IAASS-SSI-1700™
ISSUE: 2018-07

COMMERCIAL HUMAN-RATED SYSTEM CERTIFICATION

International Association for the Advancement of Space Safety

TABLE OF CONTENTS

CHAPTER 1 - GENERAL

100 PURPOSE

This document establishes the safety requirements applied by the IAASS Space Safety Institute (SSI) for the safety certification of Commercial Human Rated Systems (CHS). This standard covers any human-rated system commercially developed and operated to perform suborbital, orbital, or interplanetary missions, including transport vehicles such as capsules or winged bodies, orbital stations, unmanned cargo transport vehicles intended to dock with crewed stations, bases, descent and ascent vehicles, and integrated systems (e.g., capsule on launcher). NOTE: The mandatory (i.e., shall) requirements in this standard are based on selected best practices from past and present governmental space programs.

101 SCOPE

These requirements are intended to protect the flight personnel (i.e., crew and flight participants), the vehicle and relevant launcher or carrier, and any other interfacing system from CHS-related hazards. This document contains technical and system safety program requirements applicable to the CHS development and flight operations. CHS ground operations, interfacing ground systems, and ground support equipment (GSE) safety certification is outside the scope of this standard.

The technical requirements in this standard are applicable to the CHS, which, depending on the phase of the mission, is either the crewed vehicle or the composite (i.e., vehicle integrated on launcher or carrier). They apply also to external interfaces (e.g., with control centers, launch pad, recovery system). The requirements apply to all phases of the mission, including docking to a crewed station. The applicability of these requirements and their apportionment to CHS system functions, elements, and external interfaces, will be determined by the safety analysis.

Unique safety requirements for launchers and carriers mandated by national regulations, and unique safety requirements for the phases when they operate separately from the vehicle are outside the scope of this standard. Furthermore, all requirements related to public safety are outside the scope of this standard, in particular during launch, air-carried/air-launch, and re-entry phases.

102 RESPONSIBILITY

102.1 CHS Developer/Operator

It is responsibility of the CHS Developer/Operator (CO) to assure the safety of the system and to implement the requirements of this document.

102.2 Launcher or Carrier Operator

It is the responsibility of the Launcher or Carrier Operator to interface with the national regulatory body(ies) to obtain the necessary licenses.

103 IMPLEMENTATION

This document identifies the safety policy and requirements which shall be implemented by the CHS Developer/Operator (CO) to obtain a certificate of compliance of the IAASS Space Safety Institute (SSI). The implementation of safety requirements by the CO will be assessed by the SSI Safety Review Panel (SRP) during the safety review process and must be consistent with hazard potential. The SSI SRP assessment of safety compliance will include a complete review of the hazard reports and may include audits of the CO safety program and safety inspections of flight hardware. The detailed interpretations of these safety requirements will be by the SSI Safety Review Panel and will be determined on a case-by-case basis consistent with the CHS actual architecture and hazard potential.

103.1 Implementation Procedure

Appendix C of this standard is meant to assist the CHS Developer/Operator in implementing the system safety technical requirements and to define further the safety analyses, data submittals, and safety assessments needed in support of the safety certification process.

103.2 Flight Rules

Flight rules will be prepared for each CHS flight that 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 do define actions for the execution of the flight consistent with flight personnel safety. For example, if a vehicle which is launched by an aircraft only monitors two of three inhibits to a catastrophic hazardous function such as inadvertent deployment (this is the minimum requirement specified in paragraph 201.2.2), a flight rule related to the loss of a monitored inhibit may be imposed which may require an early termination of the flight.

104 SAFETY RISK

104.1 Probabilistic Safety Criteria

Probabilistic safety analysis methods provide a useful basis for the comparison of design options with regards to safety. However, probabilistic safety analysis methods rely on assumptions and are subject to uncertainties. Calculated values of such safety metrics are, therefore, not in themselves sufficient to determine that a system is safe but can only be an element of the case to be made that a system provides an acceptable level of safety.

104.1.1 Acceptable Orbital/Exploration Mission Safety Risk

The probability of a catastrophic event for the flight personnel (i.e., loss of crew and participants) should not exceed (TBD) for each major mission phase (e.g., launch, on-orbit, re-entry).

104.1.2 Acceptable Sub-Orbital Flight

The probability of a catastrophic event for the flight personnel during the entire flight should not exceed (TBD).

104.2 Micrometeoroids and Orbital Debris (M/OD) Risk

104.2.1 Acceptable M/OD Risk

For the vehicle, the probability that the exposure to meteoroid and debris environment will not lead to penetration of or spall detachment (from M/OD critical items) should be higher than 0.9946 over the mission.

104.2.2 Space Debris Risk Mitigation

The CHS shall be designed and operated in compliance with the requirements of ISO 24113.

105 SAFETY AND QUALITY MANAGEMENT

105.1 Safety Management System

The CHS Developer/Operator should establish a Safety Management System in accordance with IAASS-SSI-1700-01.

105.2 Quality Management System

The CHS Developer/Operator shall establish a Quality Management System in accordance with AS9100.

CHAPTER 2 - TECHNICAL SAFETY REQUIREMENTS

200 GENERAL

The technical safety requirements in this standard are applicable to a commercial human-rated space system (CHS) as determined by the safety analysis performed by the commercial developer/operator (CO). When a requirement which is identified as applicable by the safety analysis cannot be met, a noncompliance report shall be submitted to the Space Safety Institute (SSI) in accordance with Appendix C for resolution.

200.1 Design to Tolerate Failures/Faults

Failure/fault tolerance (FT) is the basic technical safety requirement that shall be used to control most CHS hazards. The CHS must tolerate a minimum number of credible failures/faults and/or crew errors determined by the hazard level. This criterion applies when the loss of a function or the inadvertent occurrence of a function results in a hazardous event.

