CHANGE NOTICE

Date Prepared: 22 July 2009

1.	2.	3. Code Ident.	4. Change Notice No.
Barrios Technology, Inc. 16441 Space Center Blvd, Suite B-100 Houston, Texas 77058	☐ Proposed ☒ Approved	5. Contract No.	DCN 004 6. Directive No. 010977
7. Document No./Rev. SSP 50021	8. Document Title Safety Requirements Document		9. SSCN No. 010977
10. Related Change No.	11. Change Title		

THIS NOTICE INFORMS RECIPIENTS THAT THE DOCUMENT IDENTIFIED BY THE NUMBER (AND REVISION LETTER) SHOWN IN BLOCK 7 HAS BEEN CHANGED. THE PAGES CHANGED BY THE CN BEING THOSE FURNISHED HEREWITH AND CARRYING THE SAME DATE AS THIS CN. THE PAGES OF THE PAGE NUMBERS AND DATES LISTED BELOW IN THE SUMMARY OF CHANGED PAGES COMBINED WITH NON-LISTED PAGES OF THE ORIGINAL ISSUE OF THE REVISION SHOWN IN BLOCK 7 CONSTITUTE THE CURRENT VERSION OF THIS SPECIFICATION.

12. DCN No.	13. Pages Changed (Indicate Deletions)	S*	A*	Date
004	Cover	S		
	Revision and History Page	S		
	i - viii	S		
	ix	A		
	3-31 – 3-36	S		
	A-2 – A-3	S		
	J-1 – J-34	A		
	Order of DCN Incorporation: DCN 001, 002, 003, 004			

14. Technical Concurrence

/s/ Vincent L. Berend 7/8/09

Date

* “S” indicates supersedes earlier page. “A” indicates added page.

SP 50021
Baseline

Safety Requirements Document

International Space Station Program

Baseline

Incorporates DCN 004

December 12, 1995

National Aeronautics and Space Administration
International Space Station Program
Johnson Space Center
Houston, Texas

REVISION AND HISTORY PAGE

REV.	DESCRIPTION	PUB. DATE
-	Initial Release (Reference per SSCD 000353, EFF. 08-16-96)	09-03-96
	DCN 001 (Reference per SSCD 001778, EFF. 11-17-98)	05-07-99
	DCN 002 (Reference per JPRCBD A096082/(1-1), dated 01-26-01)	04-06-01
	(SSCD 003826 authorizes an administrative action to update the documentation software applied to SSP 50021 from Microsoft Office 95 to the existing working version of Microsoft Office. This update also changes the acronym use of ISSP to ISS Program and allows the text to flow. All pages that have been affected by the implementation of this update have been included in this package and reflect the package release date header. No technical content has been impacted.)	
	DCN 003 (Reference per SSCD 007557, EFF. 07-08-04)	08-26-05
	Microsoft97 has been applied to SSP 50021 incorporating DCN 001, DCN 002, and DCN 003. This release is required in order to provide the community the appropriate software version of the document. No technical content has been impacted.	
	DCN 004 (Reference per SSCD 010977, EFF. 10-14-08 and SSCD 005144, EFF. 06-23-03)	07-08-09

TABLE OF CONTENTS

DCN 001

3.2.2.18 REMOVE AIRBORNE MICROBES

The purpose of this function is to remove airborne microbes from the <End Item> atmosphere.

The <End Item> shall limit the daily average airborne microbes in the <End Item> atmosphere to 1000 Colony Forming Units (CFU) per cubic meter.

3.2.2.19 MONITOR AIRBORNE MICROBES

The purpose of this function is to monitor the level of airborne microbes in the <END ITEM> atmosphere. The <END ITEM> shall monitor the <END ITEM> atmosphere for bacteria and fungi: with a sampling volume of 1 to 1000 liters of atmosphere. The <END ITEM> shall monitor bacteria with a sampling range of 0 to 1,125 colony forming units (CFU) per cubic meter and fungi with a sampling range of 1,250 CFU per cubic meter.

3.2.2.20 MODE: ASSURED SAFE CREW RETURN

This mode provides mitigation capability for life threatening illness, unrecoverable loss of station habitability, or extended problem requiring resupply/servicing which is prevented from occurring due to launch problems. This mode consists of the actions/operations/functions necessary to safely populate the Assured Crew Return Vehicle (ACRV), separate and return the ACRV to earth, and egress the ACRV upon recovery on the ground. The mode consists of the capabilities as shown in SSP 41000, Rev. B, Table VIII, and the following unique capability.

3.2.2.21 CONTROL OF WATER-SOLUBLE VOLATILE ORGANIC COMPOUNDS

Use of methanol, ethanol, isopropyl alcohol, n-propyl, n-butyl alcohol, acetone, ethylene, glycol, and propylene glycol in any quantity in a pressurized element shall follow the requirements specified in SSP 30233, Space Station Requirements for Materials and Processes, paragraph 3.1.5.

DCN 004

3.2.3 CAUTION AND WARNING

3.2.3.1 ANNUNCIATE ALARMS

The purpose of this function is to provide audible and visual alarms to the crew. The <END ITEM> shall annunciate Class 1, 2 and 3 audio and visual alarms in accordance with SSP 50005, Caution and Warning Displays. The <END ITEM> shall provide the facilities to allow on-orbit operators to acknowledge alarms. This requirement shall be located within each segment and may not apply to each end item (e.g. MPLM) if capability is provided through another end item or segment.

3.2.4 FAULT DETECTION ISOLATION AND RECOVERY

3.2.4.1 <RESERVED>

3.2.4.2 ISOLATE TO THE RECOVERY LEVEL

The USL shall automatically isolate detected failures to the functional recovery level for those functions requiring automatic isolation, identified in SSP 41000, Rev. B, Table II, column 3.

3.2.4.3 ISOLATE HAZARD

The <End Item> shall isolate hazards, that exhibit a time to catastrophic or critical effect of less than 24 hours, to the on-orbit safing level.

3.2.4.4 ASSESS FUNCTIONAL DATA

The <End Item> shall automatically assess the collected data to detect failures of those functions requiring automatic assessment and to detect hazards that may exhibit a time to catastrophic or critical effect of less than 24 hours.

3.2.4.5 MANUAL FDIR

The following categories of equipment shall utilize crew interaction or crew observation for manual failure detection, isolation, annunciation, and recovery:

A. Human/equipment interface such as visual display devices, cursor control devices, manual input devices.

B. General and specialized lighting.

C. Visual and aural caution and warning devices such as warning panel lamps/lights, speakers and volume controls.

D. Structural, mechanical, electro-mechanical, and electrical equipment that have no interconnection for data collection and transmission to the core computational data network such as fluid, power, and data lines, structure and manually operated equipment.

