc Batteries

An additional (2nd) verifiable upstream inhibit is necessary when the open circuit voltage is >200 V dc/rms, short-circuit current > 65A, power is >8.2Kw, or batteries are > 40Vdc OCV. This requirement is applicable to both EVA and IVA connectors.

Since connector testing has shown that 67 ampere at 33 volts is the threshold for significant damage to sockets, 65 ampere was chosen as the limit for connector shells. Therefore, a more stringent requirement is imposed for circuits in excess of this value. An 8.2Kw limit (65 amperes at 126 volts) was selected based on the capabilities of the ISS Direct Current-to-Direct Current Converter Unit.

Initial short duration currents with batteries >40Vdc OCV can deliver high currents that result in molten metal hazards. A shroud does not provide protection; therefore, an additional inhibit is required.

The use of Ground Fault Circuit Interrupts (GFCIs) are not allowed as a substitute for an upstream inhibit because GFCI current limits do not protect for concerns associated with molten metal hazards.

D.4.3.4.2 Rationale – Bioinstrumentation Touch/Leakage Current

This applies to nominal and failure cases of modified and/or new bioinstrumentation Class I (grounded) and Class II (double insulated) equipment and to Types B, BF and CF equipment as defined in IEC/UL 60601-1, summarized in Table 4.3.4-1.

Unintended leakage currents can be the result of:

- *Contact with available electric sources, including those sources applied by an attending crewmember's simultaneous contact with the instrumented crewmember and other equipment or ground, and*
- *Transients that may occur when the bioinstrumentation is either energized (turned ON) or de-energized (turned OFF).*

D.4.3.5.1 Rationale – Low BRC Batteries

UHRs for Low BRC batteries should use ISS Hazards System (IHS) Template # 29075. The HR Battery Description Form will be attached to the UHR and is available as an attachment to the template.

By meeting manufacturer specifications, the end item provider will have confidence that the cells/batteries will perform as expected. The lowest level of hazard control is reserved for low energy cells and battery designs for which standard emergency procedures are written and practiced. These batteries/cells have a low likelihood of causing injury or damage; therefore, a minimal amount of verification is requested for the end item. It is recommended to review the failure history of the cell/battery design

SSP 51721
Baseline

using the Consumer Product Safety Commission (CPSC) recall database at the <https://www.cpsc.gov/recalls/>.

D.4.3.5.2 Rationale – Medium/High BRC Batteries

UHRs for Medium and High BRC batteries should use IHS Template # 28907. The HR Battery Description Form will be attached to the UHR and is available as an attachment to the template.

Medium BRC batteries/cells are typically manufactured in high volumes for the consumer and have commonly available means to help determine the reliability and safety of the products. Due the consequence of a failure, these end items must follow a comprehensive test and validation plan.

High BRC batteries/cells are typically custom, high energy, or high power designs. Due the extreme consequence of a failure, these end items must follow a comprehensive test and validation plan that includes testing to determine the result of single cell thermal runaway. The analysis of the thermal runaway can lead to a redesign of the battery to mitigate the consequence.

Medium and High BRC custom batteries must characterize the performance and safety of the flight battery design by conducting an Engineering Evaluation (JSC 20793, Section 4.2.1).

Characterizing the prospective cell and battery safety under abuse conditions must include:

- *Overcharge*
- *Over-discharge into reversal*
- *Over-discharge and recharge of secondary batteries*
- *External short circuit and cell internal short circuit*
- *Temperature tolerance*
- *Vent and burst pressure determination*
- *Cell Destructive Physical Analysis (DPA)*
- *Cell radiographic inspection*
- *Confirmation of manufacturer's specifications that are relevant to the project, as well as confirm that the cell and/or battery design can handle unique requirements levied by the project. Review failure history of the cell/battery design using the CPSC recall database at the <https://www.cpsc.gov/recalls/>.*
- *The High BRC battery thermal runaway assessment test (verification 4.3.5.2.6C) must demonstrate that no propagation can be substantiated using the following criteria:*

Fully Successful is when all the following exist:

- *No Thermal Runaway (TR) propagation to other battery cells.*
- *No indication of thermal damage to adjacent cells (e.g., no soft short, no opening of a Current Interruption Device (CID), no seal failure, no venting of ejecta or gas).*
- *All adjacent battery cells have nominal electrical performance after the TR test.*

Marginally Successful is when TR propagation does not occur, but there is an indication of off-nominal adjacent cell performance post-test or thermal damage to adjacent cells (e.g., soft short, CID opening, seal failure, or venting occur) that would not result in any escape of flames, sparks, or ejecta outside of the battery enclosure that could potentially damage other non-battery spacecraft systems or hardware.

Initial Battery TR Tests:

- *Minimum of three full-scale battery tests are performed.*
- *Each demonstrates to be “fully successful” for the battery design.*
- *Each test introduces a single-cell TR condition using a “TR Trigger Cell” to demonstrate adequate battery performance and propagation resistance.*

Marginally Successful Follow-on Battery TR Tests:

- *Performed if any of the initial full-scale battery TR tests are not fully-successful but are considered “marginally successful.”*
- *Minimum of six consecutive full-scale battery TR tests are performed which may include the initial battery TR tests.*
- *Each demonstrates to be “marginally successful.”*

Full-scale Battery Test Stipulations:

- *Must place the TR Trigger Cell in a location that exposes a different set of cells to the TR condition. For example, an 8 cell banks that are configured together in series, with each bank containing 10 cells wired together in a parallel configuration. Therefore, each of the 3 (or 6) full-scale tests would locate the TR Trigger Cell in a different cell bank so that each test exposes the remaining 9 cells in parallel in that bank to the TR Trigger Cell.*
- *A single full-scale battery test article may be used for each of the 3 (or 6) battery tests, with battery inspection, cleaning and refurbishment to occur after each test.*
- *No need to replace the spent/destroyed TR Trigger Cell in between tests.*
- *Need to replace or repair any flame arresting features and remove any debris that could soft-short cells in order to restore the remaining battery cell banks to valid conditions for the next TR test.*

A battery design that results in the first 3 full-scale battery tests being declared or the first 6 full-scale battery tests being declared fully or marginally successful,

SSP 51721
Baseline

as described above, is considered sufficient to meet the intent of verification 4.3.5.2.6C.

D.4.3.6.1 Rationale - Electrolytic Capacitors

Containment can be compromised when the internal pressure of the capacitor rises due to internal heat. The pressure rise can be due to a number of production and application causes.

In the case of aluminum electrolytic capacitors, production causes include:

- *Burrs or other small metal particles on the edge of the aluminum foil*
- *A weak point on the electrolytic paper*
- *A defective oxide layer*
- *Insufficient sealing*
- *Application causes of both common types of electrolytic capacitors already mentioned include:*
- *Application of over-voltage*
- *Severe mechanical stress*
- *Excessive ripple current flow*
- *Application of reverse voltage*
- *Severe electrical stress*
- *Excessive charge/discharge*
- *Deterioration of sealing materials*
- *Excessive ambient temperatures*

UHRs for capacitors should use ISS Hazards System (IHS) Template # 33029.

The toxicity hazards for capacitors are based on considerations of liquid electrolyte contacting the eyes or skin. Section 4.7.2 requires that any chemical release that would create a toxicity hazard be contained. The information provided here considers the main risk factors that affect the likelihood of crew contact in order to balance the risk to the crew with costs of precluding electrolyte releases. Factors considered include screening for capacitors likely to leak, number of parallel capacitors, volumetric size of capacitance, and overall assembly configurations that make crew contact with electrolyte unlikely. As a result of these risk factor considerations, there are several possible options for end items to utilize in order to fly hardware containing electrolytic capacitors with reasonable risk levels. Those options are summarized below.

Constraints to Electrolytic Capacitor Usage

Several practical constraints exist with respect to capacitor electrolyte leakage on orbit. While these constraints do not absolutely preclude the release of electrolyte into the

SSP 51721

Baseline

cabin, they do make crew contact with the electrolyte extremely remote and therefore reduces crew risks to acceptable levels.

The preferred approach is that the proper levels of containment are provided based on hazard severity for any toxic materials (i.e., three levels of containment for catastrophic hazards, two levels for critical hazards). However, this is not always attainable, especially for COTS items. In those cases, a DFMR approach is recommended once a THL is determined via a Hazardous Materials Summary Table (HMST). If a toxicity assessment is not obtained (e.g., when materials details are unavailable or proprietary), the capacitors are declared a default THL 2.

DFMR Criteria

The presence of an enclosure vent and the volume of the largest wet electrolytic capacitor both determine the verification requirements. System-level capacitor-screening testing at room/lab ambient conditions serves as a verification for Medium and High CRC hardware. Medium and High CRC hardware that receive DC power from the ISS power bus is verified at worse case power quality levels as specified in the applicable requirements document [8]. Thirty-two (32) [VDC] is applied during the capacitor-screening testing to hardware that will receive power from the 28 [VDC] ISS bus. Similarly, 126 [VDC] is applied during the capacitor-screening testing to hardware that will receive power from the 120 [VDC] ISS bus [8]. For hardware that accepts AC input, use of wall power (120 [VAC] at 60 [Hz]) is acceptable during capacitor-screening testing.

High CRC Hardware is subjected to 100 hours of capacitor-screening testing; however, the duration of capacitor-screening testing can be reduced to 20 hours if the design is verified to be proper using the information listed in Table 4.3.6-1. Post capacitor-screening functional test is defined in Table D.4.3.6.1-1.

The time requirement for capacitor-screening testing can be cumulative. However, a minimum of 3 hours of the total capacitor-screening testing is conducted continuously. In other words, power is applied continuously for a minimum of 3 hours without interruption. The capacitor-screening procedure should be representative of the hardware's on-orbit concept of operations as defined by the End-Item provider. A minimum of five power on/off cycles are conducted.

Regardless of Risk Classification, providers are highly encouraged to use best design practices as provided by capacitor manufacturers such as those found in Nichicon's application guide, "General Description of Aluminum Electrolytic Capacitors" (<http://www.nichicon.co.jp>, Nichicon Corporation, www.nichicon.co.jp/english/products/pdf/aluminum.pdf).

Some examples are:

- *Capacitors are adequately de-rated to ensure safe operation within rated values during voltage spikes*
- *Design and inspection to protect the capacitor from:*
 - *reverse polarity*

**SSP 51721
Baseline**

- *overvoltage*
- *excessive ripple current*
- *overheating*
- *Obtaining documentation (e.g., Certificate of Conformance) reflecting adherence to military, commercial, or industrial standards*

Success Criteria for Capacitor-Screening Test and Post Capacitor-Screening Functional Test

In some cases, the capacitors in an End-Item can be visually inspected after capacitor-screening testing. In these cases, the capacitor-screening test and post-functional test verifications are successful if the End-Item’s capacitors have no visible signs of deterioration, such as those listed in Table D.4.3.6.1-1.

In other cases, the capacitors in an End-Item cannot be visually inspected after capacitor-screening testing. In these cases, the End-Item is actively monitored during the test to demonstrate there is no evidence of capacitor failure from the electronic assembly enclosure. Evidence of capacitor failures is listed in Table D.4.3.6.1-1.

Medium and High CRC End-Items successfully perform their various functions after capacitor-screening testing. Low CRC End-Items are not subject to the success criteria in Table D.4.3.6.1-1 but successfully perform their various functions. The functional test procedure for all hardware is subject to Exposed Pallet (EP) review and acceptance.

The inspection should not invalidate any other test or verification. Low CRC End-Items not subject to success criteria in Table D.4.3.6.1.1-1 but successfully perform various functions.

TABLE D.4.3.6.1-1 SUCCESS CRITERIA FOR POST CAPACITOR-SCREENING FUNCTIONAL TEST

For hardware containing capacitors that CAN be inspected:	For hardware containing capacitors that CANNOT be inspected:
1. All capacitors have no visible signs of deterioration: <ul style="list-style-type: none"> • failed seals • activated scores • bulging 2. Nominal operation of hardware post-test	1. No evidence of capacitor failure <ul style="list-style-type: none"> • liquid electrolyte leakage • gas release 2. Nominal operation of hardware post-test

Limited-Life Use of Aluminum Electrolytic Capacitors

AECs need special consideration because they are limited-life components. Two unique limited-life aspects will be addressed. The first relates to shelf or calendar life; the second relates to service life.

SSP 51721

Baseline

The longer that hardware containing AECs is unpowered, the greater the risk of it failing when subsequently powered. The limited-life of AECs is caused by the gradual deterioration of the oxide dielectric. When a capacitor is in use (voltage applied) the dielectric is reforming continuously; however, when the capacitor remains unpowered for extended periods of time, the oxide layer starts to react with the electrolyte, causing an increased leakage current. When subsequently powered, the leakage current may cause a localized short circuit and create a hot spot, which can lead to gas generation and venting of toxic electrolyte. Therefore, End-Items with AECs or unknown capacitors that are High CRCs need to be tracked as limited-life hardware with an unpowered shelf life of one year.

The High CRC End-Item is to be powered on for a minimum of either one continuous hour or two sessions each lasting at least 30 continuous minutes to extend its unpowered shelf life by one year. If the High CRC End-Item is turned on for two sessions each lasting at least 30 minutes, the sessions need to take place within 6 months of one another in order to extend the High CRC End-Item's shelf life by a year from the date of the second session. Off-time continues to accrue cumulatively unless the criteria for extending a High CRC End-Item's shelf life are met.

If High CRC flight hardware containing AECs or unknown capacitors has remained unpowered for greater than one year, the following precautions are recommended when initially powering on said hardware:

- 1. Donning of personal protective equipment (PPE), including safety glasses and gloves.*
- 2. Containing or orienting hardware to prevent potential release of electrolyte external to the enclosure from contacting a crewmember (i.e. enclosure vent(s) oriented away from crew when powering).*

The Failure Rate Curve for AECs follows the commonly known Bathtub Curve. Note that the term failure used in this context refers to all types of failures, including performance failures that are not associated with the release of electrolyte. The reliability of an AEC is generally measured by its life rather than failure rate since the failure mode is typically wear-out. Many factors affect expected life. The most reasonable approximation to use by providers is the Arrhenius theory regarding ambient temperature. For High CRC hardware that is intended to be operated for more than 10,000 cumulative hours, an assessment of capacitor manufacturing data will be performed to determine the safe operational life of the hardware. In particular, the provider is required to know the guaranteed life at a specified temperature. This is then compared to the projected life at the operational temperature using a Life Estimation table. The results of this assessment are used to select an intended operating time that is less than the hardware's projected life.

Capacitor Toxicity Ratings

As stated previously, the number of hazard controls and verifications for the safe use of non-solid/liquid electrolytic capacitors are primarily dependent on the THL classification

SSP 51721

Baseline

as determined by the JSC Toxicology and Environmental Chemistry Group. This section is, therefore, organized around the THL as noted in the HMST.

Toxicity hazard ratings have been established for common types of aluminum electrolytic and wet tantalum electrolytic capacitors. Wet tantalum capacitors that contain caustic sulfuric acid are considered THL-2. Aluminum electrolytic capacitors that contain dimethylformamide or gamma-butyrolactone, a conservative THL-2 is assigned. Aluminum electrolytic capacitors that contain ammonium or other common salts and only ethylene glycol (i.e., no solvent mixture) are considered THL-1. These hazard levels are based on considerations of the liquid contacting the eyes and/or skin. The vapor hazard will typically not exceed the hazard from the liquid electrolyte.

D.4.3.6.2.2 Rationale – Medium/High Risk Electrochemical Capacitors

Medium risk ECs are typically manufactured in high volumes for the consumer and have commonly available means to help determine the reliability and safety of the products. Due to the consequence of a failure, these end items will follow a comprehensive test and validation plan taking into consideration the worst-case relevant flight environments.

High Risk ECs are typically custom, high energy, or high power designs. Due to the extreme consequence of a failure, these end items will follow a comprehensive test and validation plan that includes testing to determine the result of single EC thermal runaway. The analysis of the thermal runaway can lead to a redesign of the EC assembly to mitigate the consequence.

End item is designed to take into consideration the characteristics of the EC. To characterize the EC to be used in the design, end item providers conduct an engineering evaluation to determine the prospective EC's performance and safety under abuse conditions. Based on this evaluation, manufacturer's specifications must be confirmed to ensure the EC design can handle unique requirements that are relevant to the project.

D.4.3.7.1 Rationale - Electromagnetic Effects

EME includes such areas as EMI, ESD, corona, electrical grounding, electrical bonding, and RF compatibility. EME compliance relies on ISS or equivalent specification verification activities. All end items are required to comply with the electromagnetic compatibility (EMC), EMI, corona, electrical bonding, electrical grounding, RF, and ESD bonding requirements of the IRD or equivalent specification (e.g., SSP 57000, SSP 57003, SSP 50808, SSP 50835, SSP 50005) to protect the vehicle and crew. IRD conducted and radiated susceptibility (RS), as well as ESD immunity requirements are applicable to end items containing safety critical circuits. Evaluation of the end item for determination of safety critical circuits is the purview of the ISRP or its designee (e.g., ISS Electromagnetic Effects Panel (EMEP), ISS Frequency Spectrum Management).

EME Concerns

EME is concerned with the unintentional generation, propagation and reception of electromagnetic energy which could cause hazards related to:

SSP 51721

Baseline

- *Physical damage in end item.*
- *Malfunctions due to surges, ripples, or other conditions.*
- *Degradation and undesired responses from safety critical circuits.*
- *Inadvertent action/failure of safety critical circuits.*
- *Safety Critical Circuits.*

With respect to EME, safety critical circuits are:

- *Circuits whose loss of function due to Electromagnetic Effects (EME) could result in a critical or catastrophic hazard or,*
- *Circuits whose malfunction or degradation of performance because of EME could result in a critical or catastrophic hazard or,*
- *Circuits that control inhibits whose loss due to EME could result in critical or catastrophic hazards.*

EME Applicability

EME requirements are imposed at end item, sub-system, and system level in an effort to achieve vehicle EMC. EMC denotes the electromagnetically compatible simultaneous operation of different equipment, as an ensemble, together with the electromagnetic environment within which operations expected to take place. Normally, an EMC test would be performed at the highest level of integration possible. End items developed, including most payloads, are not integrated with complementing interfaces until installed on orbit. Achieving EMC is heavily reliant on lower level verifications.

ISS EMEP

In the event end items do not show successful compliance with EME ISS equivalent specifications, it is the responsibility of the end item provider to present a HR to the ISRP to define alternate controls to prevent the hazard. The ISS EMEP has been delegated the authority to approve the disposition of EME exceptions via Tailoring Interpretation Agreements (TIAs). Based on technical review and justification of the exception, the EMEP can decide if the exception(s) is acceptable to the ISSP or recommend the exception be corrected. A UHR may be required when TIAs include unique hazard controls (e.g., operational controls).

EME and the ISRP

The ISRP will require UHRs to address:

- *Impacts to safety critical circuits safety margins.*
- *Operational controls to preclude EME hazards.*
- *RF transmissions that are a safety concern to ISS.*
- *ISS environment interactions from end item spacecraft charging with the plasma environment.*

SSP 51721

Baseline

- *Unique electrical shock hazard controls.*

Requirement Exceptions

If the ISRP determines that any ISS specification exception creates a critical or catastrophic hazard, the end item provider will be required to present an HR to the ISRP to define controls and verifications to prevent the EME hazard. In instances where the end item does not meet the ISS or equivalent specifications, IHS templates are available.