200.1a Critical Hazards

Critical hazards shall be controlled such that no single failure/fault or operator error can result in a critical event, defined as damage to CHS, a temporally disabling but not life-threatening injury, or temporarily occupational illness, or the use of unscheduled safing procedures that affect operations.

200.1b Catastrophic Hazards

Catastrophic hazards shall be controlled such that no combination of two failures/faults or operator errors can result in a catastrophic event, defined as loss of life, life threatening or permanently disabling injury, loss of CHS or other interfacing ground system, or damage/loss of interfacing orbital system.

200.2 Design for Minimum Risk

CHS hazards which are controlled by compliance with specific requirements of this document other than failure/fault tolerance are called "Design for Minimum Risk" (DFMR) areas of design. Examples are structures, pressure vessels, pressurized line and fittings, functional pyrotechnic devices, mechanisms in critical applications, material compatibility, flammability, etc. 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 CO. Minimum supporting data requirements for these areas of design are identified in Appendix C.

200.3 Equivalent Safety

“Equivalent safety” refers to conditions that do not meet specific requirements in the exact manner specified. However, the system design, procedure, or configuration satisfies the intent of the requirement by achieving a comparable or higher degree of safety. Criteria are based on: (a) use of alternative methods/controls; (b) utilization of procedures, protective devices, pre-flight verification activities, and crew experience base; (c) reduced time of exposure; (d) likelihood/probability of additional failures after loss of first control/inhibit; reduction of hazard category, and/or other factors such as minimum of single FT with a robust design.

200.4 Environmental Compatibility

A CHS shall be certified safe in the applicable worst case natural and induced environments.

200.5 Human Rating

The CHS shall be designed to be compatible with human limits and to accommodate human needs. The CHS shall be designed to effectively utilize human capabilities, to control hazards with sufficient certainty to be considered safe for human operations, and to provide, to the maximum extent practical, the capability to safely recover the flight personnel from hazardous situations.

200.6 Handling Qualities

The CHS shall have handling qualities rating of 1 or 2 on the Cooper-Harper Scale in Figure 1 for tasks that can result in loss of flight personnel or loss of vehicle.

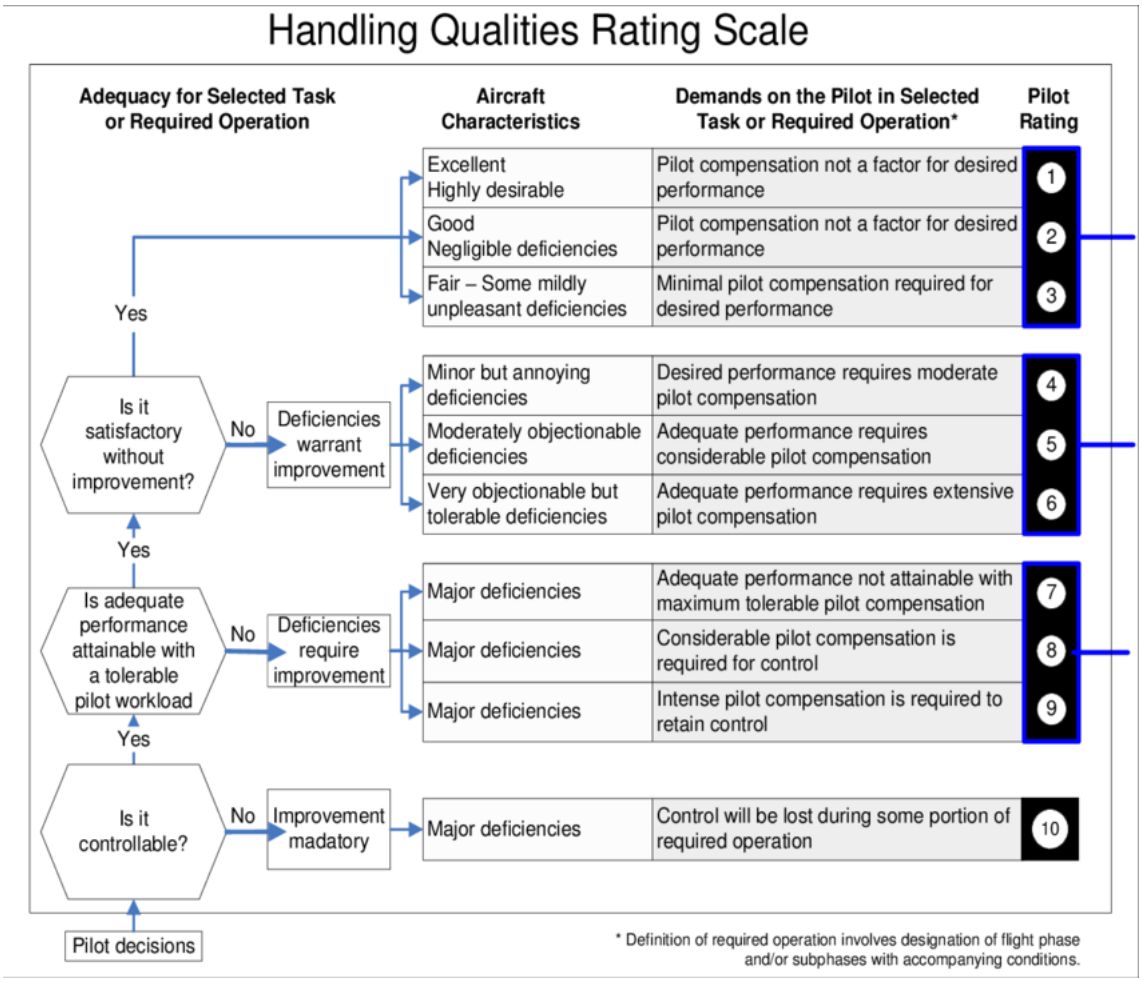

Figure 1

200.7 Flight Data Use Capability

To facilitate anomaly resolution and investigation of mishap/incident, the vehicle should be designed to provide the capability to record, recover and utilize health and status data of safety critical systems, also in case of loss of telemetry and communication with ground.