E. One-time use equipment that has manual redundancy (crew intervention upon failure of automatic function) and is not intended to be maintained on-orbit during the life of the program such as bolt motor controllers for assembly operations.

3.2.4.6 MANUAL CONTROL OF FDIR

The <End Item> shall provide for manual control of automatic detection, isolation, and recovery control processes.

3.2.4.7 COLLECT FUNCTION STATUS DATA

The purpose of this function is to collect applicable data for assessment of functional health, out of tolerance conditions, functional performance, functional failures, and other status data per SSP 50038.

3.2.4.8

The <END ITEM> shall obtain data identifying out-of-tolerance conditions, functional failures, and data describing functional operation. The <END ITEM> shall make available, to automatic capabilities and to operators on demand in accordance with the paragraph "S/W Functional Interfaces" of SSP 41143, SSP 42011, and SSP 41141, all generated Built In Test (BIT) data and results of process execution or effector manipulation per SSP 50038.

3.2.4.9 CONDITION FUNCTION STATUS DATA

The purpose of this function is to condition data into a usable form. This data is then available upon demand by other capabilities or operators.

The <END ITEM> shall condition functional data for identified users. The <END ITEM> shall make available, to automatic capabilities and to operators on demand in accordance with the paragraph "S/W Functional Interfaces" of SSP 41143, SSP 42011, and SSP 41141, all conditioned BIT data per SSP 50038, see paragraph 3.2.4.10.11.

3.2.5 LIGHTING

3.2.5.1 ILLUMINATE GENERAL AREA

The purpose of this function is to illuminate general areas of the USL.

The USL shall illuminate general activity areas at a minimum of 10 foot-candle (108 lux) of white light. The USL shall illuminate the passageways at a minimum of 5 foot candles (54 lux) of white light.

3.2.5.2 ILLUMINATE EMERGENCY EGRESS AREA

The purpose of this function is to illuminate the emergency egress areas of the <END ITEM>.

The <END ITEM> shall illuminate the emergency egress area at a minimum of 0.05 foot candle (0.5 lux) for pressurized module exits. The <END ITEM> shall illuminate the emergency controls at a minimum of 0.01 foot candle (0.108) lux for emergency controls.

3.2.5.3 CONTROL EMERGENCY EGRESS LIGHTING

The purpose of this function is to control the automatic turn on of the emergency egress lighting when an emergency is recognized.

3.2.6 NOISE

3.2.6.1 ACOUSTIC EMISSION LIMITS

The integrated acoustic environment in habitable areas in the ISS Modules/elements shall not exceed the US Noise Criteria (NC)-50 criterion during normal operating conditions when averaged over a minimum of 10-second time intervals. In areas where crewmembers must communicate by voice, the reveberation time shall not exceed 0.5 +/- 0.1 seconds at 1000 Hertz. DCN 002

3.2.6.2 NON-INTEGRATED HARDWARE ACOUSTIC EMISSION LIMITS

All non-integrated hardware to be flown in the ISS Modules shall not exceed NC-40 as measured at 0.6 meters from the noisest point on the hardware as in accordance with JSC 28322, ISS Acoustic Requirements and Testing Document for ISS Non-Integrated Equipment. All non-integrated equipment providers shall comply with JSC 28322 as the ISS Program Acoustic Requirement document. DCN 002

3.2.7 RADIATION

3.2.7.1 IONIZING RADIATION CREW LIMITS

The design of the USL shall limit the ionizing radiation dose in habital volumes to 40 rem (BFO) per year.

3.2.7.2 IONIZING RADIATION EMISSION LIMITS

Ionizing radiation emissions from USL equipment shall not exceed 2 millirads silicon per day, one centimeter from any surface.

3.2.7.3 SUPPORT RADIATION EXPOSURE MONITORING

The <End Item> shall monitor crew environment exposure to radiation.

3.2.7.4 <RESERVED>

3.2.7.5 METEOROIDS AND ORBITAL DEBRIS (M/OD)

The <End Item> M/OD critical items shall meet the requirements specified herein when exposed to the M/OD environments defined in SSP 30425, Meteoroids and Orbital Debris. Parameters of International Space Station M/OD environments definition are given in Table IX.

TABLE IX PARAMETERS FOR M/OD ENVIRONMENTS DEFINITION

Altitude	215 nautical miles (400 km)
Orbital inclination	51.6 degrees
Space Station attitude	LVLH 10% of the time (Orbiter attached) TEA 90% of the time (Orbiter not attached)
Solar flux	70 x 10^4 Jansky ($F_{10.7}$ = 70)
Orbital debris density(1)	2.8 gm/cm^3
Maximum debris diameter	20 cm

NOTE:
(1) For M/OD critical items only

3.2.7.6 PROBABILITY OF NO PENETRATION

The Space Station shall have a 0.81 (minimum) combined Probability of No Penetration (PNP) of M/OD critical items (See Appendix B) in the M/OD environment defined in 3.2.6.1.8 [of SSP 41000B], for 10 years from First Element Launch (FEL). [SSP 41000B, 3.3.12.1.1]

3.2.7.7

The <End Item> shall have provisions for M/OD protection augmentation.

3.2.7.8 ENVIRONMENTAL CONDITIONS

The <End Item> shall satisfy the requirements of this specification when subjected to the environmental conditions for the environments and environmental phases specified below.

3.2.7.9 ELECTROMAGNETIC RADIATION

3.2.7.10 EMC

The shall meet the requirements specified in SSP 30243.

3.2.7.11 EMI

Electrical and electronic equipment shall meet requirements in SSP 30237.

3.2 7.12 ELECTRICAL GROUNDING

Electrical Grounding shall be in accordance with SSP 30240.

3.2.7.13 ELECTRICAL BONDING

Electrical Bonding shall be in acordance with SSP 30245.

3.2.7.14 PLASMA

The <End Item> shall meet the performance and design requirements specified herein when exposed to the natural plasma environment as specified in SSP 30425, Section 5 and the induced environment as specified in SSP 30420, section 3.3. The difference

between the <End Item> structure floating potential and the local plasma potential does not exceed +/-40 volts.

3.2.7.15 IONIZING RADIATION

The <End Item> shall meet specified performance when exposed to the radiation dose environment as specified in SSP 30512. A radiation dose design margin of two shall be applied.

3.2.7.16 ELECTROSTATIC DISCHARGE (ESD)

The <End Item> shall meet the requirements as specified in SSP 30243.

3.2.7.17 CORONA

The <End Item> shall meet the requirements as specified in SSP 30243.

3.2.7.18 CABLE AND WIRE DESIGN

<End Item> interconnect and interconnect cable and wire design shall be in accordance with SSP 30242.