Emissions and Susceptibility

Traditionally, EMI control has been levied by NASA programs at the Line Replaceable Unit or ORU level via tailored versions of documents such as MIL-STD-461, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment. For EMI to occur, a culprit (or emitter unit), a victim (susceptible unit), and a coupling path exists. When the operation of one equipment interferes with the operation of another, and the interaction is traced to the transfer of electromagnetic energy from the culprit equipment to the victim, it is termed EMI. EMI is quantified and controlled in four categories: Conducted Emissions (CE), Conducted Susceptibility (CS), Radiated Emissions (RE), and RS.

Conducted Emissions and Susceptibility

In CE/CS interactions, the primary coupling path is via power cabling, but secondary paths could exist in the common reference, or ground plane. Noise voltages and currents on equipment enclosures and attached cabling can couple to victims via cable-to-cable coupling, (also known as cross-talk). Cross-talk is a form of near-field RE/susceptibility that is not directly controlled by traditional RE or RS measurement techniques.

ISS EMC cable/wire design and control requirements incorporate appropriate techniques for cross-talk control. Conducted susceptibilities occur due to power bus or common reference CE (Conducted Emissions) creating noise voltages that upset operations of equipment attached to the power bus.

Radiated Emissions

Traditional radiated electric field emissions measurements are designed to protect sensitive antenna-connected RF receivers, and do so by measuring electric fields that could be directly or indirectly radiated into receiver antennas. RE contributions to victims could also be caused by time varying and static magnetic fields. As with cross-talk, these are near-field measurements, but their control has been incorporated into SSP 30237, Space Station Electromagnetic Emission and Susceptibility Requirements, and related specifications and IRDs. JSC 28918, EVA Design Requirements and Considerations also defines requirements associated with DC magnetic field limits for EMU and /or associated EVA tools.

Radiated Susceptibility

Traditional radiated electric field susceptibility testing is designed to protect hardware from antenna-connected intentional RF emitters. Radiated electric field susceptibilities occur when intentionally transmitted RF power is intercepted by equipment wiring and circuits causing improper operation. Susceptibility testing is required for hardware that contains safety critical circuits as agreed to by the ISS EMEP and ISRP.

Electrostatic Discharge

EPCE ESD susceptibility requirements are contained in ISS or equivalent specifications. When requirement compliance cannot be verified using ISS or equivalent specifications verification methods, HRs may be required to document alternate controls and verifications. An ESD event is the transfer of electrostatic charge between objects at different potentials caused by direct contact or induced by an electrostatic field. ESD immunity requirements are only applicable to end items that contain safety critical circuits. Class S bonding is also necessary for MLI and other objects with large surface areas to protect ISS crew from ESD.

Corona

Corona requirements are contained in ISS or equivalent specifications. When requirement compliance cannot be verified using ISS or equivalent specifications verification methods, HRs may be required to document alternate controls and verifications. In most cases, corona may not be a safety concern when equipment is unpowered and/or equipment power is <190V. Corona is a discharge due to ionization of the gas surrounding a conductor around which exists a voltage gradient exceeding a certain critical value. Corona is undesirable because it consumes power and deteriorates dielectric materials within its vicinity. It could also create EMI. Corona design requirements are applicable to end items with any voltage capability above 190 V. Corona is strongly dependent on atmospheric pressure, atmospheric gaseous content, and electrode spacing. A review of the hardware design and its expected operation is generally required to determine whether corona is a concern.

D.4.3.7.2 Rationale – Protecting Against Hazardous RF Irradiation

RF Transmissions Hazards

RF transmissions hazards include intentional RF transmissions during ISS operations and/or unintentional RF transmissions not planned while in close proximity to ISS (e.g. cubesats). RF EME requirements are imposed at end item, sub-system, and system level to achieve ISS EMC. RF emitters are required to meet IRD or equivalent specifications to ensure ISS compatibility. NASA maintains the responsibility of ISS system level analyses. This NASA integration review helps to identify when RF transmitters potentially degrade ISS system capabilities or requires additional methods to attenuate RF signals. The ISS EMEP assesses EMC compatibility margins to discern whether RF transmitters are compliant with ISS interface requirements. NASA's JSC Spectrum Management Group reviews and approves all transmitters to ensure non-

SSP 51721
Baseline

interference with important frequencies in accordance with IRD or equivalent specifications.

Intentional Transmitters

Intentional RF transmissions can result in circuit degradation, damage, malfunction, inadvertent operations of ISS safety critical systems, crew contact hazards, or hazards to ISS EMU. Intentional RF levels are to be defined for worst case RF output without attenuation or firmware/software controls that limit transmitter power to a level lower.

Intentional Transmitters RF Hazards

Hazards related to RF can be specific to location and use dependent. The provider is required to provide a HR to the ISRP to define controls and verifications when intentional RF is a critical or catastrophic hazard. End Items are required to provide documentation of independent inhibits, controls, monitors, or design features that preclude transmissions when intentional RF transmitters are a hazard to the ISS, Crew, or EMU.

Intentional RF Transmissions during ISS Operations – Inhibits

When there are ISS compatibility concerns with end item RF and ISS critical items (including Visiting Vehicle systems while in free flight near ISS), NASA may require end item controls to prevent RF emission levels. Inhibits only require monitoring when RF radiation exceeds IRD or equivalent specification limits by more than 6db. The 6db is derived from SSP 30243 (3.2.3) - Electromagnetic Interference Safety Margins for critical Circuits. At least one inhibit is required to be interrupted in the circuit return path for End Items controlled by DC circuits.

Intentional RF Transmissions during ISS Operations – No DC Circuits

For End Items that control hazards by means other than DC circuits, (e.g., RF systems or pulse driven motor operations), it is necessary that the end item design includes protection to prevent single events/failures that bypass or remove more than one inhibit to a hazardous function. Inhibits are not required when design solutions are provided to mitigate or contain harmful RF transmissions. (e.g., no physical connection to the transmitter power source, no direct line of sight, RF constrained by point source, containment).

Intentional RF Transmissions during ISS Operations – RF, Frequency Spectrum Management, and EME Compatibility

NASA review of RF frequency spectrum and ISS compatibility is required per IRD or equivalent specifications. When NASA determines that frequency spectrum and/or other ISS compatibility concerns exist due to End Item intentional RF, hazard report operational controls or additional design controls may be required to document inhibit RF emission levels when there are ISS critical items or EMU in vicinity.

SSP 51721
Baseline

Intentional RF Transmissions during ISS Operations – RF and Keep Out Zones (KOZs)

NASA Frequency Spectrum Management relies on understanding of End Item RF effective Isotropic radiated power (EIRP) and frequency data. This data is used by NASA Frequency Spectrum Management to compute the Keep Out Zone (KOZ) distances. Not all KOZs are required based on hazards. KOZs (based on flight rules) may be implemented to ensure RF compatibility or preclude disruptions to communication. Interference with noncritical systems is not considered a hazard. KOZ are defined primarily for extravehicular activity (EVA) or extravehicular robotics (EVR) activities. When there are existing End Items or Visiting Vehicles inside a KOZ, hazard controls may be necessary to mitigate the RF hazard (e.g., mechanical stop, place RF source in another location).

Intentional RF Transmissions during ISS Operations – RF during Transportation to ISS (Launch to Proximity Operations)

Intentional RF transmissions are permitted only for critical ISS mission proximity operations. All other intentional RF transmissions are prohibited during transport to ISS (no transmitting equipment connected to an electrical power source). The JSC Transportation Working Group approval is necessary for battery powered transmitters radiating during transport.

D.4.3.8.1 Rationale – Protecting Against Hazardous RF Irradiation

D.4.3.8.1.a - Radio Frequency (RF) Compatibility

RF compatibility is concerned with intentional generation, propagation and reception of electromagnetic energy. This RF energy can potentially result in circuit degradation, damage, malfunction, inadvertent operations of ISS safety critical systems, crew contact hazards, or hazards to ISS EMU.

D.4.3.8.1.b - RF and ISS Hazards

RF transmissions hazards include intentional or unintentional RF transmissions during ISS IVA operations or intentional or unintentional RF transmissions not planned while in close proximity to ISS (e.g. cubesats). RF compatibility compliance relies ISS or equivalent specification verification activities. All end items are required to comply with RF requirements of the ISS (or equivalent) specification (e.g. SSP 57000, SSP 57003, SSP 50808, SSP 50835, SSP 50005) to protect the vehicle and crew. RF EME requirements are imposed at end item, sub-system, and system level to achieve ISS EMC. In the event end items do not show successful compliance with ISS equivalent ISS specifications, it is the responsibility of the end item provider to present a HR to the ISRP to define alternate controls to prevent the hazard.

D.4.3.8.1.c – RF and Crew Contact hazards

Intentional RF transmissions can result in crew contact hazards. NASA Human Health & Performance (HH&P) Space Radiation Analysis Group (SRAG) utilizes IEEE 95.1 (2005) -IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz to evaluate RF transmitter crew hazards. The HHP SRAG evaluation includes review of RF frequencies to determine aversive/painful electrostimulation due to excessive RF internal electric fields, RF shocks/or burns due to contact with excessively high RF voltages, heating pain/tissue burns due to excessive localized RF exposure and behavioral disruption due to heat exhaustion/heat stroke due to excessive

SSP 51721 Baseline

whole body RF exposure. It is necessary that RF emitters meet the Non-Ionizing Radiation (NIR) exposure requirements for crew protection as specified in SSP 50005 Rev. G (Section 5.7.3.2.1). When RE-02 violation is > physiological levels in 50005, a UHR with controls approved by ISRP is required. Controls may include KOZs and/or Inhibits. End Items can request access via NAMS to a NASA HH&P SRAG RF Hazard Assessment Calculation Tool to determine whether unique controls are necessary to protect the crew from intentional RF hazards crew contact hazards.

D.4.3.8.1.d – Passband Frequency

The passband frequency is the **bandwidth which a modulated RF signal needs to transmit information without attenuation**. In other words, RF levels are defined by worst case RF output without attenuation or firmware/software controls that limit transmitter power to a level lower. For example, the bandwidth of a TDRS spread spectrum signal is center frequency +/- 3 MHz for a total of 6 MHz. In an EMI test, the bandwidth which an intentional transmitter is designed to operate is not limited to the radiated emissions limits.

D.4.3.8.1.e – RF and NASA Responsibility

NASA maintains the responsibility of ISS system level analyses. This NASA integration review helps to identify when RF transmitters potentially degrade ISS system capabilities or requires additional methods to attenuate RF signals.

- **ISS EMEP**

Assesses EMC compatibility margins to discern whether RF transmitters are compliant with ISS interface requirements. When RE-02 violations occur in a frequency band used by ISS Communication Systems resulting in loss of communications capability which results in a hazardous condition (as determined by the ISRP), an UHR is required to ensure control is implemented to mitigate the hazard.

- **NASA Frequency Spectrum Management (FSM)**

End items (operational and deployable) with Intentional RF transmissions are required to meet FCC, National Telecommunication and Information Administration (NTIA), and/or International Telecommunication Union (ITU) requirements for frequency uses and obtain transmit operations licenses for space operation. JSC Spectrum Management is responsible for assessing the end item to ensure the appropriate requirements are met. For End items that do not meet the spectrum requirements, either modification, operational controls, and/or design controls are necessary to become compliant with FCC, NTIA, and/or ITU requirements. End items may be prohibited from launching to the ISS if spectrum management requirements are not met. The spectrum management requirements is independent from identification of critical or catastrophic hazards.

NASA FSM also conducts safety and operational compatibility assessment for systems destined for the ISS (operation or deployment) with radio frequency capability. RF hazard/keepout zone and radio frequency compatibility analysis are the key products of this assessment. For exceedances in Radiated Emissions requirements, a detailed analysis by the ISS Spectrum Management is required to determine whether additional controls may be required to protect ISS intentional receivers resulting in a hazardous condition. Analysis at the early phases of the design provide NASA FSM insight into whether controls (e.g. KOZ, inhibits) are necessary to ensure protection of ISS systems as defined in ISS or equivalent specifications. When NASA

SSP 51721 Baseline

FSM determines that frequency spectrum and/or other ISS compatibility concerns exist due to End Item intentional RF, end item operational or design controls may be necessary to inhibit RF emissions considered a critical or catastrophic hazard.

- **NASA Human Health and Performance (HH&P)**

RF transmitters can pose a hazard to the IVA or EVA crewmembers. NASA review by HHP is conducted on all RF transmitters to help ensure crew safety and provides feedback to the ISRP. It is necessary that RF emitters meet the Non-Ionizing Radiation (NIR) exposure requirements for crew protection as specified in SSP 50005 Rev. G (Section 5.7.3.2.1). When RE-02 violation is > physiological levels in SSP 50005, a UHR with controls approved by ISRP is required. Controls may include KOZs and/or Inhibits.

D.4.3.8.1.f EMEP Tailoring/Interpretation Agreement (TIA)

The ISS EMEP is delegated the authority to approve the disposition of ISS specification exceptions via Tailoring /Interpretation Agreements TIAs. Based on technical review and justification of the exception, the EMEP can decide if the exception(s) is acceptable to the ISSP or recommend the exception be corrected. A UHR may be required when TIAs include unique hazard controls (e.g., operational controls or inhibits).

D.4.3.8.1.g Intentional Transmitters - RF Hazards - General

Hazards related to RF can be specific to location and use dependent. The provider is required to provide a HR to the ISRP to define controls and verifications when intentional RF is a critical or catastrophic hazard. End Items are required to provide documentation of independent inhibits, controls, monitors, or design features that preclude transmissions when intentional RF transmitters are a hazard to the ISS, Crew, or EMU.

D.4.3.8.1.h Intentional RF Transmissions during ISS Operations – Inhibits

When there are ISS compatibility concerns with end item RF and ISS critical items (including Visiting Vehicle systems while in free flight near ISS), NASA may require end item controls to prevent RF emission levels. Inhibits require monitoring when RF radiation exceeds ½ of ISS or equivalent specification limit. Inhibits only require monitoring when RF radiation exceeds ISS equivalent specification limits by more than 6db. The 6db is derived from SSP 30243 (3.2.3) - Electromagnetic Interference Safety Margins for critical Circuits. At least one inhibit is required to be interrupted in the circuit return path for End Items controlled by DC circuits. . At least one inhibit is required to be interrupted in the circuit return path for End Items controlled by DC circuits.

D.4.3.8.1.i Intentional RF Transmissions during ISS Operations – Transmitters with No DC Circuits

For End Items that control hazards by means other than DC circuits, (e.g., RF systems or pulse driven motor operations), it is necessary that the end item design includes protection to prevent single events/failures that bypass or remove more than one inhibit to a hazardous function. Inhibits are not required when design solutions are provided to mitigate or contain harmful RF transmissions. (e.g. no physical connection to the transmitter power source, no direct line of sight, RF constrained by point source, containment).

SSP 51721
Baseline

D.4.3.8.1.j Intentional RF Transmissions during ISS Operations – RF and Keep Out Zones (KOZs)

Not all KOZs are required based on hazards. Interference with noncritical systems is not considered a hazard. KOZs (based on flight rules) may be implemented to ensure RF compatibility or preclude disruptions to communication.

End Item RF effective Isotropic radiated power (EIRP), operating frequency, antenna characteristics and specific operation locations are essential to support radio frequency hazard and operational compatibility of each end item. This data is used by NASA FSM to compute KOZ distances and to assess potential interference between intentional RF systems.

KOZ are defined primarily for extravehicular activity (EVA) or extravehicular robotics (EVR) activities. KOZs may be required based on hazards but may also be implemented to ensure RF compatibility or preclude disruptions to communication based on Flight Operations requirements.

D.4.3.8.1.k Intentional RF Transmissions during ISS Operations – RF during Transportation to ISS (Launch to Proximity Operations)

Intentional RF transmissions are permitted only for critical ISS mission proximity operations. All other intentional RF transmissions are prohibited during transport to ISS (no transmitting equipment connected to an electrical power source). The JSC Transportation Working Group approval is necessary for battery powered transmitters radiating during transport.

D.4.3.8.1.l Deployable end items that contain intentional RF radiating devices

Deployable end items that contain intentional RF radiating devices and maintain frequency, radiated susceptibility, and power densities below the levels in Tables 4.3.8.1-1 while in the pressurized volume of the ISS are not considered a threat to ISS. This includes inadvertent activation of the deployable end item RF emitter.

D.4.4.1 Rationale – Computer Based Control System

CBCS Applications

End items are encouraged to consider hardware design approaches such as failure tolerance or DFMR rather than use of CBCS as control without computer control rather than use of CBCS as controls to a hazard. When computers or electronic devices (such as FPGAs, etc.) are used to partially or fully control a critical or catastrophic hazard, analysis and/or test of the CBCS or electronic device is necessary to demonstrate that function is not degraded as a result of transport and operational environment (natural and induced). CBCS requirement categories include General, Must Work Function (MWF), and Must Not Work Function (MNWF). Unpowered CBCS may be exempt from SSP 50038 review when failure tolerance is provided to keep the system unpowered.

CBCS General Requirements

It is necessary to meet the CBCS General Requirements for items with other non-CBCS devices (e.g., switches, RPCs) controlling the remaining devices to meet fault tolerance levels. This is because the general CBCS requirements provide the necessary verification activity that hazard control functions as intended.

SSP 51721
Baseline

CBCS Must Work Function Requirements

MWFs are functions that are necessary to be executed successfully to prevent a hazard. MWF provide fault tolerance against inadvertent deactivation.

CBCS Must Not Work Function Requirements

A MNWF is a function which if performed inadvertently results in a hazard. Utilizing MNWF Fault Containment (FC) or Control Path Separation (CPS) approach protects against inadvertent activation of a MNWF.

D.4.4.2.1 Rationale – On-Board Computer Systems

Computer Based Control System - CBCS Applications

End items are encouraged to consider hardware design approaches such as failure tolerance or DFMR rather than use of CBCS as control without computer control rather than use of CBCS as controls of hazards. CBCS requirement categories include General, Must Work Function (MWF), and Must Not Work Function (MNWF). Unpowered CBCS may be exempt from SSP 50038 review when failure tolerance is provided to keep the system unpowered.

CBCS General Requirements

In the event that a CBCS is only controlling one level of hazard control with other non-CBCS devices (e.g. switches, RPCs) controlling the remaining devices to meet fault tolerance levels, it is necessary that the single CBCS control meet CBCS General Requirements.

In other words, controlling one inhibit does not constitute complete control of a hazard. CBCS systems that do not control multiple inhibits (no more than 1 inhibit) should be considered to meet appropriate fault tolerance since failure of the CBCS can be considered only 1 failure.

Unpowered CBCS (even if the CBCS controls all inhibits) should be exempt from SSP 50038 review, fault tolerance to keep the system unpowered may be required.

CBCS Must Work Function Requirements

MWFs are functions that are necessary to be executed successfully to prevent a hazard. MWF provide fault tolerance against inadvertent deactivation.

CBCS Must Not Work Function Requirements

A MNWF is a function which if performed inadvertently results in a hazard. Utilizing MNWF Fault Containment (FC) or Control Path Separation (CPS) approach protects against inadvertent activation of a MNWF.