200.8 Launcher or Carrier Services

200.8.1 Safe Without Services

The vehicle should be designed to maintain failure/fault tolerance or safety margins consistent with the hazard potential without launcher or carrier flight services.

200.8.2 Critical Services

When launcher or carrier services are to be utilized to control vehicle hazards, the integrated system shall meet the failure/fault tolerance requirements of this standard and adequate redundancy of the launcher or carrier services must be negotiated with the launcher or carrier operator. The CO shall provide a summary of the hazards being controlled by launcher or carrier services in the safety data package, and document in the individual hazard reports those launcher or carrier interfaces used to control and/or monitor the hazards. CHS hazards which are controlled by launcher or carrier provided services shall require post-mate interface test verification for both controls and monitors. In addition, the CO shall identify in the CHS/Launcher (or Carrier) Interface Control Document (ICD) those launcher or carrier interfaces used to control and/or monitor the hazards.

201 CONTROL OF SAFETY-CRITICAL FUNCTIONS

201.1 Must-Work-Functions

201.1.1 Functions Resulting in Critical Hazards

A CHS function whose loss could result in a critical hazard shall be one FT, whenever the hazard potential exists. No single credible failure, fault, or operator error shall cause loss of that function.

201.1.2 Functions Resulting in Catastrophic Hazards

A CHS function whose loss operation could result in a catastrophic hazard shall be two FT, whenever the hazard potential exists. No two credible failures, faults, no two operator errors, or combination thereof shall cause loss of that function.

201.1.3 Crewed Manual Flight Control

The CHS shall provide the capability for the crew to manually control the flight path and attitude, with the following exception: during the atmospheric portion of Earth ascent when structural and thermal margins have been determined to negate the benefits of manual control.

201.1.4 Crewed Autonomous Operation

The CHS shall provide the capability for autonomous crew operation of system and subsystem functions which, if lost, would result in a catastrophic event without depending on communication with Earth (i.e., mission control) to perform functions that are required to keep the flight personnel alive.

201.1.5 Monitoring Capabilities

The CHS shall provide real-time monitoring capabilities for the crew and/or ground operator to monitor, operate and control the system and subsystems, where necessary to prevent a catastrophic event and prevent an abort.

201.1.6 Redundancy Separation

Redundant subsystems or alternate functional paths shall be separated by the maximum practical distance, or otherwise protected, to ensure that an unexpected event that damages one is not likely to prevent the others from performing the function. All redundant functions that are required to prevent a catastrophic hazard shall not be routed through a single connector.

201.2 Must-Not-Work Functions

201.2.1 Functions Resulting in Critical Hazards

A system function whose inadvertent operation could result in a critical hazard shall be controlled by two independent inhibits, whenever the hazard potential exists. Requirements for monitoring (paragraph 201.2.3) of these inhibits and for the capability to restore inhibits to a safe condition are normally not imposed but may be imposed on a case-by-case basis.

201.2.2 Functions Resulting in Catastrophic Hazards

A system function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits, whenever the hazard potential exists. One of these inhibits shall preclude operation by a radio frequency (RF) command or the RF link shall be encrypted. In addition, the ground return for the function circuit must be interrupted by one of the independent inhibits. At least two of the three required inhibits shall be monitored.

201.2.3 Monitors

Monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible. Monitor circuits shall be current limited or otherwise designed to prevent operation of the hazardous functions with credible failures. In addition, loss of input or failure of the monitor should cause a change in state of the indicator. Notification of changes in the status of safety monitoring shall be given to the flight crew in real-time. Monitoring shall be available to the launch site when necessary to assure safe ground operations.

201.2.3.1 Real-Time Monitoring

Real-Time Monitoring (RTM) shall be accomplished via the use of the failure detection and annunciation system. RTM of inhibits to a catastrophic hazardous function is required when changing the configuration of the applicable system or when the provisions of paragraph 202 are implemented for flight crew control of the hazard.

201.2.3.2 Unpowered Bus Exception

Monitoring and safing of inhibits for a catastrophic hazardous function will not be required if the function power is de-energized (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.

201.2.4 Use of Timers

When timers are used to control inhibits to hazardous functions, a reliable physical feedback system shall be in place for the initiation of the timer. If credible failure modes exist that could allow the timer to start prior to the relevant physical event a safing capability shall be provided to the flight crew.

201.2.5 Control of Inhibits

A device or function that operates an inhibit is referred to as a control for an inhibit. Controls do not satisfy the inhibit or failure tolerance requirements for hazardous functions. The "electrical inhibits" in a liquid propellant propulsion system (paragraph 201.4.4.1(c) electrical inhibits) are exceptions in that these devices operate the flow control devices (i.e., mechanical inhibits to propellant flow), but are referred to as inhibits and not as controls.

The inhibits to a must-not-work function may be controlled by a computer system used as a timer, provided the system meets all the requirements for independent inhibits.

201.2.6 Overriding Inhibits/Barriers

A power failure in the circuits of an inhibit (i.e., barrier or disabling device) shall not cause it to change state. An inhibit shall not be overridden. In the event of a cancellation of an inhibit function, the system where that function was implemented shall not have effect on the interfacing system.

201.2.7 Independent Inhibits

Inhibits opposing a given undesired event (i.e., hazardous circuit or system enabled or disabled unexpectedly either due to a failure or human error) shall be independent and, if possible, of different types. They may be mechanical, electrical, software, etc.