3.2.8 RESPOND TO FIRE

The USOS shall detect a fire event in locations in accordance with the selection criteria in Figure 24 and in the open cabin volume. The USOS shall isolate a fire event within 30 seconds of detection, including removal of power and forced airflow at the affected location, in locations in accordance with the selection criteria in Figure 24. The USOS shall accommodate Portable Breathing Apparatuses (PBAs) and provide Portable Fire Extinguisher (PFEs). The USOS shall activate a Class I alarm for a detected fire event with event location. The USOS shall visually indicate a fire event at the detection location. The USOS shall prevent forced air circulation between elements within 30 seconds of annunciation of a Class I fire alarm. Fixed fire suppression, where installed, shall complete application of fire suppressant within one minute of initiation. The USOS fire suppression shall reduce the oxygen concentration at the fire event location to less than 10.5 percent within one minute of suppressant discharge. The USOS shall have fixed fire suppression in locations in accordance with the selection criteria in Figure 24. Fixed fire suppression, where installed, shall have remote activation capability. When initiated by the crew or ground, the USOS shall vent the atmosphere of any pressurized volume to space to achieve an oxygen partial pressure less than 1.0 psia within 10 minutes. The USOS shall restore the habitable environment after a fire event. [SSP 41000B, P 3.7.1.3.8.1, CCM 00077]

APPENDIX A - ACRONYMS AND ABBREVIATIONS

AC	Alternating Current	
ATV	**<TBD A-1>**	
BFO	Blood Forming Organs	
CETA	Crew and Equipment Translation Aids	
CIL	Critical Items List	DCN 004
CO2	Carbon Dioxide	
CTB	**<TBD A-1>**	
dB	Decibel	
DC	Direct Current	
EMC	**<TBD A-1>**	
EMI	**<TBD A-1>**	
ESD	**<TBD A-1>**	
EVA	Extravehicular Activity	
FDIR	<TBD A-1>	
FMEA	Failure Modes and Standard Payload Racks	DCN 004
ICD	Interface Control Document	DCN 001
ISS	International Space Station	
IVA	Intravehicular Activity	
IMV	Intermodule Venitlation (System)	
IP&CL	**<TBD A-1>**	
ISPR	International Standard Payload Racks	DCN 004
JSC	Johnson Space Center	
MDP	Maximum Design Pressure	
MEQ	Milliequilivants	
M/OD	**<TBD A-1>**	
MPE	Maximum Permissible Exposure	
MT	Mobile Transporter	
N/A	Not Applicable	DCN 002
NC	Noise Criteria	DCN 002
NASA	National Aeronautics and Space Administration	DCN 004
NSI	NASA Standard Initiator	
NSTS	National Space Transportation System	
ORU	Orbital Replacement Unit	
OSE	Orbital Support Equipment	
PBA	Portable Breathing Apparatus	
PFE	Portable Fire Extinguisher	

PIP	Payload Integration Plan	
RF	**<TBD A-1>**	
RMS	Remote Manipulator Subsystem	
RTM	Real-Time Monitor	
RWS	**<TBD A-1>**	DCN 004
SMAC	Spacecraft Maximum Allowable Concentration	DCN 001
SRMS	Shuttle Remote Manipulator System	
STS	Space Transportation System	
US	United States	DCN 002
U.S.	United States	DCN 004
USOS	United States On-orbit Segment	DCN 004

APPENDIX J

ISS PRESSURIZED VOLUME HARDWARE

DCN 004

APPENDIX J – ISS PRESSURIZED VOLUME HARDWARE

TABLE OF CONTENTS

DCN 004

DCN 004

3.0 REQUIREMENTS

3.3.6 SAFETY

3.3.6.1 GENERAL

3.3.6.1.1 CATASTROPHIC HAZARDS

The <END ITEM> shall be designed such that no combination of two failures, or two operator errors (See Appendix B), or one of each can result in a disabling or fatal personnel injury, or loss of the Orbiter or ISS. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls (See Appendix B) at the Segment/System levels.

3.3.6.1.2 CRITICAL HAZARDS

The <END ITEM> shall be designed such that no single failure or single operator error can result in a nondisabling personnel injury, severe occupational illness; loss of a major ISS element on-orbit life sustaining function or emergency system, or involves damage to the Orbiter. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.3 DESIGN FOR MINIMUM RISK

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

3.3.6.1.4 CONTROL OF FUNCTIONS RESULTING IN CRITICAL HAZARDS

3.3.6.1.4.1 INADVERTENT OPERATION RESULTING IN CRITICAL HAZARDS

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

DCN 004

3.3.6.1.4.2 LOSS OF FUNCTION RESULTING IN CRITICAL HAZARDS

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

3.3.6.1.5 CONTROL OF FUNCTIONS IN CATASTROPHIC HAZARDS

3.3.6.1.5.1 INADVERTENT OPERATION RESULTING IN CATASTROPHIC HAZARDS

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

A. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See Appendix B), whenever the hazard potential exists.

B. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

C. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 LOSS OF FUNCTION RESULTING IN CATASTROPHIC HAZARDS

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

A. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

B. The function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function".

3.3.6.1.6 SUBSEQUENT INDUCED LOADS

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

DCN 004

3.3.6.1.7 SAFETY INTERLOCKS

Safety interlocks shall be provided to prevent unsafe operations when access to equipment is required for maintenance.

3.3.6.1.8 ENVIRONMENTAL COMPATIBILITY

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

3.3.6.2 HAZARD DETECTION AND SAFING

3.3.6.2.1 <RESERVED>

3.3.6.2.2 MONITORS

3.3.6.2.2.1 STATUS INFORMATION

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

3.3.6.2.2.2 HAZARDOUS FUNCTION OPERATION PREVENTION

Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function.

3.3.6.2.2.3 LOSS OF INPUT OR FAILURE

Loss of input or failure of the monitor shall be identifiable.

3.3.6.2.2.4 LAUNCH SITE AVAILABILITY

Monitoring shall be available to the launch site when necessary to assure safe ground operations.

3.3.6.2.2.5 FLIGHT CREW AVAILABILITY

Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

3.3.6.2.3 NEAR-REAL TIME MONITORING

Near-real time monitoring of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, “Respond to Loss of Function”. The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard.

3.3.6.2.4 REAL TIME MONITORING

3.3.6.2.4.1 MAINTAIN STATUS OF HAZARD CONTROLS

DCN 004

The <End Item> shall provide real-time monitoring (See Appendix B) to catastrophic hazardous functions to maintain status of hazard controls when the crew or the <End Item> is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 CREW RESPONSE TIME AND SAFING PROCEDURES

If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 GROUND MONITORING

If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within the time to effect of the hazard upon loss of communication with the ground.