On-Board Computer Systems

Crew commanding via the PCS or any computer that connects (hardline or RF) to the 1553 data bus is required to meet the SSP 50038 CBCS requirements. The issuance of a single command cannot result in a hazard or reduction of a hazard control when the

SSP 51721
Baseline

hazard exists. Non-deployable OCS end items which control hazardous functions are subject to SSP 50038 review. Deployables which have fault tolerant controls to prevent activation of computers or complex electronics to ensure that it is not using a CBCS strategy for hazards while at ISS (e.g., it is inactive), do not have to meet the CBCS compliance. MIL-STD-1553, Digital Time Division Command/Response Multiplex Data Bus, is a standard that defines the mechanical, electrical, and functional characteristics of a serial data bus, and is commonly used in spacecraft on-board data handling subsystems. This includes complex electronics systems such as firmware controllers.

D.4.4.2.2.5 Rationale - Ku/LAN and Hazardous Commanding – Command and Data Integrity

D.4.4.2.2.5.a – Replay Resistance

Replay resistance prevents a deliberate or inadvertent recording and replay of a command, which could happen at a time when a hazard is present. Disregarding replay resistance allows recording and replay of a command by deliberate or inadvertent action. To be effective, the replay resistance feature must be protected from alteration (e.g. inside the message content protection).

Message content protection, command source authentication, unique command routing, and file transfer integrity do not typically provide a means to protect against command replay.

D.4.4.2.2.5.b – Message Content Protection

Message content protection protects a command from being altered or disclosed while in transit. Disregarding secure protocols can allow a hostile actor (man-in-the-middle attack) to decipher and then create or modify commands.

Replay resistance, command source authentication, unique command routing, and file transfer integrity do not typically provide a means to protect against unsecure protocols that can present a command hazard.

D.4.4.2.2.5.c – Command Source Authentication

Command source authentication ensures that the command source is recognized by the end-item as legitimate. Without source authentication, the end-item has no knowledge of which connections or sources are truly authentic and allowable. Command Source authentication protects against deliberate or inadvertent accepting commands from a non-authorized source. Disregarding command source authentication can allow deliberate or inadvertent acceptance of a command from an illegitimate source. To be effective, the command source authentication is protected from alteration (e.g. within or as part of the message content protection).

Replay resistance, message content protection, unique command routing, and file transfer integrity do not typically provide a means to completely protect against unauthorized command sources that can present a hazard. The end-item would accept a connection from any end-point, thus creating potential for deliberate or inadvertent hazardous commanding to the end-item.

SSP 51721
Baseline

D.4.4.2.2.5.d – Unique Command Routing

Unique command routing protects against multiple items ‘sharing’ a command path. Since end-items are developed independently, if multiple end-items were to use a broadcast or multicast, there is a potential that a command intended for end-item “A” could also be received and processed as a hazardous command by end-item “B”.

Disregarding unique command routing can allow for multiple end-items receiving and acting upon a single command if the paths are not independent.

Replay resistance, message content protection, command source authentication, and file transfer integrity do not typically provide a means to protect against non-unique command routing that can present a hazard.

D.4.4.2.2.5.e – File Transfer Integrity

File transfer integrity checking ensures that parts of a file transfer are reassembled in correct order with nothing missing. Disregarding file transfer integrity can result in arrival of fragmented files with either missing data or parts of the file in the wrong order.

Although the transfer itself is correct, reassembling the pieces into the file may become erroneous. The resulting bad file could be used by an end-item, thus creating a hazard.

Replay resistance, message content protection, command source authentication, and unique command routing do not typically provide a means to protect against erroneous file transfer that can present a hazard.

D.4.4.2.3 Rationale – Ground Initiated Hazardous Commanding

Ground Initiated Hazardous Commanding – Remote Commanding Centers-General

Verification of remote commanding centers is required when remote commanding is active and a commanding link could be established when a hazard is present to the ISS. The issuance of a single command cannot result in a hazard. All catastrophic hazards are to be protected from a single inadvertent action or single failure causing the hazard.

End items providers that do utilize a NASA approved control center are required to describe the control of the issuance of hazardous commands in a hazard report.

Ground Initiated Hazardous Commanding – Hazard Report

A UHR addressing the commanding assets can be presented with the verifications that describe the following:

- *The requirement to demonstrate approved command paths are in place prevents the risk of inadvertent execution of hazardous commands. NASA’s understanding of the command path architecture is necessary to evaluate failure modes and software errors in determining compliance with the requirements.*
- *Verifications for remote control centers are defined with the assumption that it takes a combination of any three actions or three failures (2 fault tolerant) to cause a catastrophic hazard on the vehicle or at the end item. End item providers may choose to implement independent failure tolerant solutions in place of these remote hazardous commanding requirements.*

D.4.5.2.1 – Monitoring Frequency – RTM - Real-Time Monitoring (RTM) – General

RTM is defined as immediate notification to the crew. When monitoring detects loss of an inhibit to a catastrophic hazard that is not automatically safed, an alert must be implemented via the ISS C&W system. An alert is also required when monitoring detects a potential fire event (parameter monitoring).

Payloads are prohibited from using RTM to maintain control of hazardous functions during reconfiguration. RTM for payloads is prohibited since immediate responses is not possible due to ISS loss of signal, change of state of inhibits, loss of inhibits, or crew availability during payload reconfiguration activities.

Only with ISRP review/approval may payload RTM and hazard detection and safing be considered. Payload RTM can only be considered on an exception basis by the ISRP and may require ISS program risk acceptance. Some considerations for use of RTM may include:

- *Alternate means of reduction or hazard controls are exhausted.*
- *Crew availability allows for monitoring and response time to detect and safe the system.*
- *Safing procedures are developed and approved.*
- *Monitoring functions are capable of being tested for proper operations during both ground and flight phases and*
- *Payloads verify that monitoring is properly incorporated into the ISS systems for fault detection and annunciation.*

RTM - Ground Monitoring

Ground monitoring is prohibited for RTM since maintaining a continuous real-time data link between the flight and ground crews (containing the applicable safety parameters) cannot be ensured during the required period.

RTM - ISS Caution and Warning System

The C&W System is designed to alert the crew to off-nominal situations. The following are the classifications of alerts.

- *Class 1: Emergency – used to indicate a life threatening condition that requires all crew to react immediately. This includes fire, rapid cabin depressurization or toxic release.*
- *Class 2: Warning – used to signal a potential fire event, a precursor event that could manifest to an emergency condition, or loss of a hazard control that is not automatically safed. Warnings are used for events that require manual intervention and for notification when automatic safing fails.*
- *Class 3: Caution – used to indicate a precursor event that could manifest to an emergency condition or loss of a hazard control that was automatically safed. No immediate action is required.*

SSP 51721
Baseline

- *Class 4: Advisory – used for non-emergency situations*
For situations classified as Emergency or Warning, the crew is prime to respond due to the time-critical nature of the situation. The need for hazard detection and safing by the flight crew to control time-critical hazards should be minimized and implemented only when an alternate means of reduction or control of hazardous conditions is not available. C&W requirements at the ISS level are covered in SSP 41000. SSP 41000 includes requirements that ISS will provide system status in the form of alerts, provide facility for alerts, provide the capability to turn off alerts, and activate Emergency alerts for fire event and rapid decompression. The ISS allows for a hazardous atmosphere alert to be annunciated although it requires manual activation. The requirements for the use of the C&W system by integrated racks and end items for fire detection and parameter monitoring is covered in the associated IRDs (e.g. SSP 57000).

Conditions that constitute a warning as defined above must be monitored using RTM. If the loss of a control for a catastrophic hazard is possible, monitoring must be implemented and automatic detection and annunciation must be incorporated in the hardware design. Upon annunciation of the Warning, at least one crewmember will respond to safe the system. The ISRP will dictate when monitoring is required based on hazard severity and control strategy, but requirements for the implementation of the C&W system for Warning conditions is covered in the IRDs. The IRD addresses the use of Warning alerts for subrack fire detection via parameter monitoring when the subrack volume does not exchange air with the rack smoke detector. The IRD also covers other uses of the Warning and Caution alerts as mentioned above.

FDIR is performed by on-board automated systems (including VV CBCS) that initiate programmed responses to identified failures. FDIR is normally used for actively safed systems that meet CBCS requirements. (Section 4.4.1.1 – Computer Based Control Systems).

FDIR is not allowed for payloads or MNW functions, or to provide controls for safe without services.

D.4.5.2.2 – Rationale -Monitoring Frequency - Near Real Time Monitoring

NRTM is defined as notification of changes in inhibit or safety status on a periodic basis. Periodic monitoring every 90 minutes allows for review of the inhibit status once per orbit. NRTM is normally used for MNW systems and redundant MW systems with long TTEs. NRTM can be accomplished via monitored telemetry data via ground control center, or crew monitoring.

Ground crew monitored telemetry data is acceptable since it is not necessary to maintain a continuous real-time data link between the flight and ground crews. Local visual indicators will not be used as the only source of safety monitoring unless the crew is actively engaged in operations at the visual indicator location.

Prerequisite Monitoring

Prerequisite monitoring is defined as monitoring required to confirm inhibits and controls are in place before a hazardous procedure is implemented. Prerequisite monitoring is used for situations that are only hazardous for a short time in comparison to the duration of an ISS mission (e.g., prior to connector mate/demate). When prerequisite monitoring is used, once the inhibit is established and confirmed, it does not need to be continuously monitored since the inhibit is considered to be in a safe state. Prerequisite monitoring may also be used for must work systems that do not have a catastrophic hazard potential. When hazard TTE is >90 minutes either RTM or NRTM is acceptable.

D.4.5.2.3 – Monitoring Frequency – When Inhibit Monitoring is not Required

End item inhibits used to protect against a hazardous function with no monitoring capability will ensure that inhibits between the power source and the hazardous function are de-energized during the timeframe that the hazard is present. Hazard severity determines the number of inhibits required to control the hazard. The inhibit can either be provided by the end item or by other upstream ISS resources.

This requirement is specific to end items that demonstrate inhibits are susceptible only to hardware failures. Verification testing is normally used for inactive redundant systems and for safety devices that only need to function when a hazard is present.

Due to the uncertainty of the true state of the unmonitored inhibits and controls, the ISRP may require action be taken to minimize risk of it changing state if other inhibit(s) to the same function are lost. Monitoring is generally not required for critical level hazards. The ISRP may require monitoring to minimize the risk of critical level hazards. (e.g., 0-fault tolerant to hazards - IVA crew thermal extremes, removal of containment levels during planned science activities, hazards during maintenance).

Monitoring is not required when:

- Unpowered Bus Exception - Four inhibits are in place to isolate power from the hazardous function and are certified for the worst case induced environment (e.g. launch and on-orbit environments - shock, vibration, and thermal loads). One of the inhibits must isolate the power between the source and other three inhibits.*

OR

- Three inhibits are provided when the End Item is only susceptible to hardware failures and inhibits cannot be bypassed by control centers, computers, or crew intervention.*

OR

- Confirmation of inhibits is completed after on-orbit preparations or planned ISS reconfiguration activities. A nominal inhibit state change can result when moving an end item from temporary stowage to final installation (e.g., contact switches at end item interface to deployer-CYCLOPS). Reverification of the inhibit(s) status after a change in state ensures that the inhibit is in place before the planned activities.*

D.4.6.2.1 Rationale – Ionizing Radiation

Single Event Effects (SEE) and Total Ionizing Dose (TID)

The ionizing radiation environment consists primarily of high kinetic energy charged particles many of which can induce Single Event Effects (SEE) and Total Ionizing Dose (TID) in electronics. SEE and TID can change electrical state or characteristics of an electronic device thereby creating a hazard. SEE normally occurs randomly, but will occur at an increased rate during intense solar flares (Solar Particle Events) that follow release of high energy protons and heavy ions from the Sun. These events occur infrequently, but not so infrequently as to disregard the impact to ISS (reference SSP 30512, Space Station Ionizing Radiation Design Environment, Sections 3.1.2 and 3.2.2). TID effects can slowly degrade end item performance over time as determined by dose rate and end item TID sensitivity. The rate of SEE effects normally occur randomly on the timeline at a rate that depends on the environment severity, solar activity, and end item SEE sensitivity.

Crew Exposure to Ionizing Radiation

ISS space modules protect ISS IVA crew from ionizing radiation. Current measurements indicate that the maximum dose for any location in the USOS is less than 40 Roentgen Equivalent Man (rem) Blood Forming Organs per year which is below the federal guideline for exposure.

The JSC Space Radiation Analysis Group (SRAG) assesses crew ionizing radiation dose limits on a case-by-case basis. These assessments are provided to the ISSP via the Certificate of Flight Readiness process, and determine individual crew radiation doses per NASA STD 3001, NASA Space Flight Human-System Standard. JSC SRAG assessments are based on variables including spacecraft structure, materials, altitude, inclination, status of outer zone electron belts, interplanetary proton flux, geomagnetic field conditions, and solar cycle position.

JSC SRAG review of new spacecraft is necessary to determine whether end item modules exposure to environmental ionizing radiation is a crew ionizing radiation concern. SRAG review is also necessary for end items that generate ionizing radiation to determine whether the end item is a crew ionizing radiation hazard.

When the JSC SRAG determines that end items and operations can result in a crew hazard, it is the responsibility of the end item provider to disclose the concerns to the ISRP. ISRP review of the potential concern could determine that a UHR is required to document additional safety controls to prevent end item ionizing radiation concerns.

Safety Critical Circuits

Safety critical circuits are circuits whose loss of function, malfunction, performance degradation, or inhibit loss can result in critical or catastrophic hazard.

Ionizing radiation can result in hazard control reduction when critical functions are affected by SEE and TID.

SSP 51721

Baseline

Ionizing radiation design and verification environments are described in SSP 30512, Sections 3.1.2, 3.2.1, and 3.2.2 or equivalent environments definitions that meet or exceed SSP-30512 specifications.

Consultation with the ISS Space Environments SPRT is necessary to define the correct ionizing radiation environment. The ISS Space Environments SPRT can also assist in defining alternate TID radiation environments when there are exceptions to SSP 30512 environments.

Radiation Hardened or Multiple Modular Redundancy

End item designs can either utilize radiation hardened electronics (immune to ionizing radiation) or utilize Multiple Modular Redundancy (MMR) to protect safety critical circuits for maximum expected mission duration (i.e. Design Reference Mission (DRM)). MMR is a design architecture that provides functional redundancy (as opposed to microelectronic parts that are immune to SEE). MMR removes common cause failure modes as a result of SEE. Once SEE and TID impacts are identified, failure probability equations are defined for single and multiple module failures. Probability of multiple modules being impacted with SEE faults can be calculated using Poisson statistics based on component sensitivity, shielding mass, and ISS environment variables. ISS Space Environments SPRT review is necessary to evaluate MMR protection for safety critical circuits per SSP 30512 (Sections 3.1.2, 3.2.1 and 3.2.2) when there is critical or catastrophic hazard potential.

D.4.7.1.1 Rationale – Flammable Materials

An end item can not constitute an uncontrolled fire hazard; therefore, all end item materials should be either non-flammable or controlled such that they do not allow fire propagation. Spacecraft fire control is based on minimizing potential ignition sources and eliminating materials that can propagate fire. Controlling the quantity and configuration of flammable materials to eliminate potential fire propagation paths ensures that any fire would be small, localized, isolated, and would self-extinguish without harm to the crew.

End items show compatibility with their intended environment and fulfill this requirement through verifications. Materials are tested or evaluated in the worst-case operating environment for the end item to verify this requirement. The worst-case oxygen environment for ISS is 14.7 psia with 24.1-percent oxygen for all locations except the USOS airlock. The airlock worst-case environment is 10.2 psia with 30-percent oxygen. End items materials should be tested or evaluated in the worst-case airlock environment if they intend to operate in the airlock during EVA preparations.

Materials used outside the pressurized areas should be evaluated for flammability in an air environment at 14.7 psi to account for ground processing hazards.

Flammability Control Strategies

The following flammability control strategies can be used to eliminate many materials fire propagation issues in ISS environments and, when used, are documented in the verifications:

SSP 51721

Baseline

- *All structural metallic materials are nonflammable.*
- *Materials inside sealed, nonflammable containers will not propagate fire, because insufficient oxygen is present to support prolonged combustion.*
- *Materials inside vented, nonflammable containers will not propagate fire (insufficient oxygen is present to support prolonged combustion) unless forced air convection is present. [Materials inside vented, nonflammable containers with forced air convection might not propagate fire, but testing is commonly required to verify.]*
- *Flammable end items (or end items assumed to be flammable) could be acceptable if they are stowed in a nonflammable container (such as a cargo transfer bag) when not in use and under crew control or other specified control when in use. If an item is required to be stowed when not in use due to flammability concerns, an operational control will need to be documented in the appropriate database (e.g., OCAD or PHCM) and on the associated HR. A generic flammability OCAD exists for general use crew equipment, but use of this OCAD is at the discretion of the ISRP. End items with dedicated procedures typically have a unique operational control.*
- *Flammable materials, other than hook and loop fasteners, are acceptable if their dimensions are controlled so the potential fire propagation path is less than 6 linear inches (with a maximum surface area of 12 square inches). External end items, where the potential for fire propagation exists only prior to launch, can have a maximum dimension of 12 linear inches. Note that when multiple flammable materials are adjacent to each other, the total potential fire propagation path needs to be less than these dimensions.*
- *Flammable hook-and-loop fasteners (such as Velcro) can be controlled by limiting the maximum exposed surface area to 4 square inches and the maximum dimension to 4 linear inches and maintaining a separation of 2 linear inches between fasteners.*
- *Flammable end items can be controlled by wrapping in a nonflammable material such as aluminum tape, glass cloth tape or Teflon tape. Fire propagation paths can be controlled by firebreaks fabricated from nonflammable materials such as aluminum tape.*
- *Flammable end items that cannot be controlled by the above constraints might still be acceptable, but more detailed analysis and/or flammability testing is required to verify. JSC 29353, provides additional guidance on the assessment of end items flammability in configuration. NASA-STD-6001 provides guidance on flammability testing.*

Data from literature flammability tests conducted in air (such as UL tests) cannot be used to assess materials flammability in the ISS oxygen-enriched internal environment because materials are more flammable in oxygen-enriched environments than in air. Similarly, data from oxygen-index tests might give an indication of flammability performance in the ISS internal environment, but cannot be used to verify that a material meets flammability requirements.

D.4.7.1.2 Rationale – Material Offgassing in Habitable Areas

This requirement only applies to end items in the ISS pressurized environment. Offgassing is the release of chemicals from materials – the new car smell is an example of material offgassing. Offgassing can result in a toxic atmosphere if chemical compounds accumulate in a spacecraft closed environment and reach concentrations above their Spacecraft Maximum Allowable Concentrations (SMAC). End items are assessed to ensure they do not generate toxic levels of offgassing products into the ISS environment. MAPTIS contains a listing of materials and end items that have been subjected to offgassing tests. The material offgas rating in MAPTIS is based upon the amount of the material that is allowed. If not all major use materials are listed in the MAPTIS database, toxic offgassing testing is normally required.