201.3 Fault Management

201.3.1 Failure Propagation

The design shall preclude propagation of failures from the CHS to the interfacing systems and vice-versa.

201.3.2 Detect, Isolate and Recover

The CHS shall provide the capability to detect, isolate and recover from faults identified during system development that would result in a catastrophic event.

201.4 Specific Catastrophic Hazardous Functions

In the following subparagraphs, specific requirements related to inhibits, monitoring, and operations are defined for several identified potentially catastrophic hazardous functions.

201.4.1 Explosives and Pyrotechnics

201.4.1.1 General

If premature firing or failure to fire will cause a hazard, the pyrotechnic subsystem and devices shall meet the design and test requirements of AIAA-S-113.

201.4.1.2 Initiators

NASA Standard Initiators are the preferred initiators for all safety critical explosive pyrotechnic functions. AIAA-S-113 qualification and acceptance test requirements, or equivalent, apply if other initiators are used.

201.4.2 Explosive/Pyrotechnic Operated Devices

201.4.2.2 Debris Protection

Pyrotechnic devices that are to be operated in proximity of the launcher, carrier or an interfacing system that do not meet the criteria of this document to prevent inadvertent operation, shall be designed to preclude hazards due to effects of shock, debris, and hot gasses resulting from operation. Such devices shall be subjected to a "locked-shut" safety demonstration test (i.e., a test to demonstrate the capability of the devices to safely withstand internal pressures generated in operation with the moveable part restrained in its initial position).

201.4.2.3 Must-Work Safety-Critical Devices

Where failure to operate will cause a catastrophic hazard, explosive/pyrotechnic operated devices shall be designed, controlled, inspected, and certified to criteria equivalent to those specified in NSTS 08060. If the device is used in a redundant application where the hazard is being controlled by the use of multiple independent methods, then in lieu of demonstrating compliance with criteria equivalent to NSTS 08060, sufficient margin to assure operation shall be demonstrated. When required, pyrotechnic operated devices shall demonstrate performance margin using a single charge or cartridge loaded with 85 percent (by weight) of the minimum allowable charge or other equivalent margin demonstrations. [Note: The data required for SSI SRP review are specified in Appendix C. The CO shall maintain a list of all safety-critical pyrotechnic initiators installed or to be installed on the CHS, giving the function to be performed, the part number, the lot number, and the serial number].

For pyrotechnic circuits involving a potentially catastrophic hazard, the inhibit close to the source of hazard shall mandatory be a mechanical inhibit capable of preventing the unintentional ignition of the system.

201.4.2.4 Electrical Connection

Pyrotechnic devices which if prematurely fired may cause a hazard shall be designed such that these devices can be electrically connected to the launcher or carrier after all electrical interface verification tests have been completed. Ordnance circuitry shall be verified safe prior to connection of pyrotechnic devices.

201.4.2.5 Shielding and Grounding

The components of a pyrotechnic chain, initiator, safe and arm device, transmission and distribution components, functional devices (i.e., destruction bars, cutting charges, separation thruster, valves, pistons, etc.) shall be designed so that external conductive parts (i.e., metallic or non-metallic) and shielding can be equipotential and grounded to the CHS.

201.4.3 Safe and Arm Device

201.4.3.1 Safe and Arm (S&A) Device Design

S&A devices shall be designed and tested in accordance with provisions of AIAA-S-113, and meet the following requirements:

a) The inhibit, once set to one of the states "armed" or "safe", may not leave that state in the absence of a command or under the effect of external interference (e.g., impacts, vibrations, electrostatic phenomenon, etc.);
b) The setting status report is representative of the real state, "armed" or "safe", and may be remote;

c) The "armed" or "safe" state is displayed by an indicator physically linked to the disabling device;
d) They may be remotely controlled, but manual disarming is always possible;
e) The assembly of the initiator is physically impossible if the device is not in "safe" position.

In determining compliance with paragraph 201.2.3.2, a S&A device in the "safe" position shall be counted as one of the required inhibits.

201.4.3.2 Use of Safe and Arm (S&A) Device

All solid propellant rocket motors shall be equipped with a S&A device that provides a mechanical interrupt in the pyrotechnic train immediately downstream of the initiator.

201.4.3.3 S&A Safe Position

The S&A shall be in the safe position during the launch or carry phase. There shall be a capability to re-safe the S&A device:

a) if the S&A device is to be rotated to the arm position while the vehicle is attached to the Launcher or Carrier; or
b) if the solid rocket motor propulsion subsystem does not qualify for the unpowered bus exception of paragraph 201.2.3.2.

201.4.3.4 Arming Prior to Safe Distance

If the S&A device is to be rotated to the arm position prior to the vehicle achieving a safe distance from the launcher or carrier, rotation shall be a flight crew function and shall be done as part of the final deployment activities of the vehicle.

201.4.4 Propulsion Systems

201.4.4.1 Premature/Inadvertent Firing

The premature/inadvertent firing of a propellant propulsion in any flight phase, including proximity to or attached to the launcher or carrier is a catastrophic hazard.

a) Each propellant delivery system shall contain a minimum of three mechanically independent flow control devices in series to prevent engine firing.
b) A bipropellant system shall contain a minimum of three mechanically independent flow control devices in series both in the oxidizer and fuel sides of the delivery system.
c) These devices shall prevent contact between the fuel and oxidizer as well as prevent expulsion through the thrust chamber(s). Except during ground servicing and as defined in paragraph 201.4.4.1(b)(1), these devices will remain closed during all ground and flight phases until the time of firing is foreseen.
d) A minimum of one of the three devices will be fail-safe (i.e., return to the closed condition in the absence of an opening signal).