3.3.6.3 COMMAND AND COMPUTER CONTROL OF HAZARDOUS FUNCTIONS

3.3.6.3.1 COMPUTER CONTROL OF HAZARDOUS FUNCTIONS

The computer control of hazardous functions shall comply with the safety implementation requirements as specified in SSP 50038.

3.3.6.4 HAZARDOUS MATERIALS

3.3.6.4.1 HAZARDOUS FLUID CONTAINMENT FAILURE TOLERANCE

Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate with the hazard level or be contained in an approved pressure vessel as defined in SSP 30558.

3.3.6.4.2 STORAGE OF HAZARDOUS CHEMICALS

Hazardous experiment payload chemicals/materials shall be stored only in International Standard Payload Racks (ISPRs) located in U.S. Laboratory or Logistics Modules.

3.3.6.5 PYROTECHNICS

3.3.6.5.1 PYROTECHNICS FOR USOS APPLICATION

3.3.6.5.1.1 NASA STANDARD INITIATORS

NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions.

3.3.6.5.1.2 FIRING CIRCUIT DESIGN

Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads.

3.3.6.5.1.3 PYROTECHNIC OPERATED DEVICES

Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.

3.3.6.6 NON-IONIZING RADIATION

A. The <End Item> shall limit the levels of non-ionizing radiation in accordance with SSP 50005, paragraph 5.7.3.2 or provide personnel protection.

B. Transmitters shall not irradiate the Orbiter at levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001). A two-fault tolerant combination of pointing controls or independent inhibits to transmission may be used to prevent hazardous irradiation of the Orbiter. The inhibits to prevent radiation do not require monitoring unless the predicted radiation levels exceed Orbiter limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

3.3.6.7 OPTICS AND LASERS

3.3.6.7.1 LASERS

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

3.3.6.7.2 OPTICAL REQUIREMENTS

3.3.6.7.2.1 OPTICAL INSTRUMENTS

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

DCN 004

3.3.6.7.2.2 PERSONNEL PROTECTION

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

3.3.6.7.2.3 DIRECT VIEWING OPTICAL SYSTEMS

Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems shall be limited to levels below the Maximum Permissible Exposure (MPE).

3.3.6.8 ELECTRICAL SAFETY

3.3.6.8.1 ELECTRICAL POWER CIRCUIT OVERLOADS

3.3.6.8.1.1 CIRCUIT OVERLOAD PROTECTION

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

3.3.6.8.1.2 PROTECTIVE DEVICE SIZING

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

3.3.6.8.1.3 BENT PIN OR CONDUCTIVE CONTAMINATION

A. <End Item> electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.

B. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 CREW PROTECTION FOR ELECTRICAL SHOCK

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

3.3.6.8.3 REAPPLICATION OF POWER

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

3.3.6.8.4 BATTERIES

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

3.3.6.9 <RESERVED>

3.3.6.10 FIRE PROTECTION

A. <Reserved>

B. <Reserved>

C. <Reserved>

D. Fire suppressant shall be compatible with Space Station life support hardware, not reach toxic concentrations, and be noncorrosive.

E. Fire suppressant by-products shall be compatible with the Space Station life support contamination control capability.

F. <Reserved>

G. <Reserved>

H. <Reserved>

I. <Reserved>

J. <Reserved>

K. <Reserved>

3.3.6.11 CONSTRAINTS

3.3.6.11.1 <RESERVED>

3.3.6.11.2 PRESSURIZED VOLUME DEPRESSURIZATION AND REPRESSURIZATION TOLERANCE

3.3.6.11.2.1 PRESSURE DIFFERENTIAL TOLERANCE

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

3.3.6.11.2.2 OPERATION DURING PRESSURE CHANGES

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

3.3.6.11.3 <RESERVED>

3.3.6.11.4 <RESERVED>

3.3.6.11.5 <RESERVED>

3.3.6.11.6 COMPONENT HAZARDOUS ENERGY PROVISION

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

3.3.6.11.7 <RESERVED>

3.3.6.11.8 <RESERVED>

3.3.6.11.9 <RESERVED>

3.3.6.11.10 <RESERVED>

3.3.6.11.11 CRYOGENICS

3.3.6.11.11.1 THERMAL CHARACTERISTICS

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

3.3.6.11.11.2 CRYOGENIC ENTRAPMENT

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

3.3.6.11.11.3 AIR COMPATIBILITY

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

3.3.6.11.12 HAZARDOUS GAS ACCUMULATION

3.3.6.11.12.1 ACCUMULATION PREVENTION

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

3.3.6.11.12.2 DETECTION, MONITORING, AND CONTROL

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

3.3.6.11.13 EQUIPMENT CLEARANCE FOR ENTRAPMENT HAZARD

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

3.3.6.11.14 FRANGIBLE MATERIALS

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

3.3.6.12 HUMAN ENGINEERING SAFETY

3.3.6.12.1 INTERNAL VOLUME TOUCH TEMPERATURE

3.3.6.12.1.1 CONTINUOUS CONTACT - HIGH TEMPERATURE

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

3.3.6.12.1.2 INCIDENTAL OR MOMENTARY CONTACT - HIGH TEMPERATURE

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

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

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

3.3.6.12.1.3 INTERNAL VOLUME LOW TOUCH TEMPERATURE

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

3.3.6.12.2 <RESERVED>

3.3.6.12.3 <RESERVED>

3.3.6.12.4 INTERNAL CORNER AND EDGE PROTECTION

DCN 004

3.3.6.12.4.1 EQUIPMENT EXPOSED TO CREW ACTIVITY

Surfaces of <END ITEM> equipment and ORUs located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraphs 6.3.3.1, Corner and edge requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3, Protective covers, and 6.3.3.11, Loose equipment.

3.3.6.12.4.2 EQUIPMENT EXPOSED ONLY DURING PLANNED MAINTENANCE ACTIVITIES

Corners and edges of material, equipment or ORUs which are exposed only during planned maintenance activities shall be rounded to a minimum radius or chamfer of 0.03 inches.

3.3.6.12.5 <RESERVED>

3.3.6.12.6 LATCHES

Latches or similar devices shall be designed to prevent entrapment of crewmember appendages.

3.3.6.12.7 SCREWS AND BOLTS

Screws or bolts, except internal ORU screws and bolts, in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 in. in length shall have protective features to prevent snagging, to protect against sharp edges, and impact, that do not prevent installation or removal of the fastener.

3.3.6.12.8 SAFETY CRITICAL FASTENERS

Safety critical fasteners shall be designed to prevent inadvertent back out.

3.3.6.12.9 LEVERS, CRANKS, HOOKS AND CONTROLS

Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing.