If the total mass of polymeric materials in an end item, or a system with multiple end items (such as a set of CubeSats with deployer) is less than 20lb, it is exempt from offgas testing or evaluation unless it contains one of the following excluded materials:

- *COTS end items that include uncured adhesives, lubricants, cleaning wipes, markers, pens, other items with uncontained liquids or gels, and hardware used for uncontained on-orbit processing of materials at elevated temperatures (such as 3D printers) are not exempt.*
- *Custom end items that include the materials listed above or foams and foamed fluorocarbons (cables) are not exempt.*

If excluded materials are present or the total mass of polymeric materials exceeds 20 lb, an offgassing test could be required or an offgassing evaluation could be conducted to verify that all excluded materials and major use polymeric materials are used in quantities less than the ISS maximum limit weight in the MAPTIS database.

Materials in a sealed container are not required to be assessed for offgassing if the container remains sealed and is not opened during flight. Acceptable sealed containers include heat-sealed bags and boxes with a single o-ring seal. Verification of seal performance is not required for offgassing acceptance. For pressurized volume hardware delivered to ISS by a crewed vehicle, offgassing evaluation for the crew vehicle volume is not required if the hardware is in a sealed container from launch until hatch opening after docking with ISS. Offgassing evaluation for the ISS volume is still required.

For payloads, NASA M&P can provide assistance to conduct the offgassing evaluation. When assistance is requested, the form titled “Application for Exemption by Analysis for NASA-STD-6001 Test 7 – Determination of Offgassed Products” should be used.

D.4.7.2.1 Rationale – Hazardous Materials External Release Near or Through the ISS

The primary concern for this requirement is the release of hazardous fluids (liquids/gases).

This requirement applies to all end items capable of releasing hazardous materials external to the ISS. This includes externally located end items and VVs and internally located end items utilizing the ISS Vacuum System (VS) (consisting of the Vacuum

SSP 51721
Baseline

Exhaust System/Waste Gas and the Vacuum Resource System/Vacuum Vent). It is established to prevent immediate and/or latent damage (such as soaking into MLI blankets or insulation) from corrosion and/or contamination to the EMU, ISS and/or VV equipment. Release of hazardous material near or through the ISS should also not create a hazard to other externally located end items.

Any planned hazardous material release near or through the ISS should be negotiated with the ISSP. Hazardous fluid systems should prevent the release of fluids unless the venting/dumping has been negotiated with the ISSP.

Control of release of the hazardous materials is provided through failure tolerance or DFMR based on the hazard severity. Hazard severity (reference Section 4.1.1) of externally released end item materials is jointly determined by the NASA/JSC Materials and Processes Branch, the ISS Space Environment Group, and the ISRP based on potential damage (immediate and/or latent) caused by the released materials. For end items utilizing the ISS VS, the hazardous materials are required to be evaluated for both internal and external vehicle release. Chemical release in the ISS pressurized volume is addressed in Section 4.7.2.2, Chemicals and documented on the end item's HMST. Documentation of hazardous materials usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP, reference Section 4.7.2, Hazardous Materials, for details. For many hazardous materials, there will not be an issue with external release of the material in the gas/vapor form as it will not condense and damage hardware.

For negotiated pre-planned release of water vapor or hazardous fluids, the release will be controlled. A venting analysis should be performed to demonstrate that vent effluents are not chemically reactive with ISS surfaces and do not violate contamination control requirements per SSP 30426, Space Station External Contamination Control Requirements. The venting analysis should include vent position, orientation (direction, vector), geometry, effluent composition (including trace substances), mass flow rate, venting frequency and duration. Vent position and orientation should be away from ISS and other end items. Venting of water vapor for thermal control or humidity control purposes is permitted if the water vapor contains no dissolved substances that could violate SSP 30426.

Requirements for the use of the ISS VES are covered in the applicable IRD (SSP 50835, 57000, etc). These requirements include external contamination as defined in SSP 30426. VV also meet the requirements of SSP 30426 per SSP 50808.

Additional details on EMU contamination and propulsion systems are addressed in the Section 4.10.9, Toxic/Corrosive Materials, and in Section 4.12, Propulsion Systems, respectively.

D.4.7.2.2.1 Rationale – Chemical Release

This requirement does not apply to crew food, drinking water from the galley, crew personal preference items, or items considered to be structural components. If any of these items are used in a manner different than what is intended here (such as for

SSP 51721
Baseline

experimental purposes), an evaluation may be requested by the ISRP during the safety review process.

This requirement applies to all chemicals that are located in or may be introduced into the pressurized habitable environment (including end items returning from or routinely used in the unpressurized environment). It is established to protect the crew from chemically-induced hazards and/or to protect the environment and VV/ISS equipment from contamination hazards.

This requirement encompasses all physical states and compositions (for example: solid, liquid, vapor, gas, gel, grease, and powders/particulates) for chemicals and potential products of end item chemical reactions. Radioactive materials are a unique set of chemicals addressed in Section 4.7.2.3, Radioactive Material Release. For particles that are chemically inert and/or insoluble in water, refer to Section 4.7.2.5 for Physical Agents.

End item chemicals will be evaluated and receive a hazard rating for all chemically-induced hazards including toxicity hazards, flammability hazards, and ECLSS impact hazards. The hazard ratings will be collectively documented on the end item's HMST. If the chemical is considered to not be one of the hazards identified here, the associated hazard rating would be marked as "N/A" for Not Applicable on the HMST. Toxicity hazards are chemicals (toxicants) that may be harmful to crewmembers with physiological effects such as irritation to skin or eyes. Flammability hazards are chemicals that may ignite, burn, combust, and/or catch fire resulting in harmful byproducts, decrease in breathable air, and/or equipment damage. ECLSS impact hazards are chemicals that may adversely impact ISS ECLSS hardware resulting in a degraded/compromised ISS pressurized environment (crew living environment) and/or ISS ECLSS hardware damage. Refer to Table 4.7.2-1, Levels of Containment/Control and Hazard Ratings, for the relationship between the hazard ratings. Since chemicals have multiple hazard ratings, the hazard severity for release of the chemical is determined by the highest hazard rating.

Controls to prevent release of chemicals are provided through failure tolerance or DFMR based on the hazard severity, reference Section 4.7.2 for details. All chemicals should maintain a minimum of one control to prevent release (containment or other appropriate controls) at all times. Documentation of chemical usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP.

End Items Returning From or Routinely Used in the Unpressurized Environment: Controls, such as placing the item in a sealed container or allowing for bake off time, are implemented prior to bringing external end items into the pressurized environment.

Toxicity Hazard Level (THL) Hazard Rating

The THL ratings were developed by the NASA SME, the JSC Toxicology and Environmental Chemistry Group, and are unique to the spaceflight, spacecraft, and space exploration environments. The THL is the toxicity hazard that would result if the

SSP 51721
Baseline

chemical was released into the vehicle; it assumes full release and provides expected results of crew exposure without regard to likelihood of escape or exposure.

The following is collectively taken into consideration when assessing end item chemicals and assigning THLs: the chemical's physicochemical properties (physical state and chemical properties of chemical), total quantity, human physiological effects (e.g., irritancy, carcinogenicity, systemic toxicity), and, when appropriate, the rate at which the chemical is removed from the environment/vehicle. The ECLSS Cabin Environmental Impact Rating (additional details below) is also considered when assessing chemicals as it aids in understanding length of time and dose of crewmember exposure. In such cases, an integrated assessment is coordinated between two NASA Subject Matter Expert (SME) groups. When the assessment is complete, the THL is documented on the end item's HMST.

The THL of a mixture of chemicals is determined from the toxicity of the entire mixture or, if not known, the most toxic component in that mixture. The hazards before, during, and after chemicals are processed and related products are assessed. If there is little or missing information for a chemical (for example: COTS items), the THL rating will be conservative to ensure safe conditions on ISS.

Note: Material offgassing, sometimes referred to as toxic offgassing, is generally not assessed under THL hazard ratings, refer to section 4.7.1, Material Selection, but may be assessed in special cases where material offgassing is expected to occur during operations, such as 3-D printing.

Descriptions of the five THLs are provided in Table D.4.7.2.2.1-1. Utilization of extremely hazardous chemicals, rated as THL-4, should be clearly defined and requires ISSP approval for use in the ISS pressurized habitable environment. Utilization of THL-4 chemicals may be acceptable in the external ISS environment provided they are not brought inside the ISS environment, do not contaminate and/or damage hardware that is brought inside, and/or damage other external end items.

TABLE D.4.7.2.1-1 TOXICITY HAZARD LEVEL (THL) AND HAZARD SEVERITY

Hazard Severity	THL	Description
Marginal	0	any gas, gel, solid, or liquid that has the potential for, at worst, short-term, slight chemical (i.e. not mechanical) irritation that will not require therapy
Critical	1	any gas, gel, solid, or liquid that has the potential for slight to moderate irritation that will not resolve quickly (in <30 minutes) without intervention
Catastrophic	2	a containable solid, gel, or non-volatile liquid that has the potential for moderate to severe irritation and/or ocular damage that may have a long-term performance impact
	3	a containable solid or low-volatility liquid that has the potential for appreciable systemic effects, long-term serious injury (e.g. cancer), or internal tissue damage
Catastrophic	4*	an uncontainable gas, volatile liquid, or fine particles/fume that has the potential for moderate to severe irritation, and/or appreciable systemic effects, and/or a long-term performance impact
Description developed by the JSC Toxicology and Environmental Chemistry Group based on JSC 26895, Guidelines for Assessing the Toxic Hazard of Spacecraft Chemicals and Test Materials. The final THL will be provided with the NASA SME evaluation on the HMST * THL-4 chemicals require ISSP approval for use in the ISS habitable pressurized environment		

Note: The NASA SMACs and the American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Values (TLVs) indicate maximum concentrations of exposure to airborne contaminants (i.e. vapors). The SMACs, TLVs, and THLs are based on different criteria and are meant to be used in very different circumstances so there is no direct quantitative relationship between them.

Flammability Hazard Level (FHL) Hazard Rating

The NASA/JSC Materials and Processes Branch, the NASA SME, assess flammability hazards for all chemicals and test materials. All end item chemicals to which the crew might be exposed are assigned an FHL rating. FHL ratings were developed by NASA SMEs and are unique to the spaceflight and spacecraft environments. The FHL takes into consideration the physical state and flash point of the chemical. For liquids and powders, the FHL is the flammability hazard that would result if the chemical was released into the vehicle; without regard to the controls that prevent release of the chemical. For gases, the FHL is the flammability hazard that would result based on leakage of the chemical. The assessment takes into consideration that pressurized gases can leak from a container until the internal pressure is cabin ambient pressure, resulting in the potential for formation of a localized flammable gas cloud. The flash point is the lowest temperature at which a chemical can form vapors or an ignitable mixture in the air that will ignite given an ignition source. A lower flash point is an indication that the chemical is easier to ignite. The allowable quantity of flammable chemicals that could be released depends on the chemical's flash point.

Chemical and material processing and related reactions are assessed for flammability. The FHL of a mixture of chemicals is determined from the flammability of the entire

SSP 51721
Baseline

mixture or the most flammable component in that mixture depending on the chemical components.

Note: Flammable materials used in the construction or development of end items is not assessed under FHL hazard ratings, refer to section 4.7.1.1, Flammable Materials.

Descriptions of the five FHLs are provided in the Table D.4.7.2.2.1-2. Most flammable fluids are toxic at lower concentrations than their lower flammability limit resulting in the response to leaks of flammable fluids being driven by the response to the THL. Nontoxic flammable gases such as hydrogen and methane would have a higher FHL than THL hazard rating. The preferred method to prevent release of chemicals that are flammable is through LoC. Refer to JSC 64825A, Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials, for additional details.

TABLE D.4.7.2.2.1-2 FLAMMABILITY HAZARD LEVEL (FHL) AND HAZARD SEVERITY

Hazard Severity	FHL	Description	Flash Point*	
			Temperature °F (°C)	Volume (ml)
Acceptable (Not a hazard)	0	Any liquid, powder or gas considered to be a nonflammable material and limited quantities of flammable liquids and powders based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of < 20 liters	< 120 (49)	< 5
			120 (49) – 200 (93)	< 25
			200 (93) – 300 (148)	< 50
			> 300 (148)	<250
Critical	1	Flammable liquid, powder and gas; quantity limits for liquid and powder are based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of 20-100 liters	< 120 (49)	5 – 25
			120 (49) – 200 (93)	25 – 100
			200 (93) – 300 (148)	50 – 250
			> 300 (148)	250 – 1000
Catastrophic	2	Flammable liquids and powders; quantity limits are based on the flammable material's flash point	< 120 (49)	25 – 100
			120 (49) – 200 (93)	100 – 250
			200 (93) – 300 (148)	250 – 500
			> 300 (148)	> 1000
	3	Flammable liquids and powders; quantity limits are based on the flammable material's flash point	< 120 (49)	100 – 250
			120 (49) – 200 (93)	250 – 500
			200 (93) – 300 (148)	500 – 1000
			> 300 (148)	
	4	Flammable liquid, powder and gas; quantity limits for liquid and powder are based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of ≥ 100 liters	< 120 (49)	> 250
			120 (49) – 200 (93)	> 500
			200 (93) – 300 (148)	> 1000
			> 300 (148)	

Description details developed in coordination with NASA/JSC Materials and Processes Branch based on JSC 64825A, Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials.

The final FHL will be provided with the NASA SME evaluation on the HMST.

* The flash point is the lowest temperature at which a chemical can form vapors or an ignitable mixture in the air that will ignite given an ignition source. A lower flash point is an indication that the chemical is easier to ignite.

ECLSS Impact Hazard Ratings

There are two ECLSS impact hazard ratings that were developed by the NASA SME, the NASA/ISS ECLSS Engineering Group, and are unique to the ECLSS hardware, and the spaceflight and spacecraft environments. The ECLSS ratings are based on release of the chemical into the vehicle; it assumes complete failure of the controls that prevent release of the chemical. The potential hazards from mixtures of chemicals and from chemical reaction and thermal decomposition products are also assessed as necessary.

The ECLSS Cabin Environmental Impact Rating is an indicator of how long the chemical may persist in the cabin environment and depends upon the chemical and the

SSP 51721
Baseline

ECLSS hardware’s ability to remove the chemical from the cabin environment. Sometimes it is only possible to make a rough estimate of removal times or contaminant (chemical) concentrations during and after scrubbing. Descriptions of the five ECLSS Cabin Environmental Impact Ratings are provided in the Table D.4.7.2.2.1-3. The ratings do not directly correlate to hazard severity; however, they are a consideration for crew exposure and determination of THL ratings.

The ECLSS Hardware Impact Rating (E-Rating) is used to understand ECLSS performance or hardware impacts such as functional degradation, operational constraints and/or life cycle impacts relative to planning for resupply and/or refurbishment. Descriptions of the seven E-Ratings are provided in the Table D.4.7.2.2.1-4.

TABLE D.4.7.2.2.1-3 ECLSS CABIN ENVIRONMENTAL IMPACT RATING

ECLSS Cabin Environmental Impact Rating	Time for ECLSS to Reduce Contamination Concentration by 95%*
A	0-2 hours
B	2-24 hours
C	24-72 hours (1-3 days)
D	72-168 hours (3-7 days)
E	> 168 hours (7 days) ECLSS is unable to remove chemical and it persists in the environment
Details developed in coordination with NASA/ISS ECLSS Engineering Group based on JSC 66869, Guidelines for the Assessment of Chemicals and Materials for Impacts to Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft. The final ECLSS Cabin Environment Impact Rating will be provided with the NASA SME evaluation on the HMST. * Acceptable level for crewmember to breath without protective filtration masks	

TABLE D.4.7.2.2.1-4 ECLSS HARDWARE IMPACT RATING (E RATING) AND HAZARD SEVERITY

Hazard Severity	ECLSS Hardware Impact Rating (E Rating)	Description
Acceptable (Not a hazard)	E0	No ECLSS performance degradation. No change in scheduled maintenance. (Operational capacity* consumption is <2%, with 100% of the capacity margin** retained.)
	E1	No ECLSS performance degradation. No change in scheduled maintenance. (Operational capacity consumption is >2% and <10%, with > 10% of the capacity margin consumed.)
Marginal	E2	ECLSS functional performance is degraded by <10%. Early replacement of consumable components may be necessary within nine months. (Operational capacity consumption is >10% and <25%, with > 25% of the capacity margin consumed.)
	E3	ECLSS functional performance is degraded by >10% and <25%. Early replacement of consumable components may be necessary within six months. (Operational capacity consumption is >25% and <50%, with > 50% of the capacity margin consumed.)
Critical	E4	ECLSS functional performance is degraded by >25% and <50%. Early replacement of consumable components may be necessary within one month. (Operational capacity consumption is >50% and <75%, with > 75% of the capacity margin consumed.)
	E5	ECLSS functional performance is degraded by >50% and <75%. System maintenance is required to restore functional performance within one week. (Operational capacity consumption is >75% and <90%, with 100% of the capacity margin consumed.)
	E6	ECLSS functional performance is degraded by >75%. System maintenance is required to restore functional performance within one day. (Operational capacity consumption is >90%, with >100% of the capacity margin consumed.)
<p>Description details developed in coordination with NASA/ISS ECLSS Engineering Group based on JSC 66869, Guidelines for the Assessment of Chemicals and Materials for Impacts to Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft.</p> <p>The final E Rating will be provided with the NASA SME evaluation on the HMST.</p> <p>* Operational capacity: capability of the system performance</p> <p>** Capacity margin: allowance provided for system performance (hardware is nominally operated at less than 100% to allow for margin)</p>		

***ECLSS E-Ratings and THL:** The ECLSS E-Ratings and THL are generally considered to be independent of one another with one exception, when interaction with the ECLSS hardware or environment results in chemical reactions and additionally hazardous chemicals. This would be the case when a chemical thermally decomposes upon exposure to the ECLSS hardware processing temperatures, the moisture in the cabin atmosphere, and/or the condensing heat exchangers to produce products that are more*

SSP 51721 Baseline

harmful than the flown chemical. Any potential products from interaction with ECLSS hardware is provided to the toxicologist for consideration when assigning the THL rating.

For end item chemicals whose release does not result in specific toxicity hazards (chemical is rated THL-0), there can still be adverse impacts to the ECLSS hardware that result in contamination to the environment and ISS/VV equipment and thus, affect crew health in an indirect manner.

When considering chemicals for flight hardware, it is recommended to select chemicals that are low volatility, exhibit low solubility in water, are thermally stable to $\geq 500^{\circ}\text{C}$, and chemically stable in the presence of atmospheric humidity and liquid water. Refer to JSC 66869, Guidelines for the Assessment of Chemicals and Materials for Impacts to the Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft, for additional details.

Water-Soluble Volatile Organic Compounds: There are specific restrictions on water-soluble volatile organic compounds such as alcohol (ethanol and isopropyl alcohol, acetone, glycol, etc.) due to adverse impacts to ECLSS hardware. End items are required to meet the requirements in SSP 30233 and/or the applicable IRD. Small quantities (< 1g/day allowed in total for all of ISS) of these compounds may be released based on a pre-coordinated ISSP Volatile Organic Compound Usage Agreement. Some alcohols, glycols, and ketones are not restricted. Refer to the applicable IRDs for details.

Chemical Assessments and the Hazardous Materials Summary Table

All chemicals used in and/or for an end item should be included in the chemical assessment request. This includes chemicals used to make the hardware function, chemicals used for experiments, and chemicals that result from experiments. Specific examples of chemicals to include in the assessment request are identified here. There may be additions to this list as the end item goes through the safety review process. For specific questions, contact the ISRP. Where possible, hazard rating (THL, FHL, and ECLSS impact hazards) information is provided for reference. The final hazard ratings will be provided with the NASA SME evaluation on the HMST.