201.4.4.1(a) Safe Distance Criteria

The hazard of engine firing close enough to inflict damage to the launcher, carrier or interfacing space system due to heat flux, contamination, and/or perturbation of the launcher, carrier, or interfacing space system, is in proportion to the total thrust imparted by the vehicle in any axis and shall be controlled by establishing a safe distance for the event. The safe distance shall be determined using Figure 2. For large thruster systems with greater than 10 pounds total thrust, the collision hazard with the launcher, carrier or interfacing space system shall be controlled by considering the safe distance criteria in Figure 2, together with the correct attitude at time of firing. For small reaction control system (RCS) thrusters with less than 10 pounds total thrust, the collision hazard shall be controlled by the safe distance criteria in Figure 2 with consideration of many variables such as deployment method, appendage orientation, and control authority.

201.4.4.1(b) Isolation Valve

One of the flow control devices shall isolate the propellant tank(s) from the remainder of the distribution system.

201.4.4.1(b)(1) Opening the Isolation Valve

If a vehicle 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 shall be opened after the vehicle has reached a safe distance for firing the reaction control thrusters provided the applicable requirements of paragraphs 201.4.4.1(c) and 201.4.4.1(d) have been met and shall provide two mechanical flow control devices remain to prevent thrusting of the larger system or equivalent failure tolerance measures.

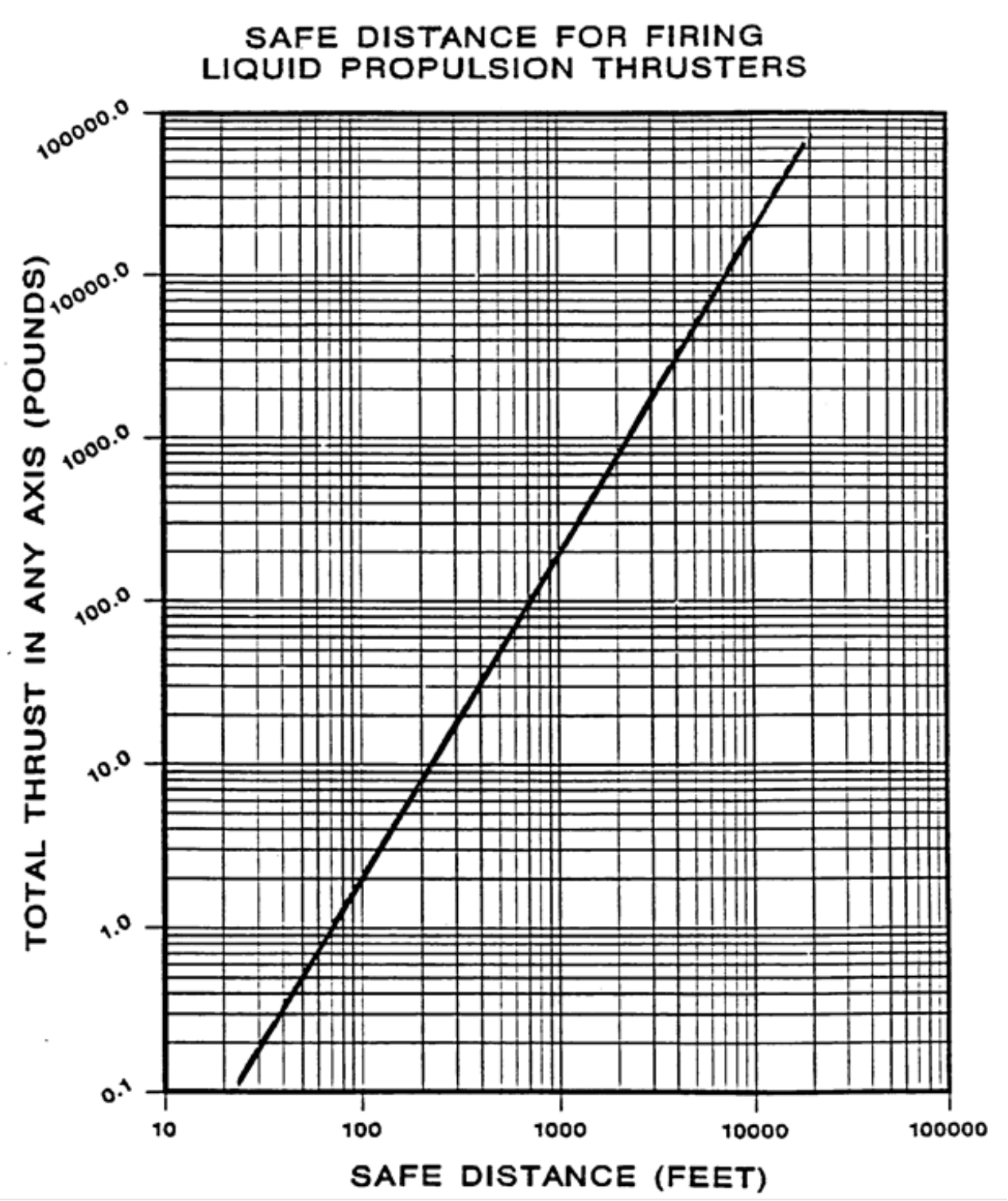

Figure 2

201.4.4.1(b)(2) Pyrotechnic/Explosive Isolation Valves

If a normally closed, pyrotechnically initiated, parent metal valve is used, fluid flow or leakage past the barrier will be considered mechanically non-credible if:

a) The valve has an internal flow barrier fabricated from a continuous unit of non-welded parent metal.
b) The valve integrity is established by rigorous qualification and acceptance testing.

When a valve is used as a flow control device, the number of inhibits to valve activation shall determine the failure tolerance against fluid flow.