3.3.6.12.10 BURRS

Exposed surfaces shall be smooth and free of burrs.

DCN 004

3.3.6.12.11 HOLES

3.3.6.12.11.1 EQUIPMENT LOCATED INSIDE HABITABLE VOLUMES

Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside habitable volumes.

3.3.6.12.11.2 <RESERVED>

3.3.6.12.12 <RESERVED>

3.3.6.12.13 <RESERVED>

3.3.6.12.14 <RESERVED>

3.3.6.12.15 <RESERVED>

3.3.6.12.16 FLEXHOSES

Flexhoses and lines with delta pressure shall be restrained or otherwise captured to prevent injury to crew and/or damage to adjacent hardware.

3.3.6.12.17 <RESERVED>

3.3.6.12.18 <RESERVED>

DCN 004

4.0 VERIFICATION

4.3.3.6 SAFETY

No verification required. (Title only)

4.3.3.6.1 GENERAL

No verification required. (Text only)

4.3.3.6.1.1 CATASTROPHIC HAZARD

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analyses, operational procedures, integrated schematics and drawings, and integration documentation to identify catastrophic hazards, their causes, and controls. The analysis shall assess hardware failures, software errors, and human errors such that the ISS on-orbit system can tolerate a combination of two failures/software errors or two operator errors or one of each and still not result in the catastrophic event. The verification shall be considered successful when controls are in place to tolerate two failures or two operator actions or a combination of one failure and one operator action and still not result in the hazardous event.

4.3.3.6.1.2 CRITICAL HAZARDS

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analyses, operational procedures, integrated schematics and drawings, and integration documentation to identify critical hazards, their causes, and controls. The analysis shall assess hardware failures, software errors, and human errors such that the ISS on-orbit system can tolerate a hardware failure, software error, or operator action and still not result in the critical event. The verification shall be considered successful when controls are in place to tolerate a failure or an operator action and still not result in the hazardous event.

4.3.3.6.1.3 DESIGN FOR MINIMUM RISK

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall identify on-orbit hazards which are not controlled by failure tolerance, but are controlled through adherence to the design requirements specified in the segment and end item specifications. Items that will be evaluated for design for minimum risk include structures, pressure vessels, pressurized lines and fittings, pyrotechnic devices, mechanisms in critical applications, material compatibility, flammability, etc. Minimum supporting engineering data as specified in SSP 30599, paragraph B.2, shall be provided as part of the hazard closure process. The verification shall be considered successful when the engineering data as specified in SSP 30599, paragraph B.2, verifies that the USOS on-orbit design has met the criteria for design for minimum risk and the USOS on-orbit hazard reports show that the controls have been implemented.

4.3.3.6.1.4 CONTROL OF FUNCTIONS RESULTING IN CRITICAL HAZARDS

DCN 004

No verification required. (Text only)

4.3.3.6.1.4.1 INADVERTENT OPERATION RESULTING IN CRITICAL HAZARDS

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, and integration documentation to identify functions whose inadvertent operation would result in a critical hazard. The hazard analysis will identify two inhibits to preclude the event from inadvertently occurring. The analysis shall verify that the inhibits are independent. The verification shall be considered successful when the analysis verifies that the two inhibits are independent and are implemented in the design.

4.3.3.6.1.4.2 LOSS OF FUNCTION RESULTING IN A CRITICAL HAZARDS

Verification shall be done by using methodology documented in hazard reports. A hazard analysis shall be conducted to: identify the hazards; determine their severity; identify causes, and appropriate hazard controls to be implemented in the design; determine the compliance of those controls with safety requirements; and define the methods to be used to verify those hazard controls. The verification shall be considered successful when the hazard reports documenting the results of the hazard analysis are approved by the ISS Safety Review Panel.

4.3.3.6.1.5 CONTROL OF FUNCTION IN CATASTROPHIC HAZARDS

No verification required. (Text only)

4.3.3.6.1.5.1 INADVERTENT OPERATION RESULTING IN CATASTROPHIC HAZARDS

A. This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, and integration documentation to identify functions whose inadvertent operation would result in a catastrophic hazard. The hazard analysis will identify three inhibits to preclude the event from inadvertently occurring. The analysis shall verify that the inhibits are independent. The verification shall be considered successful when the analysis verifies that the three inhibits are independent and are implemented in the design.

B. This requirement shall be verified by analysis. The hazard analysis will identify where a credible failure (short) past the last inhibit would lead to activation of a hazardous event. In those cases, one of the inhibits shall be relocated to the ground side. The verification shall be considered successful when no credible failure or short can occur past the last inhibit on the high side and the load or that the design implements one of the three inhibits on the ground return.

C. This requirement shall be verified by analysis. The hazard analysis will assess the capability to monitor the status of two of the three inhibits. Monitoring the inhibits will not be required if the function power is deenergized (i.e., an additional fourth inhibit is in place between the power source and the three required inhibits) and the control circuits for the three required inhibits are disabled (i.e., no single failure in the control

circuitry will result in the removal of an inhibit) until the hazard potential no longer exists. The verification shall be considered successful when two of the three inhibits are monitored or a fourth inhibit is in place.

4.3.3.6.1.5.2 LOSS OF FUNCTION RESULTING IN CATASTROPHIC HAZARD

Verification shall be done by using methodology documented in hazard reports. A hazard analysis shall be conducted to: identify the hazards; determine their severity; identify causes, and appropriate hazard controls to be implemented in the design; determine the compliance of those controls with safety requirements; and define the methods to be used to verify those hazard controls. The verification shall be considered successful when the hazard reports documenting the results of the hazard analysis are approved by the ISS Safety Review Panel.

4.3.3.6.1.6 SUBSEQUENT INDUCED LOADS

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, integration documentation, and integrated FMEA/Critical Items Lists (CIL) to identify components that would be subject to induced loads when extended, deployed, or unstowed. The hazard analysis will include an assessment of the safing provisions for those items to determine if they can tolerate one or two failures and still be made to meet the structural factor of safety. The verification shall be considered successful when the identified components meet the structural factor of safety.

4.3.3.6.1.7 SAFETY INTERLOCKS

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics/drawings, integration documentation, and integrated FMEA/CILs to identify components that contain hazardous functions which are only exposed during maintenance. Such hazardous functions are rotating fans, belts, capacitors, microwaves, etc. When access to ORUs containing such hazardous functions is required for maintenance, an interlock shall be provided to de-energize the hazardous function. The hazard analysis shall identify the ORUs continuing the hazardous functions which require access for maintenance. The hazard analysis will identify if interlocks are required. The verification shall be considered successful when the interlocks are in place.