Chemical Products Resulting From Reactions: During processing, some chemicals may undergo changes in phase (e.g., solid to liquid or to gas or to vapor), change in concentration (e.g., dilution), and/or produce new chemicals (such as through combustion). The potential products of chemical reactions, intentional in experiment hardware or unintentional due to potential misuse of hardware or failures, should be considered.

Examples of chemicals from reactions:

- *Decomposition products from high temperatures (pyrolysis); for example: materials science furnace facilities*

SSP 51721

Baseline

- *Metal dusts and fumes (particles equal to or less than 1 micron) from heating metals enough to produce metal vapors which condense into fine particles in a gaseous atmosphere*
- *Products from combining two or more chemicals*
- *Gas or waste produced from biological material samples (not considered to be biological materials)*

Chemicals Used On Orbit: *Chemicals used with the end item on orbit (such as when an end item is launching empty and connected to other hardware on orbit) should be included in the assessment request.*

Battery Electrolyte: *The chemical composition of battery electrolyte, including electrolyte chemistry and number and size of batteries, should be provided. Battery electrolyte is considered to be THL-2 or higher.*

Note: *The use of Lithium Thionyl Chloride batteries inside the pressurized (habitable) environment is strongly discouraged and requires ISSP approval due to the potential for release of highly toxic compounds. The electrolyte for these types of batteries is THL-4. These types of batteries have been allowed for use in the unpressurized (external) environment of ISS.*

Capacitor Electrolyte: *The chemical composition of capacitor electrolyte, including electrolyte chemistry, number, and size of capacitors, should be provided. Capacitors can be classified into two general categories based on whether or not they contain liquid electrolyte at room temperature. "Dry" (solid) capacitors that do not contain liquid electrolyte do not need to be assessed; whereas capacitors that contain liquid electrolyte do require assessment.*

For reference, wet tantalum capacitors are considered to be THL-2 due to sulfuric acid and aluminum electrolytic capacitors containing ethylene glycol are generally considered to be THL-1.

Gas-filled Light Bulbs (such as Halogen bulbs): *Gas components of light bulbs should be provided. If the gas is a mixture, the percentage of individual gases should be identified.*

Mercury: *Any items (such as electronics, lighting, or computer backlights) containing mercury should be identified and provided. The use of mercury containing items is discouraged as mercury can produce toxic vapors and can amalgamate with metals or metal alloys used in spacecraft hardware.*

Exceptions to Chemical Assessments

Liquid Crystal Displays (LCDs): *The liquid crystal materials used in LCDs and touchscreens available today are high molecular weight, low volatility compounds that are sandwiched between glass-type plates. The liquid crystals are prevented from escaping due to surface tension (even if the outer plates break). The liquid crystals used in LCDs and touchscreens are regarded as toxicologically safe and do not need to be assessed for chemical composition.*

D.4.7.2.3 Rationale – Radioactive Material Release

This requirement applies to all radioactive materials that are located in or may be introduced into the pressurized habitable environment and are not considered exempt or under exemption per the U.S. Nuclear Regulatory Commission (NRC) Regulations Title 10, Code of Federal Regulations (CFR). It is established to protect the crew from physiological impacts and the environment and vehicle from contamination due to exposure to radiation source material and secondary emissions. Radioactive material is a source of ionizing radiation; requirements for other sources of ionizing radiation are addressed in section 4.6.2, Ionizing Radiation and section 4.3, Electrical. All radioactive material (for example radioactive isotopes) is classified as a catastrophic hazard (the highest hazard severity). Accordingly, the primary radioactive material or source of radiation is controlled to prevent release through failure tolerance (LoC or appropriate controls) or DFMR, reference Section 4.7.2, Hazardous Materials, for details. A material capable of absorbing any primary or secondary radioactive emissions is provided in the design; this can be part of the controls or a separate design feature. Emissions that cannot be shielded are kept As Low As Reasonably Achievable (ALARA). If the operation or use of the end item has the potential to release radiation (or emissions), the end item provider should show how radiation is controlled during operations and hardware use. Details and criteria for utilizing the failure tolerance approach (LoC or appropriate controls) is provided in section 4.7.2. Documentation of the use of the radioactive material, along with the controls for all phases and conditions of use is supplied for review and approval by the ISRP. Major radioactive sources also require approval by the Interagency Nuclear Safety Review Panel through the NASA coordinator for the panel. Department of Defense (DoD) end items involving radioactive materials will also be processed through DoD established procedures.

There are limitations on the use of radioactive material across IP Modules so special agreements may be necessary for end items that will be located in IP modules or will move between modules on-orbit.

The NASA SME that reviews radioactive materials is the NASA/JSC SRAG who will assess the primary radioactive material (source) and potential secondary emissions. Request for SRAG review of all radioactive materials (those considered exempt and those not considered exempt) is done every flight in accordance with SSP 30599 through submission of the JSC Form 44 (NAMS request is required for login). Details on the end item radioactive material, exemption details and any special instructions are captured in the final approved JSC Form 44.

The necessity and utilization of radioactive material in end items should be carefully reviewed and the radiation source material should be kept ALARA. For example, if radioactive material is used to calibrate equipment, it should be a radiation source that produces the lowest amount of radiation to achieve the required result.

Note: It is recommended that if the end item does need radioactive materials. the end item development team include a radiation expert that understands the complexity of working with radioactive materials. For pre-/post-flight ground processing, the end item

SSP 51721

Baseline

provider should comply with appropriate license requirements. This may include obtaining special license(s).

D.4.7.2.4 Rationale – Biological Material Release

This requirement does not apply to crew food or crew personal preference items.

This requirement applies to all biological materials that are located in or may be introduced into the pressurized habitable environment. It is established to protect the crew and environment from immediate or latent biohazards, including contamination of food and water supplies. Biohazards are biological materials or biological agents that may be harmful to the crew and/or to the environment. This requirement encompasses live and cultured biological materials used in end items and/or collected as samples from ISS. This requirement also applies to vectors of biological materials such as animals and plants, non-biological materials such as soil or dust, and environmental conditions such as warm, moist air that may harbor or promote the growth of biological materials.

Controls to prevent release of the biological materials are provided through failure tolerance or DFMR based on the hazard severity, reference section 4.7.2, Hazardous Materials, for details. The preferred method to prevent release of biological materials is through LoC. Documentation of biological materials usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP.

Due to the typically nonvolatile nature, biological materials do not impact the ECLSS impact hazard ratings (reference section 4.7.2.2.1).

In-Flight Biosafety Level

The In-Flight BSL ratings provided by the NASA SMEs, NASA/ JSC BRB, are unique to spaceflight. The rating structure was derived from the four BSL categories established for biohazardous materials in ground-based laboratories by the U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (CDC) and the National Institutes of Health (NIH) with additional considerations made for the unique environment and conditions of spaceflight. For example, due to microgravity conditions in space, aerosols from microorganisms can be more of a risk factor than on Earth as larger particles and droplets can be suspended as aerosols for longer timeframes. In consideration of microgravity, the BSL-2 category is divided into BSL-2M (Moderate) and BSL-2H (High). Descriptions of the five In-Flight BSLs are provided in Table 4.7.2.3-1.

Biological material is documented on the HMST. Biological material considered to be biohazardous material will be assigned an In-Flight BSL rating, also referred to as BSL. Biological material that is determined to be non-infectious and outside the biohazard category will not be assigned a BSL rating.

Factors that affect the BSL rating include the origin and volume of the biological material, physical state of the sample growth medium (solid or liquid), infectivity dose, medical or spacecraft integrity consequences, and proposed operations/usage. If there is limited information available on a biological material or the operation and use, the

SSP 51721
Baseline

BSL rating may be elevated to ensure safe conditions on ISS. When two or more biohazardous materials or agents are present in an end item, the hazard severity will be driven by the highest BSL rating.

Samples and cell lines purchased from suppliers will typically be identified with a BSL rating. The NASA BRB In-Flight BSL rating evaluation may differ from supplier BSL information. The NASA BRB rating will serve as the rating by which the end item hardware will be evaluated for flight.

Prohibited Biological Material: Biological materials rated BSL 3 and 4 are prohibited from the ISS as the ISS (both the internal and external environments) is not equipped to provide the necessary protection from these biological materials. Prions are considered BSL-3 and are not allowed on ISS.

TABLE D.4.7.2.4-1 NASA IN-FLIGHT BIOSAFETY LEVEL RATING AND HAZARD SEVERITY

Hazard Severity	NASA Biosafety Level (BSL) Rating	Description
Marginal	1	Well-characterized agents not known to consistently cause diseases in healthy adults, minimal hazard to environment
Critical	2M (Moderate)	Moderate risk agents associated with human disease. Primary exposure routes include: skin (percutaneous) exposure, ingestion, and mucous membrane exposure.
Catastrophic	2H (High)	Higher risk agents associated with human disease. Risk is increased by lower infectious dose, likelihood of aerosolization, larger amounts of agent presents and other factors
Not Allowed*	3	Agents with potential for airborne transmission. May cause life-threatening diseases.
	4	Agents with high potential for life threatening disease. High potential for aerosol transmission of agent with no disease prevention (prophylactic) or specific therapy
<i>Description developed in coordination with NASA/JSC Biosafety Review Board based on JSC Procedural Requirements (JPR) 1800.5, Biosafety Review Board Operations and Requirements.</i> NOTE: The In-Flight BSL is commonly referred to as BSL instead of In-Flight BSL * BSL 3 and 4 are prohibited from use on ISS		

Animals

The NASA SMEs that review animal use are the JSC BRB, the NASA/Flight Institutional Animal Care and Use Committee (IACUC), and the NASA Chief Veterinarian.

Invertebrates are typically reviewed by the BRB and vertebrates are jointly reviewed. An integrated assessment is coordinated between the SME groups with the assigned In-Flight BSL and any special notes documented on the end item's HMST.

End items involving animals and related operations are reviewed on a case-by-case basis. Special consideration is given to operations that involve the crew handling animals or coming into contact with animal experiment products such as waste. The primary concern with animals is the prevention of zoonotic disease, a disease that can

SSP 51721
Baseline

spread from animals to humans, and contamination of the environment. The use of feral or non-colony born animals is discouraged due to the potential for a greater variety of pathogens.

Animals and samples taken from animals are required to be appropriately controlled at all times. Animal housing units and glove boxes or work stations should be designed to filter particulate matter and keep it from exhausting into the ISS environment. Procedures involving renewing animal food supplies or removing animal waste should not expose the crew to the animals. Refer to requirements in JPR 1800.5, Biosafety Review Board Operations and Requirements, for additional details on animal experiments.

Rodents: NASA has developed a listing of mouse pathogens based on potential zoonotic diseases. Specific Pathogen Free (SPF) certified rodents are required to be utilized for crew flight activities. For a listing of the NASA approved vendors and detailed testing protocols pre-flight to certify mice as SPF mice, refer to JPR 1800.5.

End Item Design Considerations

End items can promote the growth of biological materials such as fungus on orbit by producing certain environmental conditions through the materials used in end items or through end item operations and use. The environmental conditions produced inside an end item (such as warm, moist air) should also be considered for potentially promoting biological growth.

Materials that prevent the growth of biologicals should be used when possible. When that is not possible or organic material is needed for the end item, precautions should be taken to prevent growth. End items or ISS provided hardware used for experiments, such as ISS glove boxes, should be routinely cleaned. The requirements in SSP 30233 for moisture and fungus resistance (section 4.2.10) should also be followed.

Requirements for condensation prevention are addressed in the applicable IRDs. The IRDs also include material requirements for end items connecting to the ITCS MTL or LTL to prevent fungal growth inside the MTL or LTL systems.

Biological Material Assessments and the Hazardous Materials Summary Table

All end item biological materials launched, planned for use, included in special operations, and non-biological materials that promote biological growth should be included in the assessment review request (<https://www.nasa.gov/feature/hazardous-material-summary-tables-hmsts>). Examples of launched biological material to include are: plants, animals, bacteria, fungi, cell cultures, protozoa, viruses, recombinant Deoxyribonucleic Acid (rDNA), recombinant Ribonucleic Acid (rRNA), microbial toxins, and allergens. Samples planned to be taken from the crew, the environment, or ISS hardware are also examples of biological material to include. Examples of biological vectors and environmental conditions that may result in biological growth are provided at the beginning of this section. There may be additions to this list as the end item goes through the safety review process.

SSP 51721

Baseline

The following BSL ratings are provided for reference. References for samples collected in-flight are specific to crewmember sampling only. The final BSL will be provided with the NASA SME evaluation.

- *Human cell lines are generally rated as BSL-2M based on information contained in the 5th edition of “Biosafety in Microbiological and Biomedical Laboratories” published by the CDC and NIH. The rating will be higher if the human cells are determined to be a higher risk.*
- *Waste from SPF rodents is assessed as BSL-1*
- *Blood samples collected in-flight are assessed as BSL-1*
- *Saliva samples collected in flight are BSL-1*
- *Urine samples (freshly voided, treated with disinfectant/preservatives, or frozen) collected in-flight are assessed as BSL-1*
- *Urine samples (not treated with disinfectant/preservatives and stored at ambient temperature or refrigerated for more than 24 hours) collected in flight are considered BSL-2M*

D.4.7.2.5.1 Rationale – Physical Agents Release

This requirement encompasses particles and fluids that are located in or may be introduced into the pressurized habitable environment and act as physical agents when released. It is established to protect the crew from physiological hazards and/or to protect the environment and VV/ISS equipment from hazards resulting from contamination.

Requirements for materials or substances that are chemically reactive, toxic, and/or significantly soluble in water are covered in Section 4.7.2.2, Chemicals, and biological materials, including allergens, are covered in Section 4.7.2.4, Biological Material Release.

Control to prevent release of physical agents is provided through failure tolerance or DFMR based on the hazard severity, reference Section 4.7.2, Hazardous Materials and Table D.4.7.2.5.1-1 below for details. Documentation of physical agent usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP.

Particle Release

The NASA SMEs, NASA/ JSC Toxicology and Environmental Chemistry Group and NASA/JSC Space Medicine, have developed a Particle Policy to define the risk and hazard severity for particle release based on particle size, concentration, and duration of exposure.

Particles that are determined to be chemically inert and/or insoluble in water are a nuisance at low concentrations and a physical hazard at high concentrations. The concentrations identified in the Table D.4.7.2.5.1-1 apply to short duration events driven

SSP 51721
Baseline

by failures that would release particles rapidly. It does not apply to a routine or intermittent source of particles or over long periods of time. For these particles and use, hazard control measures to limit exposures should be implemented. For example, nanoparticle generation by routine three dimensional (3D) printing should be controlled to prevent release or limit release to acceptable levels. Consideration should also be given to implementing the Occupational Health and Safety Administration (OSHA) recommendations that work with nanomaterials occur in ventilated enclosures (e.g. glove box, laboratory hood, or process chamber) equipped with High Efficiency Particulate Air (HEPA) filters.

Table D.4.7.2.5.1-1 is provided as a reference based on specific particle density, lung deposition, and minute volume; the concentration limit will differ for different minute volumes or particle densities. The routine or purposeful release of particles should be identified when the end item data is provided for review as indicated in the verifications. As particles addressed here are considered physiological hazards instead of chemically induced toxicity hazards, a THL rating is not assigned; instead, the details will be captured in the end item's HMST as a note in the comments section.

Physiological Hazards: The unique attributes of the decreased gravitational environment cause particles to remain suspended in the air for extended timeframes. The main physiological hazards caused by particle release for the crew are suffocation and asphyxiation. Particles > 10 µm in diameter released in large amounts cannot be inhaled deeply into the lower respiratory tract (lungs) but could cause acute asphyxia (suffocation within a few minutes) due to mechanical blockage of the upper respiratory tract, especially the larynx. Particles ≤ 10 µm diameter can be inhaled deeply into the lungs and cause a slow asphyxiation (suffocation within many minutes to hours) by obstructing the deep lung and interfering with oxygen exchange.

Acceptable Level: Concentrations below occupational limits are considered acceptable as they are not expected to cause any significant hazard or permanent health issue. Control to prevent release is not required but remains recommended when feasible. The release of particles in this size and concentration are considered to be a nuisance and will be indicated as such on the HMST.

TABLE D.4.7.2.5.1-1 PHYSICAL AGENTS AND HAZARD SEVERITY

Type of Physical Agent	Not a Hazard	Hazard Severity		
	Acceptable Level	Marginal	Critical	Catastrophic
Inert, Insoluble Particle				
Size of particle > 10 µm	C ≤ 10 mg/m ³	N/A	10 mg/m ³ < C < 50 g/m ³	C ≥ 50 g/m ³
Size of particle ≤ 10 µm	C ≤ 3 mg/m ³	N/A	3 mg/m ³ < C < 13 g/m ³	C ≥ 13 g/m ³ *
Inert, Insoluble Particle				
Sharp Particles ⁺	PS ≤ 50 µm ^{**}	N/A	N/A	PS > 50 µm
Fluid				
THL-0 fluid ^{**}	N/A	R < 1 gallon	N/A	R ≥ 1 gallon

Table is based on NASA/ JSC Toxicology and Environmental Chemistry Group and NASA/JSC Space Medicine Particle Policy and ISSP Fluid Release Policy.

C = concentration; R = release; PS = particle size

* Concentration limit will vary based on minute volumes and particle density. The value identified here assumes a particle density of 1.5 g/cc, 50% deposition in the lungs, and a minute volume of 10 liters/min during an exposure duration of about 360 minutes, divided by a safety factor of 2.

** Release limits here are specific to THL-0 fluids (galley water or ITCS fluid); limits are ISSP derived based on ISS System capability.

+ Note: Inert, insoluble sharp particles are addressed in section 4.7.2.5.2, Shatterable Materials.

** Particles of this size may present a potentially catastrophic hazard if released at high velocity.

Fluid Release

The ISSP has established a quantity limitation on the release of low toxicity, THL-0, fluids (such as galley water or ITCS cooling fluid) due to potential physiological and equipment hazards. This requirement is specific to THL-0 fluid. The hazard rating for some THL-0 fluid increases after the fluid evaporates to a more concentrated (less dilute) material. For THL-0 fluids that adversely impact ECLSS hardware, the limitation may be smaller than identified in the table due to potentially adverse environmental impacts. For impact to the environment and ECLSS hardware, refer to the ECLSS impact hazard ratings in section 4.7.2.2.1, Chemical Release.

The hazard severity for release of THL-0 fluid is categorized based on potential leakage volume as indicated in the table. End items should determine potential leakage based on both the volume of fluid held inside the end item and the volume of fluid from ISS systems the end item connects to for service (e.g. cooling through the ITCS Moderate Temperature Loop (MTL)). End items connecting to ISS systems or services (for example connecting to the MTL through an EXpedite the PROcessing of Experiments for Space Station (EXPRESS Rack) can utilize the ISS system response as one control in the prevention of the hazard. In such a case, the end item would need to provide appropriate controls for a critical level hazard. The ISRP reviews end item designs and fluid usage on a case-by-case basis. The hazard rating for the fluid and potential leakage will be included in the end item's HMST. All chemicals should maintain a

SSP 51721
Baseline

minimum of one control to prevent release (containment or appropriate controls) at all times.