201.4.4.1(c) Electrical Inhibits

If the vehicle is closer to the launcher, carrier or interfacing system than the minimum safe distance for engine firing, there shall be at least three independent electrical inhibits that control the opening of the flow control devices. The electrical inhibits shall 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 paragraph 201.4.4.1(b), prior to the vehicle achieving a safe distance for firing a large thruster, three independent electrical inhibits shall control the opening of the remaining flow control devices for the large thruster system.

201.4.4.1(d) Monitoring

At least two of the three required independent electrical inhibits shall be monitored by the flight crew until final separation of the vehicle from the interfacing system. The position of a mechanical flow control device shall be monitored in lieu of its electrical inhibit, provided the two monitors used to meet the above requirement are independent.

Real-time monitoring will be required as defined in 201.2.3.1. One of the monitors shall be the electrical inhibit or mechanical position of the isolation valve. Monitoring will not be required if the vehicle qualifies for the unpowered bus exception of paragraph 201.2.3.2.

If the isolation valve will be opened prior to the vehicle achieving a safe distance from the interfacing system, all three of the electrical inhibits that will remain after the opening of the isolation valve during final preparatory activities by the flight crew.

201.4.4.2 Adiabatic/Rapid Compression Detonation

If the vehicle is attached to the launcher, carrier or interfacing space system, the inadvertent opening of isolation valves in a hydrazine (N_2H_4) propellant system shall be controlled as a catastrophic hazard unless the outlet lines are completely filled with hydrazine or the system is shown to be insensitive to adiabatic or rapid compression detonation. Hydrazine systems will be considered sensitive to compression detonation 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.

Test plans shall be submitted to the SSI SRP as part of the appropriate hazard report. If the design solution is to fly wet downstream of the isolation valve, the hazard analysis shall consider other issues such as hydrazine freezing or overheating, leakage, single barrier failures, and back pressure relief.

201.4.4.3 Propellant Overheating

Raising the temperature of a propellant above the fluid compatibility limit for the materials of the system is a catastrophic hazard. Components in propellant systems that are capable of heating the system (e.g., heaters, valve coils, etc.) shall be two-FT to avoid heating the propellant above the material/fluid compatibility limits of the system. These limits shall be based on test data derived from qualified test methods (i.e., NASA-STD-6001B) or on data furnished by the manufacturer and approved by the SSI SRP.

Propellant temperatures less than the material/fluid compatibility limit, but greater than 110 °C (200 °F) must be approved by the SSI SRP. The use of inhibits, cutoff devices, and/or crew safing actions may be used to make the system two-FT to overheating. Monitoring of inhibits (paragraphs 201.2.3 and 201.1.2) or of propellant temperature will be required.

201.4.4.4 Propellant Leakage

The system shall be two-FT to prevent leakage of propellant 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 such a leak will be one FT.

The vehicle shall provide data related to pressure, temperature, and quantity gauging of the propulsion system tanks, components, and lines to the flight crew to ensure system health and safety.

201.4.4.5 Hazardous Impingement and Venting

The vehicle attitude control shall be designed to prevent hazardous thrusters' impingement on the launcher, carrier or interfacing space system. The propulsion system vents (i.e., relief valves, turbo pump assemblies, etc.) shall perform the venting function without causing an additional hazard to another interfacing space system.

201.4.4.6 Cryogenics

Cryogenic systems shall:

a) allow for component thermal expansion and contraction without imposing excessive loads on the system;
b) incorporate an automatic relief anywhere a cryogenic can be trapped between any valves in the system to preclude excess pressure causing rupture from conversion from liquid to gaseous state;
c) be insulated with an oxygen compatible material or be vacuum-jacketed to preclude liquefaction of air.

201.4.5 Inadvertent Deployment, Separation, and Jettison Functions

Inadvertent deployment, separation or jettison of a vehicle element or appendage is a catastrophic hazard unless it is proven otherwise. The general inhibit and monitoring requirements of paragraph 201 shall apply.

201.4.6 Planned Deployment/Extension Functions

201.4.6.1 Cannot Withstand Subsequent Loads

If during planned operations an element of the vehicle is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be design provisions to safe the vehicle with appropriate redundancy to the hazard level. Safing may include deployment, jettison or provisions to change the configuration of the system to eliminate the hazard.

201.4.7 RF Transmitters

Allowable levels of transmitters radiation from/to the vehicle shall be defined in the vehicle-launcher or -carrier, and other interfacing space systems (e.g., space station) ICDs. A two FT combination of pointing controls or independent inhibits to transmission may be used to prevent hazardous irradiation. The inhibits to prevent radiation do not require monitoring unless the predicted radiation levels exceed the limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

201.4.8 Fluid Release from a Pressurized System Inside of a Closed Volume

Release of any fluid from pressurized systems shall not compromise the structural integrity of any closed volume in which the hardware is contained, such as internal volumes.

Pressurized systems that are two FT to release of fluid through controlled release devices do not require analysis. Systems which do not meet the above shall be reviewed and assessed by SSI SRP for safety on a case-by-case basis.

201.4.9 On-Orbit Rendezvous and Docking

201.4.9.1 Control During Proximity Operations

The CHS shall provide the capability for the crew to monitor, operate, and control an uncrewed spacecraft during proximity operations, where: (a) the capability is necessary to execute the mission; or (b) the capability would prevent a catastrophic event; or (c) the capability would prevent an abort.

201.4.9.2 Direct Voice Communication

The CHS shall provide the capability for direct voice communication (i.e., signal not routed through mission control on Earth or another communication relay satellite) with other crewed spacecraft (two or more) during proximity operations.