4.3.3.6.1.8 ENVIRONMENTAL COMPATIBILITY

This requirement shall be verified by analysis. A hazard analysis shall be conducted to identify hazards, their causes, and controls. The analysis will then assess the controls to determine if they are designed to the worst case natural and induced environments specified. The verification shall be considered successful when controls have been designed to the worst case environments.

4.3.3.6.2 HAZARD DETECTION AND SAFING

No verification required. (Text only)

4.3.3.6.2.1 <RESERVED>

4.3.3.6.2.2 MONITORS

No verification required. (Text only)

4.3.3.6.2.2.1 STATUS INFORMATION

Verification shall be done by analysis and test. A hazard analysis shall be conducted to: identify the hazards; determine their severity; identify causes, and appropriate hazard controls to be implemented in the design. An analysis or design review shall be conducted using drawings and specifications and the hazard analysis to determine which devices should be monitored to ensure safety. A further analysis or review will be conducted to determine where the monitors and circuits should be located to ensure that the status of the monitored device provides adequate information. Tests are required to show that the appropriate monitor devices provide the necessary data. The verification shall be considered successful when it is shown that the information provided is directly related to the status of the monitored device and that the monitor circuits are implemented such that they do not contain failure modes that would invalidate the hazard controls defined in the hazard reports.

4.3.3.6.2.2.2 HAZARDOUS FUNCTION OPERATION PREVENTION

Verification shall be done by using methodology documented in hazard reports. A hazard analysis shall be conducted to: identify the hazards; determine their severity; identify causes, and appropriate hazard controls to be implemented in the design; determine the compliance of those controls with safety requirements; and define the methods to be used to verify those hazard controls. The hazard analysis shall consider potential credible failures related to monitor circuits and devices. Specifications and drawings shall be evaluated to show where design features (such as current limiters) in the monitor circuits are provided to control or eliminate the hazards. The verification shall be considered successful when the hazard reports documenting the results of the hazard analysis are approved by the ISS Safety Review Panel.

DCN 004

4.3.3.6.2.2.3 LOSS OF INPUT OR FAILURE

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, integrations documentation, integrated FMEA/CILs, and FDIR assessments to verify that the loss of input to a monitor or the loss of the monitor is clearly identifiable. The verification shall be considered successful when the analysis proves that failure of the monitor or loss of input to the monitor can be distinguished from the status of the function being monitored.

4.3.3.6.2.2.4 LAUNCH SITE AVAILABILITY

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, integration documentation, integrated FMEA/CILs, and FDIR assessments to determine if any USOS cargo elements require monitoring during ground processing. The analysis shall verify that components which require ground monitoring have the capability to provide monitoring to the launch site. The verification shall be considered successful when the analysis verifies that monitoring is available to the launch site.

4.3.3.6.2.2.5 FLIGHT CREW AVAILABILITY

Analysis and/ or test will be conducted to assure that the safety monitoring and other failure data are annunciated to the RWS in real time or near real time. The verification shall be considered successful when the required safety monitor data will be available to the RWS in either real time or near real time.

4.3.3.6.2.3 NEAR-REAL-TIME MONITORING

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, and integration documentation to identify hazards with a time to effect greater than 24 hours. The analysis shall identify monitoring needs in order for the flight/ground crew to ascertain the status of ISS functions, safety devices, inhibits, and parameters with hazards with a time to effect greater than 24 hours. The verification shall be considered successful when monitoring is available to the ground/flight crew.

4.3.3.6.2.4 REAL-TIME MONITORING

No verification required. (Text only)

4.3.3.6.2.4.1 MAINTAIN STATUS OF HAZARD CONTROLS

This requirement shall be verified by an integrated failure safing analysis. The analysis shall evaluate identified hazardous conditions that, due to functional operation or out-of-tolerance conditions, may manifest a catastrophic or critical hazard within 24 hours. The analysis will use data from Hazard Analysis Reports, FMEA, IP&CL, schematics, and software detailed design documents. The analysis will also be supported by end item testing conducted to simulate functional operation or out-of-tolerance conditions that require automatic safing in less time than the time to catastrophic or critical effect. The

DCN 004

verification shall be considered successful when the analysis, supported by test data, shows that the USOS monitors safety critical functions, safety devices, inhibits, and safety parameters that may manifest a catastrophic or critical hazard.

4.3.3.6.2.4.2 CREW RESPONSE TIME AND SAFING PROCEDURES

Verification shall be accomplished by analysis and training. A hazard analysis shall be conducted to: identify the hazards; determine their severity; identify causes, and appropriate hazard controls to be implemented in the design; determine the compliance of those controls with safety requirements; and define the methods to be used to verify those hazard controls. For those cases identified in the hazard analysis as requiring the crew to provide an operational control to a hazard, analysis and training shall be accomplished to evaluate crew response time and safing procedures. The verification shall be considered successful when analysis and training demonstrate that there is margin for crew response time. Margin exists if it is shown that the time available to the crew in each of the available situations is greater than the crew's total reaction time and the time to convert the systems from a hazardous condition to a safe one.

4.3.3.6.2.4.3 GROUND MONITORING

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, integration documentation, integrated FMEA/CILs, and FDIR assessments to determine if ground monitoring is used to meet the real-time monitoring requirements. If ground monitoring is used, the analysis shall show that the flight crew can safe the hazardous function upon loss of communication with the ground before the hazardous event could occur. The verification shall be considered successful when the analysis proves the flight crew can safe the hazardous function upon loss of communication with the ground before the hazardous event could occur.

4.3.3.6.3 COMMAND AND COMPUTER CONTROL OF HAZARDOUS FUNCTIONS

No verification required. (Text only)

4.3.3.6.3.1 COMPUTER CONTROL OF HAZARDOUS FUNCTIONS

Verification of this requirement shall be by analysis. An analysis shall be performed to assure completeness of the verification results of the applicable requirements in SSP 50038, Computer−Based Control System Safety Requirements. Verification shall be considered successful when the verifications specified in SSP 50038, Computer−Based Control System Safety Requirements have been completed.

4.3.3.6.4 HAZARDOUS MATERIALS

No verification required. (Title only)

4.3.3.6.4.1 HAZARDOUS FLUID CONTAINMENT FAILURE TOLERANCE

This requirement shall be verified by analysis. The analysis shall be based on the end item level qualification data. The verification shall be considered successful when the analysis of end item level qualification data has shown that hazardous fluids are contained in an approved pressure vessel as defined in SSP 30558 or have failure tolerant containment.

4.3.3.6.4.2 STORAGE OF HAZARDOUS CHEMICALS

This requirement shall be verified by inspection. The inspection of top level drawings shall be performed to verify that hazardous chemicals are stored in the USL or storage capability is provided external to the habitable volumes. The verification shall be considered successful when the inspection shows that storage for hazardous chemicals is limited to the USL or storage capability is provided external to the habitable volumes.