Physiological Hazards and Equipment Damage: The unique attributes of the decreased gravitational environment cause fluids to coalesce into fluid bubbles and/or adhere to surfaces in microgravity. Depending on the amount of leakage and/or release, the fluid bubble can get large and may become uncontrollable; adhering fluids can hide in and/or behind hardware or racks. This can result in physiological problems for the crew and/or damage to equipment.

Note: Leakage of ITCS fluid is monitored and tracked to determine ITCS performance. In the event that a leak occurs, the ISS C&W system would be activated.

Physical Agent Assessments and the Hazardous Materials Summary Table

All end item physical agents should be included in the assessment review request. Specific examples of items to include in the assessment request are end item materials that produce particles such as dust, constituents of thermal insulation panels such as vacuum insulation panels and filters such as activated carbon and particle mesh filters. These items can degrade and release particles while on-orbit. All end item fluids should also be included. There may be additions to this list as the end item goes through the safety review process. For specific questions, contact the ISRP.

D.4.7.2.5.2.1 Rationale Shatterable Materials Release

This requirement encompasses shatterable materials that are located in or may be introduced into the pressurized habitable environment. It is established to protect the crew from physiological hazards and/or to protect the environment and VV/ISS equipment from hazards resulting from contamination.

Control to prevent release of shatterable materials is provided through failure tolerance or DFMR based on the hazard severity, reference Section 4.7.2, Hazardous Materials, for details. The control strategy for shatterable materials often relies on a DFMR philosophy with appropriate verifications rather than failure tolerance as applying failure tolerance can be a challenge for many of the applications where shatterable materials are used. Documentation of shatterable material usage, along with the controls for all phases and conditions of use, is supplied for review and approval by the ISRP.

The NASA SMEs, NASA/JSC Toxicology and Environmental Chemistry Group and NASA/JSC Space Medicine, have defined the size limit of concern with shatterable materials through the Particle Policy; refer to Table D.4.7.2.5.1-1. Release of shatterable materials, inert sharp particles, > 50 μm in their longest dimension is considered a catastrophic hazard due to the potential to cause a disabling injury, even after a brief exposure. Shatterable materials can potentially cut/damage the eye or skin; they can also contaminate the environment and pose an asphyxiation risk. Shatterable materials $\leq 50 \mu\text{m}$ are considered to be acceptable (refer to rationale for Physical Agents Release, section 4.7.2.5.1, for acceptable level). However, shatterable materials $\leq 50 \mu\text{m}$ can present a potentially catastrophic hazard if released at high velocity, and will be assessed on a case-by-case basis by the ISRP.

SSP 51721
Baseline

The SMEs also assessed whether there was an upper size limit at which the risk and hazard from shatterable materials would be considered acceptable. Although the blink reflex may exclude some particles, it cannot be relied upon to prevent exposure; therefore there is no upper size limit that would be acceptable for the shatterable material hazard.

Guidance is provided here on preventing the release of shatterable material.

- The preferred method to prevent release of shatterable materials is through containment. Shatterable materials should fully and permanently contained by design whenever possible. Containment precludes escape of glass particles in the event of breakage. For example, glass displays and glass Light Emitting Diodes (LEDs) should be covered with non-shatterable material such as Lexan or plastic film. Alternatives to a solid covering would include filters or a mesh screen that is shown to prevent the release of glass particles > 50 µm. With appropriate verifications, the ISRP has accepted these types of contained coverings as DFMR for this application.*
- If containment is not practical for operational reasons, the end item should still be contained for non-operational timeframes (i.e launch). For the operational phase, the end item should be operated in a way that protects the shatterable material. An alternative for the operational phase could be to qualify the hardware under structural requirements and perform testing on the flight hardware based on the worst-case conditions as addressed in section 4.2, Structures.*
- If an end item is not tested nor is the shatterable material permanently contained, the end item should contained in a transparent bag so that it can be inspected within the bag prior to usage. The transparent bag allows for visual inspection without exposing the crew to fragments in the event there is breakage. If the worst-case load is determined to be launch, the item should be packaged for launch to minimize loading and inspected prior to initial usage. This option is utilized for shatterable material that has operational limitations or is considered to be optical glass. For optical glass, refer to section 4.7.2.5.2.2.*

D.4.9.1.1 Rationale – Impulse Noise Hazard Limit

This requirement is applicable to all individual noise sources. Impulse noise higher than this value could result in temporary to permanent hearing loss. Impulse noise is defined as a change in Sound Pressure Level (SPL) of more than 10 dB in one second or less.

This requirement is applicable during the worst-case operational scenario and closest nominal distance to the crewmember's head. This includes the equipment operating in the loudest mode of operation that can occur on orbit under nominal crew or hardware operation circumstances, during setup, and/or when doors/panels are opened or removed.

SSP 51721
Baseline

D.4.9.1.2 Rationale – Class 1 and Class 2 Alarm Audibility

This requirement is applicable to emergency and warning tones and ensures they are audible over the continuous noise in the habitable areas. Acoustic measurements are periodically taken on-orbit and are used as a basis to quantify the ambient noise.

If the alarm signal is intended to arouse sleeping occupants, option 1 above must be utilized. When using options 2 or 3, the alarm must meet the requirement in at least one octave or 1/3 octave band, respectively.

“Effective masked threshold” is the level of alarm signal just audible over the ambient noise, taking into account the acoustic parameters of both the ambient noise in the signal reception area and any listening deficiencies (hearing protection, hearing loss and other masking effects, i.e. upward spread of masking).

Class 3 and 4 alarms are not included in this requirement because the crew is not the primary responder. For Class 3 caution alarms, automatic safing has occurred and no immediate crew action is required. Class 4 is an advisory and is used for ground monitoring.

D.4.9.1.5 Rationale – Composite Continuous Acoustic Emissions – ISS Level Requirement (USOS)

Excessive noise in the ISS exceeding NC~52 could impact crew hearing and communication. This requirement is applicable to the overall ISS environment, including VVs, and is verified at the integrated level. This requirement is not applicable to individual end items but data from the individual end items may be used in the integrated analysis.

This requirement originates from the fact that the former NC-48 allocation for the payload complement and NC-50 allocation for the vehicle sum to approximately NC-52, termed NC~52, levels in most octave bands, and thus Table 4.9.1.5-1 contains rounded NC-52 values except for the 63 Hz and 125 Hz octave bands, where values of 2 dB over the NC-50 levels were used instead of the straight NC-52 values. Equivalently, these values in the 63 Hz and 125 Hz octave bands are 1 dB over the rounded NC-52 values. This departure from the NC-52 set of values prevents significant complications in transitioning from separate NC-48 and NC-50 allocations for payload complements and the vehicle to a joint set of requirement levels.

ISS Integration performs this assessment to satisfy SSP 57011, Verification # EN-02. The results are presented to the ISRP if an exception is required.

If the limits in Table 4.9.1.5-1 are exceeded, acoustical analyses are performed to develop operational scenarios to ensure the integrated payload plus vehicle complement acoustical noise limit is at or below the level defined. These operational constraints will be used to produce timelines that do not exceed the acoustical noise limit.

An NC-40 requirement is levied on all integrated racks and GFE/CFE continuous noise sources per applicable IRD. Continuous noise source sub-rack and non-rack payloads

SSP 51721
Baseline

have an NC-34 requirement. This ISS-level requirement takes into account the fact that some end items might exceed their IRD requirement and allows for managing the entire complement of hardware aboard ISS to meet an overall acoustic requirement. Noise levels are only hazardous if the levels of the integrated environment are high.

Intermittent noise generators are not included in the complement analysis for continuously operating items. Intermittent noise generators are documented within the Guidelines and Constraints documents with their allowed operational time limits so that mission planning can incorporate any constraints.

D.4.9.2.1 Rationale – Touch Temperature Limits

This requirement applies to end items inside and/or connected to the ISS internal pressurized environment.

The end item exposed surface touch temperature range from 0°C (32°F) to 45°C (113°F) is considered non-hazardous and is acceptable for bare skin contact. Contact with exposed surfaces outside of this temperature range are either prevented through failure tolerance or DFMR based on the hazard severity or shown by analysis to meet the T_{PM} based on end item material properties and skin contact time. Anything outside of the T_{PM} range is considered a critical or catastrophic hazard (reference section 4.1.1) as determined by the Flight Activities Control Board (FACB) and ISRP based on potential skin damage.

Additional guidance on touch temperature hazard severity is provided in Table/Figure for touch temperature hazard severity <TBR D-11>.

To verify this requirement, end item exposed surface temperature (T_{ES}) are assessed based on the worst case temperature the end item can reach. This should take into account the appropriate number of failures based on potential hazard severity. For end items with worst case T_{ES} that fall within the non-hazardous range, no additional analysis/calculations are needed. For end items with worst case T_{ES} that is at or outside the non-hazardous range, the end item T_{PM} should be calculated.

Touch temperature limits depend on contact thermal conductance, which is a function of an end item's material properties and initial temperature, and skin contact time. Additional information on the derivation of hot and cold temperature limits can be found in NASA/SP-2010-3407, Human Integration Design Handbook (HIDH).

Term Definitions

Exposed Surfaces

Exposed surfaces are all external and internal surfaces the crew could touch or contact. Thermal conductance of exposed surfaces could vary within one end item if the exposed surfaces vary in material composition (e.g., glass and metal surfaces).

Worst Case T_{ES}

End item worst case T_{ES} is the most extreme temperature (hot or cold) that the end item T_{ES} could become without thermal controls. It is based on failure of thermal controls that the end item could reasonably be exposed to and/or experience. It should be

SSP 51721
Baseline

determined after end item exposure to worst case environments, internal/external failure(s) and/or ISS system failure(s) (for example: fan failure, heater failure, furnace failures, stuck on heater, freezer temperature sensor error in control loop, low cabin ventilation [within limits], high cabin temperature [within limits], etc.). It should also take into account the appropriate number of failures based on potential hazard severity (i.e. 1 failure should be considered for critical hazards and 2 failures should be considered for catastrophic hazards).

If there are multiple end items surfaces, each T_{ES} should be measured or calculated and compared to determine the end item's worst case T_{ES} .

Incidental Contact

Incidental contact is unplanned, accidental or unintended contact with a short skin contact time of 1 second or less ($t \leq 1$ second).

End items having surfaces with the potential for incidental crew contact should be designed such that nominal surface temperatures are non-hazardous or design provisions should be in place that preclude incidental contact with surfaces outside the acceptable range for bare skin contact.

Intentional Contact

Intentional contact is planned contact for normal operational manipulation such as, but not limited to, lifting, holding, or grasping with a specified skin contact time period (for any length of time).

End item designs having surfaces necessitating intentional crew contact should be designed such that nominal surface temperatures are non-hazardous for bare skin contact. For end items susceptible to temperature changes, design provisions should be in place such as active thermal management (for example: fans, heaters, furnaces, and active cooling devices) that prevent surfaces from exceeding the acceptable range for bare skin contact.

Operational Controls

End Items with a non-compliant surface that is not nominally exposed (e.g. the surface is shielded, inside the rack, etc.) may utilize an operational control prior to intentional contact. The use of operational controls such as a cool-down or warm-up wait time and/or PPE should be coordinated with the operations community and approved by the ISRP. The wait time should not negatively impact operations. Worst case T_{ES} should be considered in the generation of the operational control analysis to define the minimum wait time for T_{ES} to reach the non-hazardous touch temperature range.

Utilizing T_{PM}

Hot Temperature Hazards (exposed surface temperature (T_{ES}) > 45°C (113°F))

- A. For incidental contact, calculate T_{PM} and implement control for hazard as follows.
1. If T_{ES} is less than or equal to T_{PM} ($T_{ES} \leq T_{PM}$), bare skin contact is permissible.

SSP 51721

Baseline

2. If T_{ES} is greater than T_{PM} ($T_{ES} > T_{PM}$), bare skin contact is not permissible; implement design control for hazard.
- B. For intentional contact, calculate T_{PM} for the expected contact time and implement control for hazard as follows.
1. If T_{ES} is less than or equal to T_{PM} ($T_{ES} \leq T_{PM}$), bare skin contact is permissible.
 2. If T_{ES} is greater than T_{PM} ($T_{ES} > T_{PM}$), bare skin contact is not permissible; implement design control for hazard.

Cold Temperature Hazards (exposed surface temperature (T_{ES}) < 0°C (32°F))

- A. For incidental contact, calculate T_{PM} and implement control for hazard as follows.
1. If T_{ES} is greater than or equal to T_{PM} ($T_{ES} \geq T_{PM}$), bare skin contact is permissible.
 2. If T_{ES} is less than T_{PM} ($T_{ES} < T_{PM}$), bare skin contact is not permissible; implement design control for hazard.
- B. For intentional contact, calculate T_{PM} for the expected contact time and implement control for hazard as follows.
1. If T_{ES} is greater than or equal to T_{PM} ($T_{ES} \geq T_{PM}$), bare skin contact is permissible.
 2. If T_{ES} is less than T_{PM} ($T_{ES} < T_{PM}$), bare skin contact is not permissible; implement design control for hazard.

Calculating Permissible Material Temperature (T_{PM}):

When calculating T_{PM} for intentional contact, a minimum time of 10 seconds applies. Where contact time for nominal operations is planned to exceed 10 seconds, time increments for up to 30 seconds, up to 60 seconds, or infinite time are to be used. Because contact time is a factor in establishing permissible material temperature, calculate T_{PM} using higher or infinite contact time. When a time less than infinite time is used to calculate T_{PM} , the planned task time should be determined through a crew task analysis and be encompassed by the selected time increment.

The equation for T_{PM} assumes the object material is homogeneous. If the object is a layup of different materials (i.e., is comprised of layers), T_{PM} is to be calculated using the thermo-physical properties of the material with lowest value for inverse thermal inertia. Alternately, with justification, T_{PM} can be calculated using the thermo-physical properties of the material in the layup that is the largest contributor to the change in skin temperature. Additional information on calculating T_{PM} can be found in the NASA/SP-2010-3407.

Figure D.4.9.2.1-1 (Hot T_{PM} Touch Temperature Limits) and Figure D.4.9.2.1-2 (Cold T_{PM} Touch Temperature Limits) illustrate hot and cold T_{PM} for incidental (unplanned) and intentional (planned) contact times and four common materials.

SSP 51721
Baseline

1. For incidental contact (unplanned contact time $t \leq 1$ second):

$$T_{PM} (\text{°C}) = a * (k\rho c)^{-1/2} + b$$

Where:

$(k\rho c)^{-1/2}$ = inverse thermal inertia of material (cm²°C sec^{1/2})/cal

(Table 4.9.2.1-1: Inverse Thermal Inertia for Commonly Used Materials)

a, b = constants in Table D.4.9.2.1-2 (Constants for Incidental (Unplanned) ($t \leq 1$ s) Contact)

2. For intentional contact, (planned skin contact for any length of time):

$$T_{PM} (\text{°C}) = a * (k\rho c)^{-1/2} + b$$

Where:

$(k\rho c)^{-1/2}$ = inverse thermal inertia of material (cm²°C sec^{1/2})/cal

(Table D.4.9.2.1-1)

a, b = constants in Table D.4.9.2.1-3 (Constants for Intentional (Planned) Contact)

TABLE D.4.9.2.1-1 INVERSE THERMAL INERTIA FOR COMMONLY USED MATERIALS

Material	Inverse Thermal Inertia ($k\rho c$) ^{-1/2} (cm ² °C sec ^{1/2})/cal
Aluminum (6061T-6)	2.2
316 Stainless Steel	5.9
Glass	28.8
Teflon	57.5
Nylon Hook Velcro	586 (effective)
k = thermal conductivity ρ = density c = specific heat	

TABLE D.4.9.2.1-2 CONSTANTS FOR INCIDENTAL (UNPLANNED) (T ≤ 1 S) CONTACT

time (s)	$(k\rho c)^{-1/2}$	Hot		Cold	
		a	b	a	b
1	≤ 43.5	0.92	69.97	-1.16	0
	> 43.5	0.92	69.97	-0.88	-12.29

TABLE D.4.9.2.1-3 CONSTANTS FOR INTENTIONAL (PLANNED) CONTACT

time (s)	Hot		Cold	
	a	b	a	b
10	0.48	50.07	-0.71	4.78
30	0.46	46.61	-0.62	9.51
60	0.45	45.90	-0.53	10.00
∞	0.42	44.87	-0.37	10.00

Note: When calculating T_{PM} for intentional contact, use contact time of 10 seconds, 30 seconds, 60 seconds, or infinite time, as appropriate.