201.4.9.3 Safe Trajectories

The trajectory of the (active) vehicle during rendezvous and proximity operations with an orbital (passive) system shall be such that the natural drift including 3 sigma dispersed trajectories ensures that:

a) prior to the Approach Initiation (AI) burn, the vehicle shall stay outside the Approach Ellipsoid (AE) for a minimum of 24 hours;
b) after the AI burn and prior to the vehicle stopping at the arrival point on V-bar inside the AE, the vehicle shall stay outside the keep-out sphere (KOS) for a minimum of 4 orbits;
c) during any retreat out of the Approach Ellipsoid, the vehicle shall maintain a positive relative range rate until it is outside the Approach Ellipsoid and thereafter it shall stay outside the Approach Ellipsoid for a minimum of 24 hours.

201.4.9.4 Use of Dedicated Rendezvous Sensors

Relative navigation during rendezvous shall be based on the use of rendezvous sensors for docking operations on the active vehicle (where relative GPS data may be corrupted by multi-path effects and/or will not provide sufficient accuracy) and corresponding target pattern on the passive orbital system.

201.4.9.5 Collision Avoidance Maneuver

The active vehicle shall implement collision avoidance maneuver strategies in addition to safe free drift trajectories, as a mean to avoid collision with a passive space system in case of contingencies up to docking.

201.4.10 Hazardous Commands

201.4.10.1 General

All hazardous commands shall be identified from the system safety analysis. Hazardous commands are those that can:

a) remove an inhibit to a hazardous function or
b) activate an unpowered hazardous system or
b) deactivate an operational function resulting in a catastrophic hazard.

Failure modes associated with the CHS system including hardware, software, and procedures used in commanding shall be considered in the safety analysis to determine compliance with the requirements of paragraphs 200.1, 201, and 201.4.

201.4.10.2 Command Fault Tolerance Approach

The computer system (CS) shall be designed such that no combination of two failures/faults, or two operator actions, or one of each will cause a catastrophic hazardous event. The computer system (CS) shall be designed such that no single failure/fault or operator action will cause a critical hazardous event.

201.4.10.2a Catastrophic Loss of Capability Hazard

Where loss of a capability could result in a catastrophic hazard, the computer system shall provide three independent and unique command messages to deactivate any function within a failure tolerant capability.

201.4.10.2b Critical Loss of Capability Hazard

Where loss of a capability could result in a critical hazard, the computer system shall provide two independent and unique command messages to deactivate the capability.

201.4.10.3 Pre-Requisite Checks

Pre-requisite checks for the safe execution of hazardous commands shall be performed by computer systems compliant with requirements of paragraph 205.

201.4.10.4 Rejection of Commands

The computer system (CS) shall reject hazardous commands which do not meet pre-requisite checks for execution.

201.4.10.4a Out of Sequence Commands

Where execution of commands out of sequence can cause a hazard, the computer system (CS) shall reject commands received out of sequence.

201.4.10.5 Integrity Checks

Integrity checks shall be performed when data or commands are exchanged across transmission or reception lines and devices.

201.4.10.6 Independent Commanding Method

Where software provides the sole control for safety-critical must-work functions, another non-identical method for commanding the function shall be provided.

201.4.10.7 Shutdown Independent Operator Action

At least one independent operator action shall be required for each operator-initiated command message used in the shutdown of a capability or function that could lead to a hazard.

201.4.10.8 Removal of Software Controlled Inhibits

Command messages to change the state of inhibits shall be unique for each inhibit.

201.4.10.9 Unique Command for Inhibit Removal

A unique command message shall be required to enable the removal of inhibits.

201.4.10.10 Hard-Coded Automated Failure Recovery

A separate and functionally independent parameter (with at least one operator controllable) shall be checked before issuance or execution of every hazardous command, which can be initiated by a hard-coded failure recovery automated sequence.

201.4.10.11 Overrides

Overrides shall require at least two independent actions by the operator.

202 HAZARD DETECTION, ANNUNCIATION AND SAFING

The need for hazard detection, annunciation 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. When implemented, these functions shall be capable of being tested for proper operations during both ground and flight phases. Likewise, CHS designs should be such that real-time monitoring is not required to maintain control of hazardous functions. With SSI SRP approval, real-time monitoring and hazard detection and safing may be utilized to support control of hazardous functions provided that adequate crew response time is available and acceptable safing procedures are developed.

202.1 Critical Systems, Subsystems and Crew Health

The CHS system shall provide the capability to detect and annunciate failures/faults that affect critical systems, subsystems and flight personnel health.

202.2 Emergency Caution and Warning

The CHS system shall incorporate an emergency, caution and warning system. All safety emergencies, caution and warning parameters shall be redundantly monitored and shall cause annunciation. As a minimum, vehicle total pressure, fan differential pressure, fire detection, oxygen partial pressure and carbon dioxide partial pressure shall be monitored. The status of all monitored parameters shall be available to the crew prior to in-flight entry into a habitable module. The caution and warning system shall include test provisions to allow the crew members to verify proper operation of the system.

202.3 Emergency Response

The CHS system shall provide the capability for the crew to readily access equipment involved in the response to emergency situations and the capability to gain access to equipment needed for follow-up/recovery operations.

202.4 Rapid Safing

Safe aborts and contingency return shall include design provisions for rapid safing. Hazard controls may include deployment, jettison or design provisions to change the configuration of the CHS.

203 ABORT, ESCAPE, AND SAFE HAVEN CAPABILITIES

203.1 Design for Safe Abort

The CHS design and operations shall allow for safe abort, including as necessary flight personnel escape and rescue capabilities, for all flight phases starting with on pad spaceport operations. The escape system, including any sensor, equipment and circuitry shall comply with the requirements 200.1 and 200.2.

203.2 Abort Capability

The CHS system shall provide abort capability from the launch pad until Earth-orbit insertion to protect for the following ascent failure scenarios (minimum list):

a) Complete loss of ascent thrust/propulsion;
b) Loss of attitude or flight path control.