4.3.3.6.5 PYROTECHNICS

No verification required. (Title only)

4.3.3.6.5.1 PYROTECHNICS FOR USOS APPLICATION

No verification required. (Title only)

4.3.3.6.5.1.1 NASA STANDARD INITIATORS

This requirement shall be verified by analysis. An analysis of end item qualification data shall be performed to verify that NSI are used for all safety critical pyrotechnic applications. The verification shall be considered successful when the analysis shows that only NSI are used.

4.3.3.6.5.1.2 FIRING CIRCUIT DESIGN

This requirement shall be verified by analysis of end item qualification data. The analysis of end item qualification data shall verify that unconnected (unpowered) launch elements use resistors with values less than 100 ohms or relay contacts to short the NSI leads. The verification shall be considered successful when the analysis shows that firing circuits are designed as specified.

DCN 004

4.3.3.6.5.1.3 PYROTECHNIC OPERATED DEVICES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that pyrotechnic operated devices are designed and tested as specified.

4.3.3.6.6 NON-IONIZING RADIATION

This requirement shall be verified by analysis performed using lower-level EMI qualification data to assess the effect of non-ionizing radiation on the ISS on-orbit crew. The analysis shall determine the effect of non-ionizing radiation to the on-orbit crew using the data obtained from component testing. The analysis shall show that the crew exposure to non-ionizing radiation has a margin over the equipment tolerances. The verification shall be considered successful when the analysis shows that the limits as specified are not exceeded or personnel protection against non-ionizing radiation is provided.

4.3.3.6.7 OPTICS AND LASERS

No verification required. (Title only)

4.3.3.6.7.1 LASERS

Verification of this requirement shall be obtained by analysis of the applicable qualification results. The verification shall be considered successful when the applicable test, demonstration, analysis, or inspection results show that the requirements of ANSI-Z-136.1 have been satisfied.

4.3.3.6.7.2 OPTICAL REQUIREMENTS

No verification required. (Title only)

4.3.3.6.7.2.1 OPTICAL INSTRUMENTS

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that optical instruments on end items have been designed to prevent harmful light intensities and wavelengths from being viewed by operating personnel.

4.3.3.6.7.2.2 PERSONNEL PROTECTION

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that optical instruments on end items contain quartz windows, apertures, or beam stops and enclosures for hazardous wavelengths and intensities unless suitable protective measures are in place to protect personnel from Ultraviolet or Infrared burns or X-ray radiation.

4.3.3.6.7.2.3 DIRECT VIEWING OPTICAL SYSTEMS

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that light intensities

DCN 004

and spectral wavelengths at the eyepiece of direct viewing optical systems have been designed to be limited to levels below the Maximum Permissible Exposure as specified.

4.3.3.6.8 ELECTRICAL SAFETY

No verification required. (Title only

4.3.3.6.8.1 ELECTRICAL POWER CIRCUIT OVERLOADS

No verification required. (Title only)

4.3.3.6.8.1.1 CIRCUIT OVERLOAD PROTECTION

This requirement shall be verified by analysis. A hazard analysis, as specified in SSP 30309, shall be performed using end item hazard analysis, operational procedures, integrated schematics and drawings, and integration documentation to identify safety critical electrical power circuits. The hazard analysis shall assess the USOS electrical power distribution circuitry for failures to distribution circuits, generation of toxic products in pressurized areas and damage to other safety critical circuits. The analysis shall verify that protective devices are in place to guard against circuit overloads. The verification shall be considered successful when the analysis shows that no damage could occur from circuit overloads.

4.3.3.6.8.1.2 PROTECTIVE DEVICE SIZING

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that circuit protective devices have been sized to preclude steady state currents in excess of the values allowed as specified.

4.3.3.6.8.1.3 BENT PIN OR CONDUCTIVE CONTAMINATION

The requirements in a. and b. shall be verified by analysis using end item hazard analysis, operational procedures, integrated schematics and drawings, ICDs, and integration documentation to identify safety critical connectors. The analysis shall identify pins that are used to control inhibits to hazardous functions. The analysis shall determine if an inhibit could be invalidated if the pin were bent or a conductive material contaminated the connector. The verification shall be considered successful when the analysis shows that no more than one inhibit can be invalidated due to a bent pen or conductive contamination.

4.3.3.6.8.2 CREW PROTECTION FOR ELECTRICAL SHOCK

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that the crew is protected from electrical hazards as specified.

4.3.3.6.8.3 REAPPLICATION OF POWER

This requirement shall be verified by analysis. An analysis shall be performed using data from drawings, integration and software architecture documentation, and operational procedures to identify the elements/components that require power to be removed for maintenance, the manual procedures for repowering, and the methods for ensuring that manual repowering does not require automatic avionics controls. The verification shall be considered successful when analysis shows that the onboard crew alone is able to power down and power up components requiring maintenance.

4.3.3.6.8.4 BATTERIES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that batteries are designed to control buildup or venting of flammable, corrosive, or toxic gases and reaction products; expulsion of electrolyte; and failure modes of over temperature, shorts, reverse current, cell reversal, leakage, cell grounds, and over pressure, in accordance with the safety guidelines for batteries as specified.

4.3.3.6.9 <RESERVED>

4.3.3.6.10 FIRE PROTECTION

A. <Reserved>

B. <Reserved>

C. <Reserved>

D. This requirement shall be verified by analysis. An analysis shall be performed usingsegment qualification data, material usage agreements, material compatibility assessments, and material toxicity assessments to determine if the release of the fire suppressant material is compatible with ISS on−orbit Space Station life support hardware and to determine if the fire suppressant material is noncorrosive. An analysis shall be done using threshold limit values of the fire suppressant material and ISS on orbit volumetric assessments to determine if the release of fire suppressant could reach a toxic concentration. The verification shall be considered successful when the analysis results show that the requirements have been met as specified.

E. This requirement shall be verified by analysis. An analysis shall be performed usingsegment qualification data, material usage agreements, material compatibility assessments, and material toxicity assessments to determine if the release of the fire suppressant byproducts are compatible with ISS on−orbit Space Station life support hardware and to determine if the fire suppresant byproducts are

DCN 004

noncorrosive. An analysis shall be done using threshold limit values of the fire suppressant byproducts and ISS on−orbit volumetric assessments to determine if the release of fire suppressant could reach a toxic concentration. The verification shall be considered successful when the analysis results show that the requirements have been met as specified.