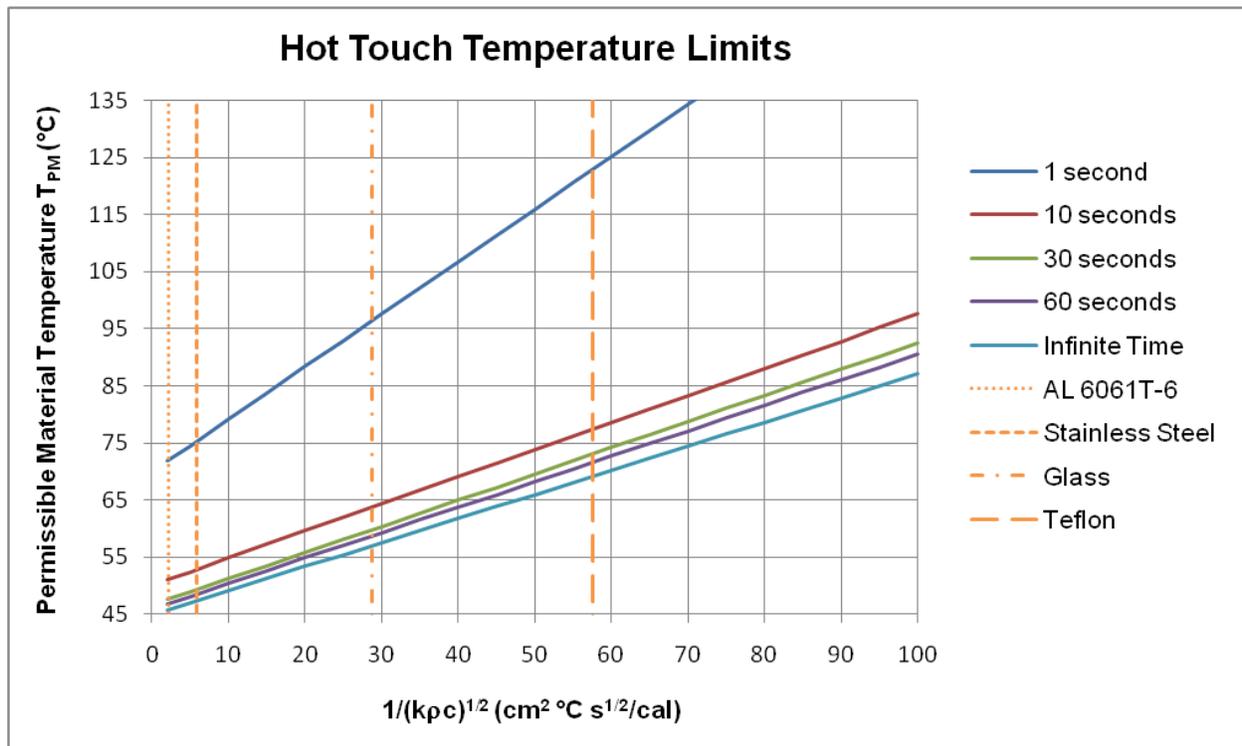


FIGURE D.4.9.2.1-1 HOT T_{PM} TOUCH TEMPERATURE LIMITS

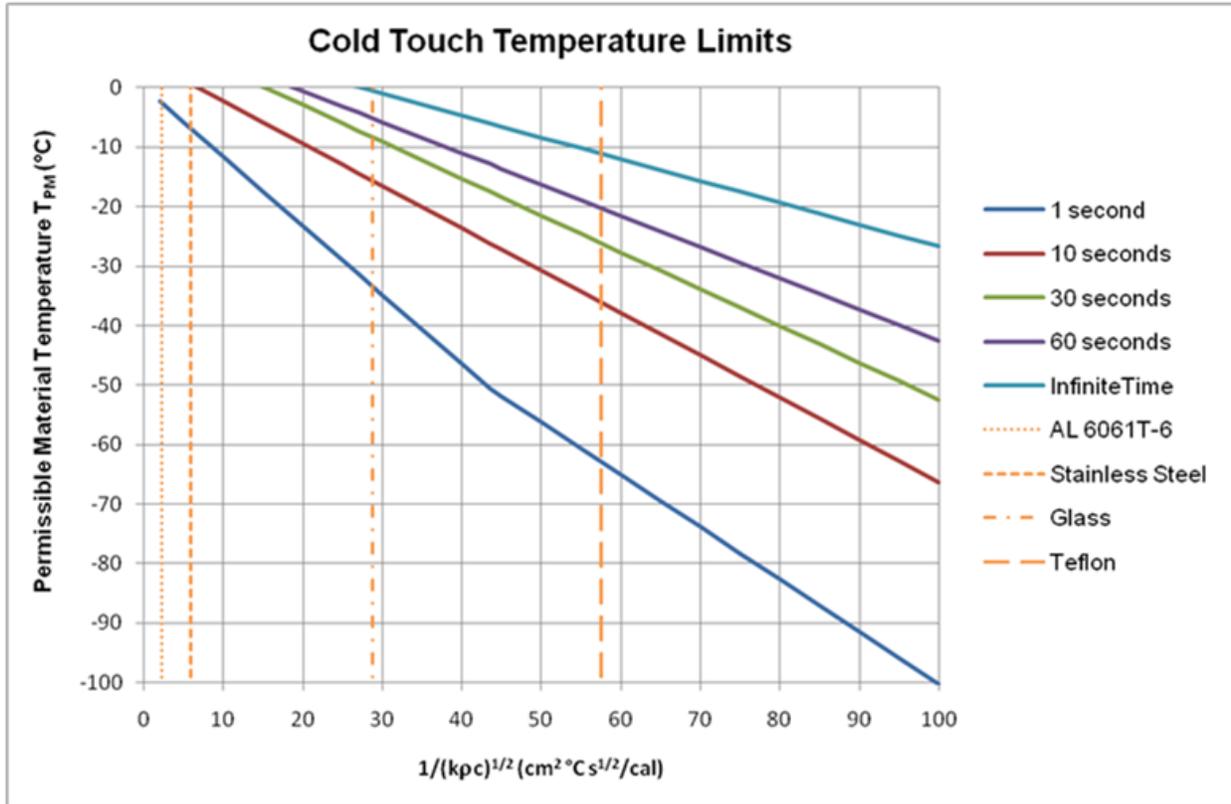


FIGURE D.4.9.2.1-2 COLD T_{PM} TOUCH TEMPERATURE LIMITS

D.4.9.4.1 Rationale – Lasers - General

This requirement is applicable for all end items with lasers.

The ANSI standard provides for the safe use of lasers and laser systems by providing laser classifications according to their relative hazards and then specifying appropriate controls. The basis of the hazard severity is the ability of the laser beam to cause biological damage to the eye or skin during use. This standard is used to protect the crew as well as ground-based general public with and without optical aid consideration. The ANSI standard also provides the Maximum Permissible Exposure (MPE) for each classification. Use of ANSI Z-136.1 2007 or newer is acceptable and should be specified when providing data to the NASA SME, the JSC/Non-Ionizing Radiation (NIR) Group.

End item laser classification should be done based on vendor-provider data or through testing of the laser at the source. Any modifications made to a COTS laser (i.e. change in use or power input/output, etc.) should be assessed to confirm there is no change in the laser output at the source as this may change the laser classification. Testing of the maximum output (based on max power or energy to the laser with no inhibits) may be needed to confirm there is no change in the laser classification.

SSP 51721

Baseline

Fully contained lasers are acceptable with no additional controls under the general laser requirement. If access to a contained laser is possible, safety interlocks or other controls should be provided.

Class 1 and 2 lasers are considered to be safe without containment or eye protection. Class 1 lasers are considered to be incapable of producing damaging radiation levels during operation. Class 2 lasers emit in the visible portion of the spectrum and eye protection is afforded by the eye aversion response.

Class 1M, 2M and higher lasers are not safe when magnified; therefore they require an ocular hazard assessment per section 4.9.4.2 to address the potential for viewing with ISS optical equipment (cameras, binoculars, etc.).

Class 3R, 3B and 4 are considered catastrophic and require full containment and two failure tolerant controls against crew exposure per section 4.9.4.3.

For lasers operating in free-space, additional guidance can be obtained from ANSI Z-136.2 (2012), Safe Use of Optical Fiber Communication Systems Utilizing Laser Diode and LED Sources, and ANSI Z-136.6 (2015), Safe Use of Lasers Outdoors, as referenced in ANSI Z-136.1. These references are not specific to spaceflight so additional information and guidance would be needed from the NASA SME to apply these to spaceflight.

D.4.9.4.4 Rationale – Broadband Light from Artificial Sources

This requirement is intended to prevent ocular injury and skin damage caused by overexposure to visible light from artificial sources. Examples of artificial light sources include LEDs, illumination lamps and display screens. Artificial visible light sources with an average output of 10,000 nits (1 nit = Candela per meter squared or Cd /m²) or less are not considered hazardous. The value of 10,000 nits is a commonly utilized specification in commercial hardware and is established based on guidance from the ACGIH (2014 or newer).

Visible sources that exceed 10,000 nits should use the information provided in SSP 50005, section 5.7.3.2.1.C to determine the TLV. The information in ACGIH allows for the quantification of the relationship between source strength and acceptable exposure times for each of four potential injury pathways, including: retinal thermal injury due to exposure to visible light, retinal photochemical injury due to chronic exposure to blue-light, thermal injury to the ocular lens and cornea due to infrared exposure, and exposure of the unprotected skin or eye to ultraviolet radiation.

D.4.9.5.1 Rationale – Emergency Egress Path Indication

The ISS will visually indicate emergency egress hatches in the absence of power to general area lighting by using glow in the dark indicators for the ISS EEGS. In order to provide emergency path marking, the indicators must produce a minimum of 2 mcd/m², which is the industry safety standard for minimum luminance visibility (ISO

SSP 51721
Baseline

16069, *Graphical Symbols – Safety Signs – Safety Way Guidance Systems (SWGS), section 7.3.2).*

Emergency egress path indicators need to be able to produce enough light for a long enough duration in total darkness in order to guide the crew back to the Soyuz in the event of an emergency. Charge lighting for glow in the dark material is assumed to be standard white light (any source – LED, fluorescent, etc.).

An illuminating material ASTM rating of 600/90 mcd/m² is defined as: a glow in the dark material, when charged by 1000 lux (white light) for 5 minutes, will have a luminance of 600 mcd/m² after 10 minutes and 90 mcd/m² after 1 hour. The EEGS is required to maintain above the minimum luminance visibility of 2 mcd/m² after 8 hours of dark exposure. 600/90 mcd/m² material meets this requirement when only 50 lux of illumination is applied for 10 minutes.

The EEGS markers will also need to meet the requirements for flammable materials, similar to Velcro and labels (i.e., no larger than 4 square inches and no closer than 2 inch spacing per section 4.7.1.1) and must be no smaller than 1 inch in diameter to ensure adequate visibility.

D.4.9.6.1 Rationale – Egress from End Item Apparatus

The crew must be able to free themselves from any apparatus such that they can evacuate/relocate if necessary. Thirty seconds is based on engineering judgment and is meant to represent expedited egress in the event of emergencies. This 30 second timeframe is a subcomponent of the overall three minute time to isolate a volume by closing a hatch. Margin is already accounted for in the overall egress scenario, so no safety factor needs to be added to account for microgravity conditions.

If the crew can evacuate by detaching themselves rather than complete removal of the apparatus (e.g., exercise equipment harness), that is acceptable as long as it does not impede their ability to don emergency breathing apparatus and/or emergency entry suits.

Desktop analysis/engineering judgment is typically adequate to satisfy this requirement. If the ISRP determines analysis is inadequate, a demonstration is necessary.

D.4.9.6.2 Rationale – Intramodule Emergency Egress

A minimum emergency translation corridor of 32 X 45 inches (81 X 114 cm) is maintained within the USOS modules and 32 x 32 inches (81 x 81 cm) within the Russian Segment. A 32 X 45 in (81 X 114 cm) corridor allows for a crewmember to reverse direction at any point along the corridor during emergency situations. Temporary intrusions or items that can be quickly relocated or reconfigured will be assessed by the ISRP on a case by case basis. Rack rotation due to maintenance and rack translation are acceptable protrusions into the emergency translation corridor. Cables, hoses, and wires in the translation corridor must be restrained to prevent entanglement during emergency egress. Cable/hose restraint requirements are levied via the associated IRD and detailed cable management is left up to crew discretion.

SSP 51721
Baseline

Desktop analysis/engineering judgment is typically adequate to satisfy this requirement for individual end items. If the ISRP determines the hardware has potential to impact the translation path, the end item will be included in the integrated assessment performed by the Internal Volume Configuration Working Group (IVCWG).

D.4.9.6.3 Rationale – Volume Isolation

In emergency situations (i.e., fire, depress, or toxic atmosphere), the crew must be able to isolate themselves or the affected module within three minutes. The volume to be isolated could be more than one module but closing one hatch would isolate the crew from the hazard. Preventing stowed cargo from interfering with the ability to egress and isolate a volume within three minutes is accomplished through compliance with the constraints and requirements for stowed cargo identified in the Generic On-Orbit Stowage Capabilities and Requirements: Pressurized Volume (OSCAR), SSP 50621, Generic On-Orbit Stowage Capabilities and Requirements: Pressurized Volume. An integrated hatch closure assessment is performed per HR ISS-NTN-001, Cable Drag-Through Assessment, prior to each flight to evaluate drag throughs and ensure each hatch can be closed within three minutes. The integrated assessment allocates 1 minute for crew reaction time (including items such as waking up, translating to the hatch, and/or egressing end item apparatus) and 30 seconds for actual hatch closure. In an emergency situation, the intermodule ventilation valve is closed automatically to ensure environmental isolation and although the crew would confirm the valve is closed, it is not considered an impact to the timeline. Time may also be required to clear the hatch of drag throughs, etc. The time allocated for a specific end item removal or reconfiguration can vary based on location and must be assessed at an integrated level and approved by the ISRP.

D.4.10.1.1 Rationale – Incidental Contact

The values in this table assumes the skin temperature as the boundary (from medical limits and testing), with a linear conductor to account for the contact resistances and material thermal resistances of the glove (based on testing), and the maximum allowable heat rate (based on testing). The end item provider must apply these values to the object to be contacted by the skin boundary through the prescribed linear conductor. The objects initial temperature and material properties must be considered.

The EMU gloves can withstand contact temperatures of -180 to 235 degrees F (-118 to 113 degrees C) with a contact pressure of 0.1 psi (0.7 kPa) without discomfort to the hand for nearly 5 minutes. The TMG can withstand these contact temperatures under any operational scenario.

The EMU suit and EMU gloves have some margin exceeding the ISS touch temperature requirement ranges under certain operational circumstances. These capabilities vary by EMU region (suit, glove palm, glove back), applied pressure (0.1 psi to 10.0 psi), and duration (3 seconds to unlimited). Details of these capabilities can be found in NCR-EVA-XA002, ISS Hardware/Module Touch Temperature Exceedances. This generic NCR can be referenced in the associated HR if an analysis shows that the hardware temperature is within the guidelines of the touch temperature testing outlined in the

SSP 51721

Baseline

NCR attachment and the EVA AIT determines that the required EVA interaction with the hardware meets the limitations of the testing. Any potential contact with hardware exceeding the ISS touch temperature requirements must be assessed against these factors and coordinated by the EVA AIT.

Analysis is the preferred approach to verify this requirement because recreating the EVA environment can be too costly or impractical.

End item temperatures can be controlled passively or actively. Passive controls include the choice of material, coatings or insulation while active controls include items such as heaters or cold plates.

D.4.10.2.1 Rationale – Sharp Edges and Protrusions

End items in EVA accessible areas must be designed to preclude sharp edges and protrusions or must be covered in such a manner as to protect the crew and critical support equipment. The thin material specification typically applies to radiator or cold plate fins.

If the end item design cannot be compliant (i.e., Star Tracker), non-compliant areas may be able to be operationally controlled (Once negotiated with the operations community) by defining a No Touch Area (NTA) that will be used as a warning in crew procedures. NTA's are not allowed in primary translation paths.

Equipment that is intended to go into a pressurized volume for planned maintenance or storage must also meet the IVA sharp edge requirements specified in the applicable IRD.

In the event that the hardware provider does not meet each of the sharp edge criteria, the hardware provider could potentially use a successfully-passed Vehicle Inspection Test Organization sharp edge inspection in lieu of meeting all applicable requirements, but only with the approval of the EVA AIT and the ISRP. A generic NCR-EVA-XX-004, which can be used at the discretion of the ISRP has been generated for hardware that meets this criteria. Disclosure of the sharp edge violation is required in the appropriate HR. Reference to the generic NCR in the HR allows for the violation to be accepted without implementing an operational control.

D.4.11.1 Rationale – Micrometeoroid and Orbital Debris

MMOD strikes to externally mounted end items with catastrophic hazard potential can result in loss of the ISS or endanger the crew.

*Shielding is one method of reducing the risk. The Assessed PNP of the shielding must be equal or greater than the required minimum PNP that is determined from the lesser value of 0.9999 or $0.99999^{(A*Y)}$. The assessed PNP must be calculated for the cumulative on-orbit exposure time of the end item beginning with the initial launch date. The required minimum PNP parameter $A = \text{Total hazardous impact surface area in square meters}$ while $Y = \text{Exposure time in years}$.*

SSP 52005 specification is for payloads but the same requirements are applicable to any/all MMOD critical end items (those with potential to create a catastrophic hazard).

SSP 51721
Baseline

SSP 50808 specification is for cargo and crew transfer vehicles.

Requirements defined here and in SSP 52005 and SSP 50808 do not alter or define the existing ISS process for evaluation of MMOD contribution to ORU failure rates or ORU procurement decisions. ORU procurement decisions based on predicted MMOD failure events are evaluated on a case by case basis and decisions made by appropriate ISS boards.

NASA uses the risk analysis program, Bumper-3, to calculate PNP. The code quantifies the probability of penetration of shielding and the damage to spacecraft equipment as a function of the size, shape, and orientation of the spacecraft; the parameters of its orbit; and the impact damage resistance of each spacecraft. The Bumper-3 software was specifically designed for the ISS and contains several dozen ballistic limit equations that are based on results from thousands of hypervelocity impact tests conducted on ISS shielding. The meteoroid environment is defined in the NASA Meteoroid Engineering Model Release 2.0 (MEM R2). The orbital debris environment is defined in NASA/TP-2014-217370, NASA Orbital Debris Engineering Model (ORDEM) 3.0 – User's Guide, using an altitude of 400km and orbital inclination of 51.6° for the PNP assessment.

For the purposes of MMOD, a penetration is defined as damage/failure to stored energy devices that causes a hazard to crew or ISS survivability. Typically, penetration is defined as a partial or complete perforation of the pressure vessel or casing, detached spall from the pressure vessel wall, damage to the pressure vessel that would allow unstable crack growth, or deformation of a casing of rotating machinery such that the deformation could intrude into the dynamic envelope of the rotating device.

Shielding might not be necessary if the assessed PNP is greater than the required probabilities documented in the specification.

D.4.12.1 Rationale - Solid Propellant Rocket Motors

Premature firing of a solid propellant rocket motor, while the end item is closer to the ISS than the minimum safe distance, is a catastrophic hazard.

Pyrotechnics with Safe and Arm (S&A) devices can be used to control propellant firing.

A S&A device provides a mechanical interrupt in the pyrotechnic train immediately downstream of the initiator.

In addition to the S&A, at least two independent electrical inhibits to prevent firing of the motor is necessary if the S&A device will be in the "safe" position until the end item reaches a safe distance from the ISS. At least three independent electrical inhibits are necessary, in addition to the S&A, if the S&A device will be rotated to the arm position prior to the end item reaching a safe distance from the ISS.

Monitoring is a function of the design and operations as follows:

- If no rotation of the S&A is planned prior to a safe distance, then it is necessary for the design to include the capability to monitor the status of the S&A device and one electrical inhibit in near real-time until final separation of the end item*

SSP 51721
Baseline

from the ISS. No monitoring is required if the end item qualifies for the unpowered bus exception of section 4.5.2.2.

- *If the S&A will be rotated to arm prior to a safe distance, then it is necessary for the design to include the capability for the flight or ground crew to have continuous real-time monitoring to determine the status of the S&A and to ensure that two of the three electrical inhibits are in place (section 4.5) prior to rotation of the S&A and separation of the end item from the ISS.*

If the S&A device is to be rotated to the arm position while the end item is attached to the ISS; or if the solid rocket motor propulsion subsystem does not qualify for the unpowered bus exception of section 4.5.4, three inhibits are required to control the hazard. In determining compliance with section 4.5.2, the S&A device in the safe position will be counted as one of the required inhibits.

It is necessary for the planned deployment orientation to take into account many variables such as deployment method, appendage orientation, and control authority. The orientation is coordinated with the ISSP.

D.4.12.2 Rationale – Liquid Propellant Propulsion System

The premature firing of a liquid propellant propulsion system can cause a catastrophic hazard. 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.

Leakage and rupture of pressure systems are addressed in section 4.2.2.

For each propellant delivery system, a minimum of two mechanically independent flow control devices in series are needed to prevent engine firing. If in a primary EVA translation path or using monopropellant, it is necessary for each propellant delivery system to contain a minimum three mechanically independent flow control devices in series to prevent engine firing. It is necessary for these devices to prevent contact between the fuel and oxidizer as well as prevent expulsion through the thrust chamber(s). A minimum of one of the three devices is needed to be fail-safe, i.e., return to the closed condition in the absence of an opening signal. Propellant systems that require an igniter (i.e. non-hypergolic) may be permitted to use an igniter inhibit as part of flow and hazard control, subject to review and approval by ISRP.

When a valve is used as a flow control device, the number of inhibits to valve activation determines the failure tolerance against fluid flow.

Opening the Isolation Valve

If an end item with a large liquid propellant thruster system also uses a small reaction control thruster system for attitude control, the isolation valve in a common distribution system can be opened after the end item has reached a safe distance for firing the reaction control thrusters provided the appropriate electrical inhibits and monitoring are

SSP 51721
Baseline

designed into the system and two mechanical flow control devices remain to prevent thrusting of the larger system. Isolation valves can be opened during ground servicing.

Electrical Inhibits

While the end item is closer to the ISS than the minimum safe distance for engine firing, at least three independent electrical inhibits that control the opening of the flow control devices are necessary. It is necessary for the electrical inhibits to be arranged such that the failure of one of the electrical inhibits will not open more than one flow control device. If the isolation valve will be opened under the conditions of above "Opening the Isolation Valve" paragraph prior to the end item achieving a safe distance for firing a large thruster, three independent electrical inhibits are needed to control the opening of the remaining flow control devices for the large thruster system.

Monitoring

It is necessary for at least two of the three required independent electrical inhibits to be monitored by the flight or ground crew until final separation of the end item from the ISS. The position of a mechanical flow control device may be monitored in lieu of its electrical inhibit, provided the two monitors used to meet the above requirement are independent. Either near real-time or real-time monitoring is required as defined in sections 4.5.2.1 and 4.5.2.2. It is necessary for one of the monitors to be the electrical inhibit or mechanical position of the isolation valve. Monitoring will not be required if the end item qualifies for the unpowered bus exception of section 4.5.2.3. If the isolation valve will be opened prior to the end item achieving a safe distance from the ISS, all three of the electrical inhibits that will remain after the opening of the isolation valve is necessary to be verified safe during final pre-deployment activities by the flight or ground crew.

Pyrotechnic Isolation Valves

If a normally closed, pyrotechnically initiated, non-welded parent metal valve is used, fluid flow or leakage past the barrier will be considered mechanically non-credible.

Plume impingement on the ISS can cause permanent damage to ISS hardware. Plume impingement pressures, thermal (passive and heat flux), loads, disturbance effects and contamination acting on the ISS is not to exceed limits documented in SSP 50808, section 3.2.2.6.4.5.2. The analysis will be jointly performed by the ISSP and the end item provider. All vehicles with thrust capabilities will be assessed for compliance.

Propellant venting is addressed in section 4.7.2.1.

D.4.12.3 Rationale – Adiabatic/Rapid Compression Detonation

For the inadvertent opening of isolation valves in a hydrazine (N₂H₄) propellant system, it is necessary to be controlled as a catastrophic hazard or the system is shown to be insensitive to ACD. Hydrazine systems will be considered sensitive to ACD unless insensitivity is verified by testing on flight hardware or on a high-fidelity flight type system that is constructed and cleaned to flight specifications.

SSP 51721

Baseline

For the inadvertent opening of isolation valves in a hydrazine (N₂H₄) propellant system, it is necessary to be controlled as a catastrophic hazard or the system is shown to be insensitive to ACD. Hydrazine systems will be considered sensitive to ACD unless insensitivity is verified by testing on flight hardware or on a high-fidelity flight type system that is constructed and cleaned to flight specifications.

System analysis is necessary to characterize the worst-case transient pressures throughout the system for all operational environments on the ground and in flight. Analysis will be validated by the system testing.

Test plans are submitted to the ISRP as part of the appropriate HR. If the design solution is to fly wet downstream of the isolation valve, it is necessary for the hazard analysis to consider other issues such as hydrazine freezing or overheating, leakage, single barrier failures, and back pressure relief. It is necessary for priming into evacuated lines to be designed to prevent ACD. Monitoring of pressure on downstream hydrazine lines is necessary.

D.4.12.4 Rationale – Propellant Overheating

Components capable of heating the system are heaters, valve coils, etc. Raising the temperature of a propellant above the fluid compatibility limit for the materials of the system is a catastrophic hazard. Typically, heaters are sized to not overheat the system in a failed-on scenario.

The use of inhibits, cutoff devices, and/or crew safing actions can be used to make the system two failure tolerant to overheating.

D.4.12.6 Rationale – Monitoring Propulsion System Status

It is necessary for the end item to provide real-time data related to pressure, temperature, and quantity gauging of propulsion system tanks, components, and lines to ISS. Monitoring gives the ISS insight into the health of the propulsion system and provides notice of any developing issues. Refer to sections 4.5.1 and 4.5.2 for real-time monitoring.

If real-time monitoring is not practical during some mission phases such as there is no system power available, the end item is to show two failure tolerance in the design. Refer to section 4.5.2.3.

D.4.13.1 Rationale – Pyrotechnic Loss of Function (Must Work)

Where failure to operate causes a catastrophic hazard, pyrotechnic operated devices are designed, controlled, inspected, and certified to criteria equivalent to those specified in JSC 62809. End Item hardware provider should consult the NASA JSC Pyrotechnics Office for guidance as early as possible. The data required for ISRP review are identified in SSP 30599.

D.4.13.2 Rationale – Electrical Explosive Devices

If the MIL-STD-1576 is unavailable to the end item provider, a NASA approved equivalent can be used.

SSP 51721

Baseline

Over the years it has been NASA and DoD's experience that the most reliable and preferred initiators are the NASA Standard Initiators (NSI). If other initiators are used, the hardware provider needs to perform an extensive qualification and acceptance test program. NSI's have undergone extensive testing to show that they will function as intended when used as designed. By selecting these type of devices the end item provider can avoid costly qualification and acceptance testing.

Initiators other than NSI's may not have a history that shows that it has undergone extensive testing that they will function as intended. The qualification and acceptance program will be extensive and approved by the NASA JSC Pyrotechnic Office. The program will include a test plan and test data that will be provided and approved at each step.

D.4.13.3 Rationale – Pyrotechnic Electrical Circuits

If designed incorrectly, the firing circuit could cause a hazard by firing prematurely or not firing as expected. The following information must be used in the design of the firing circuit.

The design of connectors and pins used with EEDs prevent the possibility of premature firing from short circuits that could occur due to manufacturing defects, bent pins, or contamination.

Firing circuits for each EED are isolated and capable of carrying the initiator firing current. The circuit has the ability to be safed and indicate if it is armed or disarmed. Independent timing circuits used as logic for firing EEDs are to be fail-safe.

Monitor circuits and test equipment limit the current and utilize best practices to preclude unintentional electrical paths.

The electro-explosive subsystem firing sources use separate and dedicated power distribution points.

The firing source circuit return side is isolated.

The firing circuits are grounded at one point only and it is not a structural ground. Relays, fuses, or current limiting resistors may be used as positive protection for line-to-line and line-to-ground shorts.

All pyrotechnic circuitry wiring uses isolated shielded twisted pairs unless other configurations can be shown to be more effective.

Electrical cables meet section 4.3.7 with no splicing and connectors provide for mating and demating.

Cable shielding provides a minimum of 90 percent of optical coverage with 360 degree continuous shields that are grounded to structure. Multiple point grounding of cable shields to structure is recommended. The method for determining optical coverage is determined in accordance with the following formula. (Section 5.2(b), MIL-STD-1576, modified)

SSP 51721
Baseline

$$K = 100 (2F - F^2)$$

$$F = (NPW) / (C \sin A)$$

$$\tan A = [2\pi (D + 2W) P] / C$$

where:

K	=	percent coverage of braided shield, %
F	=	optical coverage parameter
A	=	braid angle, degrees
C	=	number of carriers
D	=	inside diameter, in
N	=	total number of ends
P	=	picks per inch
W	=	diameter of individual braid wire, in

All current-carrying components and conductors are electrically insulated from each other and system ground.

Both the high voltage side and the return side of the stored energy output firing circuit have inhibits.

If the inhibits in the firing circuit (high and return voltage sides) are independent (one firing command closes the high voltage side and a different firing command closes the return voltage side), a minimum of one additional inhibit is necessary which prevents storing energy and arming the circuit. Otherwise if the firing circuit inhibits are not independent (one firing command closes both the high voltage side and return side inhibits), a minimum of two independent inhibits is necessary which prevent storing energy and arming the circuit and in the design of the arming circuit inhibits, at least one of the inhibits interrupts the arming power source and the other interrupts the return leg of the arming power source.

In meeting Section 4.3.7, the analysis/test includes not only the firing output circuits, but all of the firing circuit elements, in particular the control circuits that can couple power to the EED. The radiated and conducted electromagnetic environment produces a peak alternating current power level at the EED and this level is compared to the maximum direct current no fire power level of the EED, which is determined from the square of the direct current no fire current times the nominal bridgewire resistance.

The verification can be part of the normal EMC compliance program used for the overall (completely assembled and powered-up) system, e.g., connect an ordnance simulator or power measuring device to the firing output circuit. The monitoring device minimizes its effects on the overall system. The direct current detector has the capability of detecting pulses at least as short as one millisecond. The ordnance simulator and measuring device have sensitivities to levels far less than the no fire level of the EED so

SSP 51721
Baseline

that a 16.5dB safety margin can be demonstrated without irradiating the system at damaging levels.

The firing circuit including the EED is completely shielded or shielded from the EED back to a point in the firing circuit at which isolators eliminate RF entry into the shielded portion of the system.

Firing circuit switching devices are protected as required to prevent inadvertent operation or degradation.

The electro-explosive subsystem is designed to limit the power produced at each device in the firing circuit that can complete any portion of the firing circuit.

The electrical pyrotechnic circuit elements have low DC bonding resistance to connection points of the shielded system, metallic enclosures, and structural ground. Reefing line cutters are exempt from this measurement.

EEDs are designed to withstand a constant direct current firing pulse without initiation or deterioration of performance (dudding).

EEDs are protected from electrostatic hazards by the placement of bleed resistors from line-to-line and from line-to-ground (structure). The placement of line-to-structure static bleed resistances is not considered to violate the single-point ground requirements of this specification as long as the parallel combination of these resistors are 10k Ω or more.

EEDs are not fire, dud, or deteriorate in performance as a result of being subjected to an electrostatic discharge.

D.4.13.4 Rationale – Pyrotechnic Mechanical Containment

This pyrotechnic containment section covers requirements for debris containment from pyrotechnics use, including design, development, and qualification.

Tensile test data is necessary for component parts that are heat treated after receiving from the mill. Tensile test data is also necessary for component parts that have to withstand operating pressures or primary structural loads or both.

A minimum of three standard tensile coupons, in accordance with ASTM E8, Standard Test Methods of Tension Testing of Metallic Materials, are processed with the component parts. Before acceptance, the supplier conducts tensile tests on each coupon as defined by the procuring agency, or if no specific direction is provided, tensile testing is too completed in accordance with ASTM E8.

As a minimum, ultimate strength, 0.2 percent offset yield, and elongation data is obtained from the test coupons and recorded on the lot acceptance data sheets. Failure to meet the minimum material tensile acceptance criteria causes rejection of the component parts associated with those test coupons.

For pyrotechnic device metallic component parts that are not heat treated after machining and are not exposed to operating pressures or primary structural loads, the

SSP 51721
Baseline

standard mechanical properties test report delivered with the raw material will suffice, provided all test data required by the material specification are included in the report.

All threaded parts are positively locked. Liquid locking compounds may be used provided the implementation meets the following restrictions:

- *Liquid locking compounds are not to be used as secondary locking features on safety critical fasteners.*

For the purposes of this requirement, safety critical fasteners are defined as:

- *All primary or secondary structural fasteners used in the exterior and interior of flight modules.*
- *All non-structural fasteners used exterior to flight modules, which could pose a FOD risk to vehicle operations and which have not been vibration tested during qualification or acceptance of the hardware.*

Where applicable, locked-shut capability is to be demonstrated with redundant charges operating simultaneously. This demonstration is not applicable to premature initiation failure modes. Demonstration of this capability is not necessary if the release of shrapnel, debris, or hot gasses does not jeopardize crew safety or mission success as verified by analysis using credible failure modes.

The design yield FOS and ultimate FOS of 1.4 are not applicable to the loads generated by the firing of the pyrotechnic charge.

For pyrotechnic devices that fire within an ellipsoid of a manned vehicle, an analysis to 1.5 times the maximum operating pressure may be substituted provided it includes 100 percent NDE. The maximum operating pressure is defined as the highest measured operating pressure from a minimum of five firings using nominal cartridge load. If the cartridge design, propellant or application make direct pressure measurements impractical or if a measured transient pressure spike establishes an unrealistic proof pressure requirement, an analytically derived proof pressure requirement may be established.

D.4.13.5 Rationale – Auto-Ignition

The auto-ignition temperature of a pyrotechnic device is the lowest temperature at which it spontaneously ignites in normal atmosphere without an external source of ignition, such as a flame or spark. Auto-ignition tests are to be performed to a minimum temperature level 50°F above the maximum expected temperature of the pyrotechnic device in question. Temperature rise rate of the test article and dwell time at maximum temperature is derived from the expected exposure cycles of the pyrotechnic device in question. The device is not required to function afterwards.

D.4.13.6 Rationale – Maximum Energy Test

Other suitable methods, such as adding powder into the firing cavity, may be applied. This requirement will be satisfied during qualification testing. Devices should not be

SSP 51721

Baseline

fabricated specifically to permit 115 percent overload if internal dimensions of the device do not permit overloading.

Devices that have the sole function of transferring detonation and energy within a pyrotechnic system are exempt from this requirement. This exemption applies to delay fuses and columns, Shielded Mild Detonating Cords, Flexible Confined Detonating Cords, and Confined Detonating Fuse assemblies.

Where multiple explosive components exist within a device, each component is uploaded simultaneously. Initiators, primers, delay columns, detonators and any device with the sole function of transferring energy is not uploaded to meet this requirement.

D.4.14.1 Rationale – Re-entry Human Risk

Each IP has a responsibility for re-entry human risk based on IP's law. For NASA sponsored end items the risk of human casualty on the ground is limited to less than 1 in 10,000 as required per NASA-STD-8719.14A, Process for Limiting Orbital Debris. Note that for NASA sponsored end items there could be additional applicable requirements in NASA-STD-8719.14A that must be met. In 1995, NASA established a policy of limiting the risk of world-wide human casualty from a single, uncontrolled re-entering space structure to 1 in 10,000. The principal factors used in calculating the risk of human casualty from uncontrolled reentries include the number of debris expected to reach the surface of the Earth, the kinetic energy of each surviving debris, and the amount of the world population potentially at risk. The last factor is a function of both the orbital inclination of the space structure prior to re-entry and the year in which the re-entry occurs. Extensive human casualty studies by the U.S. Government, including ones by the Department of Defense and the Department of Energy, have examined the probability of injury and/or death from falling debris for a variety of impacting kinetic energies to humans. A kinetic energy threshold criterion of 15 joules is widely accepted as the minimum level for potential injury to an unprotected person. Existing NASA Orbital Debris Program Office (ODPO) analysis demonstrates that objects with mass ≤ 5 kilogram will not violate the 1/10,000 NASA requirement.

Debris Assessment Software (DAS) is provided by the NASA ODPO located at JSC. For details on DAS, refer to NASA STD 8719.14A. If the DAS result indicates a risk greater than the IP limit, the end item could still be compliant, but an Object Reentry Survival Analysis Tool (ORSAT) assessment is necessary to determine the actual risk. The ISS Vehicle Integrated Performance Environments and Resources (VIPER) Team will coordinate with ODPO to determine whether additional analysis utilizing the higher-fidelity ORSAT is necessary to determine the risk to ground population due to the end item's re-entry into the Earth's atmosphere. End item providers must coordinate with the ISS VIPER Team until the analysis is complete.

D.4.14.2 Rationale - Trackability

The ability of the SSN to track end items is a function of its radar reflectivity and optical properties. This allows NASA to monitor the item for potential collision with the ISS or VVs. Data is acquired using ground-based radars, optical telescopes, and space-based telescopes.

SSP 51721
Baseline

In general, the smallest trackable object is considered to be a primarily metallic sphere with a minimum diameter of 10 cm. This determination is typically coordinated between the end item provider and NASA ISS Trajectory Operations and Planning (TOPO) group with the Joint Space Operations Center.

D.4.14.3 Rationale - Fragmentation

Minimizing unintentional fragmentation decreases the number of items to track and the probability of collision (P_c) with ISS, VVs, and casualty on the ground. For reference, the internal NASA standard for accepting no further mitigation of fragmentation risks is a 1/10,000 chance of fragmentation over the remaining life.

Fragmentation could be minimized by safing actions which could include depleting batteries, venting pressurized volumes, depleting on-board propellant, etc. by the end of mission. Safing actions would be necessary if these subsystems were of sufficient size to cause fragmentation.

This requirement does not consider subcomponent deployment as fragmentation.

D.4.14.4 Rationale – EVA Deploy Clearance

This velocity vector will ensure there is initial clearance of all ISS/VV structures. The object must be under acceptable EVA control which is characterized by the responsible EVA Office. The desired cone axis will be defined to the EVA crew in relation to readily identifiable landmarks such as structure or the horizon. This analysis can be performed by the ISS Manipulator Analysis, Graphics, and Interactive Kinematics (MAGIK)/ Configuration Analysis Modeling & Mass Properties (CAMMP) or comparable end item team.

The US or sponsoring IP should provide a means to bundle multiple jettison candidates from a single EVA into a single collected object to minimize number of items that are jettisoned.

D.4.14.5 Rationale – Robotic Deploy Clearance

This velocity vector will ensure there is initial clearance of all ISS/VV structures. The half angle of accuracy of the deploy mechanism is defined by the robotics deploy mechanisms system owner and implementing ISS robotics team.

Worst-case conditions include accuracy of the deploy mechanism stacked up with all associated robotics pointing accuracies (like SSRMS accuracy for example) and potential accuracy errors induced by the deploy force. This analysis can be performed by the ISS MAGIK/CAMMP or comparable end item team.

D.4.14.6 Rationale - Controllability

Examples of capabilities that can modify orbit energy are attitude control systems, propulsion systems, tethers, and deployable subcomponents. In addition to the general inhibit and monitoring requirements of sections 4.5.1 and 4.5.2, the Monitoring Of Deployable End Items from ISS requirements of section 4.5.3 also apply. Operation concepts and flight plans should demonstrate how end items will keep the ISS, VVs and

SSP 51721
Baseline

other on-orbit assets safe from collision. This can be accomplished by demonstrating that according to the nominal flight plan and within credible systems failure scenarios as defined by the end item provider and ISRP, the candidate cannot at any time maneuver itself onto a trajectory that could intercept the ISS within 10 days. 10 days is the TOPO office's best estimate of how long it will take for United States Strategic Command (USSTRATCOM) to perform orbit determination on the object, and for the TOPO office to assess if the object may return to ISS and plan a avoidance maneuver if deemed necessary.

D.4.14.7.1 Rationale – Keep-Out Sphere

This ensures safe relative motion with the ISS. There must be a velocity component in the $-V_{bar}$ direction from anywhere within the allowed jettison cone. Relative motion analysis is completed, assuming deploy velocity of 0.05m/s, if the end item is EVA deployed or minimum velocity of robotic mechanism for robotic deploy. This analysis is typically completed by NASA TOPO group.

D.4.14.7.3 Rationale – R-Bar Crossing

ISS planned reboosts are performed with a 30-day interval on average. Requiring a minimum 30-day return makes it likely that the ISS will perform a planned reboost that would mitigate the return of a low drag end item.

In addition, a timeframe of 30 days provides flight control teams time to develop item tracking, monitor relative trajectory, and plan an avoidance maneuver to mitigate potential end item collision with the ISS. The ISS R-bar is along the line of the radius of the orbit with respect to Earth. Relative motion analyses are completed assuming deploy velocity of 0.05m/s, if the end item is EVA deployed or minimum velocity of robotic mechanism for robotic deploy. This analysis is typically completed by NASA TOPO group.