F. <Reserved>

G. <Reserved>

H. <Reserved>

I. <Reserved>

J. <Reserved>

K. <Reserved>

4.3.3.6.11 CONSTRAINTS

No verification required. (Title only)

4.3.3.6.11.1 <RESERVED>

4.3.3.6.11.2 PRESSURIZED VOLUME DEPRESSURIZATION AND REPRESSURIZATION TOLERANCE

No verification required. (Title only)

4.3.3.6.11.2.1 PRESSURE DIFFERENTIAL TOLERANCE

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that equipment located in pressurized volumes is capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard.

4.3.3.6.11.2.2 OPERATION DURING PRESSURE CHANGES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that equipment expected to function during depressurization or repressurization is designed to operate without producing hazards.

4.3.3.6.11.3 <RESERVED>

4.3.3.6.11.4 <RESERVED>

4.3.3.6.11.5 <RESERVED>

4.3.3.6.11.6 COMPONENT HAZARDOUS ENERGY PROVISION

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that components which retain hazardous energy potential are either designed to prevent a crewmember

conducting maintenance from releasing the stored energy potential or are designed with provisions to allow safing of the potential energy, including provisions to confirm that the safing was successful.

4.3.3.6.11.7 <RESERVED>

4.3.3.6.11.8 <RESERVED>

4.3.3.6.11.9 <RESERVED>

4.3.3.6.11.10 <RESERVED>

4.3.3.6.11.11 CRYOGENICS

No verification required. (Title only)

4.3.3.6.11.11.1 THERMAL CHARACTERISTICS

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that thermal expansion and contraction will not imposing excessive loads on the system.

4.3.3.6.11.11.2 CRYOGENIC ENTRAPMENT

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that pressure conversions from liquid to gaseous state is adequately controlled and will not create a hazard.

4.3.3.6.11.11.3 AIR COMPATIBILITY

This requirement shall be verified by inspection and analysis of end item qualification data. The verification shall be considered successful when the inspection and analysis shows that the hazards associated with the liquefaction of air is controlled.

4.3.3.6.11.12 HAZARDOUS GAS ACCUMULATION

No verification required. (Title only)

4.3.3.6.11.12.1 ACCUMULATION PREVENTION

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that the USOS prevents uncontrolled hazardous accumulations of gases.

4.3.3.6.11.12.2 DETECTION, MONITORING, AND CONTROL

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that the USOS can detect, monitor, and control hazardous gases or vapors in critical areas and closed compartments.

4.3.3.6.11.13 EQUIPMENT CLEARANCE FOR ENTRAPMENT HAZARD

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that clearance is provided for equipment removal and replacement.

4.3.3.6.11.14 FRANGIBLE MATERIALS

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that equipment inside habitable volumes containing frangible materials have features to contain all fragments in the case of breakage.

4.3.3.6.12 HUMAN ENGINEERING SAFETY

No verification required. (Title only)

4.3.3.6.12.1 INTERNAL VOLUME TOUCH TEMPERATURE

No verification required. (Title only)

4.3.3.6.12.1.1 CONTINUOUS CONTACT - HIGH TEMPERATURE

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that (1) surfaces which are subject to continuous contact with crewmember bare skin do not exceed 113 degrees Fahrenheit and (2) surfaces exceeding 113 degrees Fahrenheit have guards or insulation to prevent crewmember contact.

DCN 004

4.3.3.6.12.1.2 INCIDENTAL OR MOMENTARY CONTACT - HIGH TEMPERATURE

The requirements in a. and b. shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that (1) surfaces which are subject to incidental or momentary contact with crewmember bare skin do not exceed 122 degrees Fahrenheit and (2) surfaces exceeding 122 degrees Fahrenheit have guards or insulation to prevent crewmember contact.

4.3.3.6.12.1.3 INTERNAL VOLUME LOW TOUCH TEMPERATURE

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that (1) surfaces which are subject to continuous or incidental contact with crewmember bare skin are not less than 39 degrees Fahrenheit and (2) surfaces below 39 degrees Fahrenheit have protective equipment available to the flight crew and the equipment has warning labels at the surface site.

4.3.3.6.12.2 <RESERVED>

4.3.3.6.12.3 <RESERVED>

4.3.3.6.12.4 INTERNAL CORNER AND EDGE PROTECTION

No verification required. (Title only)

4.3.3.6.12.4.1 EQUIPMENT EXPOSED TO CREW ACTIVITY

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that surfaces of equipment and ORUs located in pressurized volumes and exposed to crew activity are designed as specified with the exceptions specified.

4.3.3.6.12.4.2 EQUIPMENT EXPOSED ONLY DURING PLANNED MAINTENANCE ACTIVITIES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that corners and edges of material, equipment, or ORUs which are exposed only during planned maintenance activities are rounded to a minimum radius or chamfer of 0.03 inches, with the exceptions as specified.

4.3.3.6.12.5 <RESERVED>

4.3.3.6.12.6 LATCHES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that latches or similar devices are designed to prevent entrapment of crewmember appendages.

4.3.3.6.12.7 SCREWS AND BOLTS

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that screws or bolts

DCN 004

with exposed threads protruding greater than 0.12 inches in length have protective features that do not prevent installation or removal of the fastener.

4.3.3.6.12.8 SAFETY−CRITICAL FASTENERS

An analysis shall be performed using data from drawings, integration documentation, and operational procedures to verify that safety−critical fasteners will not back out under all environmental conditions. Verification shall be considered successful when safety−critical fasteners will not back out.

4.3.3.6.12.9 LEVERS, CRANKS, HOOKS, AND CONTROLS

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that levers, cranks, hooks, and controls are located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing.

4.3.3.6.12.10 BURRS

This requirement shall be verified by analysis or inspection of end item qualification data. This requirement may be verified by inspection only if the inspection of hardware drawing shows that all end item hardware is deburred. The verification shall be considered successful when the analysis shows that exposed surfaces are smooth and free of burrs.

4.3.3.6.12.11 HOLES

No verification required. (Title only)

4.3.3.6.12.11.1 EQUIPMENT LOCATED INSIDE HABITABLE VOLUMES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that round or slotted holes that are uncovered are less than 0.4 inches or greater than 1.0 inch in diameter.

4.3.3.6.12.11.2 <RESERVED>

4.3.3.6.12.12 <RESERVED>

4.3.3.6.12.13 <RESERVED>

4.3.3.6.12.14 <RESERVED>

4.3.3.6.12.15 <RESERVED>

4.3.3.6.12.16 FLEXHOSES

This requirement shall be verified by analysis of end item qualification data. The verification shall be considered successful when the analysis shows that flexhoses and lines with delta pressure are restrained or otherwise captured to prevent injury to crew and damage to adjacent hardware.

4.3.3.6.12.17 <RESERVED>

4.3.3.6.12.18 <RESERVED>