203.3 Automatic Abort Initiation

The vehicle shall monitor the launcher or carrier performance during ascent and automatically initiate separation and abort when an impending catastrophic failure is detected.

203.4 Neutralization and Escape

To ensure public safety a destruct system is often part of a launcher design. The destruct system could be triggered from ground or by an on-board automated system. The automatic on-board system could trigger the destruct system when a non-nominal stage separation or a stage rupture occurs. The destruct system could also be triggered by an on-board automated device in the event of drift from the specified flight conditions.

203.4.1 Launcher Neutralization and Abort System Sequence

If a safety destruct command is issued, the CHS shall automatically initiate the abort sequence with sufficient delay to allow crewed vehicle separation and mission abort. The time delay shall be determined such to allow safe flight abort.

203.4.2 Launcher Stage Neutralisation

If an on-board automatic system is used to trigger the neutralisation of a launcher stage after nominal separation and before impact on ground to ensure the dispersal of remaining propellant, the time delay shall be determined to avoid any risk for the upper stages and for the crewed vehicle.

203.4.3 Inhibition of On-Board Receiver

The on-board receiver equipment for the safety destruct system commanding from ground shall be inhibited when in the course of the flight the commanding from ground is no longer required.

203.5 Safe-Haven

Safe-haven capabilities shall be included in the CHS system design to cope with uncontrollable emergency conditions (e.g., fire, depressurisation). The safe-haven is meant to sustain flight personnel life until escape or rescue can be accomplished.

203.6 Flight Personnel Egress

The CHS system design shall be compatible with emergency safing and rapid egress. The flight personnel shall be provided with clearly defined escape routes for emergency egress in the event of a hazardous condition. Where practical, dual escape routes from all activity areas shall be provided. Equipment location shall provide for protection of compartment entry/exit paths in the event of an accident. Routing of hard lines, cables, or hoses through a tunnel or hatch which could hinder flight personnel escape or interfere with hatch operation for emergency egress is not permitted. Hatches which could impede flight personnel escape shall remain open during all crewed operations.

203.7 Unassisted Emergency Egress

The CHS system shall provide the capability for unassisted flight personnel emergency egress during Earth pre-launch activities, and after Earth landing.

203.8 Earth Orbit Systems Abort

The crewed space system shall provide the capability to autonomously abort the mission from Earth orbit by targeting and performing a deorbit to a safe landing on Earth.

203.9 Earth - Lunar Transit and Lunar Orbit Systems

The crewed space system shall provide the capability to autonomously abort the mission during lunar transit and from lunar orbit by executing a safe return to Earth.

203.10 Lunar Descent Systems

The crewed space system shall provide the capability to autonomously abort the lunar descent and execute all operations required for a safe return to Earth.

203.11 Crew Overriding Automation/Control

The CHS shall provide the capability for the flight crew to manually override higher level software control/automation (such as automated abort initiation, configuration change, and mode change) when the transition to manual control of the system will not cause a catastrophic event.

204 CONTINGENCIES AND SURVIVAL CAPABILITIES

204.1 Survival Capabilities

Contingencies scenarios shall be considered to address relevant flight personnel survival capabilities. These should include system failures and emergencies not limited to fire, collision, toxic atmosphere, decreasing atmospheric pressure and medical emergencies among others.

204.2 Dissimilar Redundant System Capabilities

Contingencies scenarios shall be considered to provide possible dissimilar redundant system capabilities.

204.3 Fire Detection and Suppression

The vehicle design shall include capability and equipment for fire detection and suppression for each potential fire event location. Fire suppressant shall be compatible with vehicle life support hardware, not reach toxic concentrations, and be noncorrosive. Fire suppressant by-products shall be compatible with the vehicle life support contamination control capability.

204.4 Crashworthiness Capabilities

The vehicle design should protect occupants from injury in the event of a crash landing. Crash injury arises from three distinct sources:

a) excessive acceleration forces;
b) direct trauma from contact with injurious surfaces, and;
c) exposure to environmental factors such as fire, smoke, water, and chemicals resulting in burns, drowning or asphyxiation.

Effective crashworthiness design must consider all possible sources of injury and eliminate or mitigate as many as practical. This involves considerations of:

1) prevention of structure intrusion into occupied spaces, following collapse;
2) adequacy of seats and restraint systems;
3) adequacy of energy attenuation features;
4) elimination of injurious objects in the habitable environment, and;
5) post-crash scenarios risk assessment and mitigation.

205 COMPUTER SYSTEMS: FAILURE TOLERANCE APPROACH

205.1 Computer System Software Development

The computer system (CS) software development, verification and validation shall be performed in compliance with NASA-STD-8719.13B.

205.2 General

While a computer system (CS) is being used to actively process data to operate a system with catastrophic potential, the catastrophic hazard shall be prevented in a two-failure tolerant manner. One of the methods to control the hazard shall be independent of the computer system. A computer system shall be considered zero fault tolerant in controlling a hazardous system (i.e., a single failure will cause loss of control), unless the computer system complies with the requirements here below and the fault tolerance approach is approved by the SSI SRP.

205.2.1 Safe State

The computer system (CS) shall safely arrive to a known safe state when:

a) initializing a function,
b) performing an orderly shutdown of a function upon receipt of a termination command or detection of a termination condition
c) recovering upon anomaly detection.

205.2.2 Critical Software Behaviour

The CHS shall provide the capability to mitigate the hazardous behaviour of critical software where the hazardous behaviour would result in a catastrophic event.

205.2.3 Off-Nominal Power Condition

The CS shall continue to operate safely during off-nominal power conditions or contain design features which safe the processor during off-nominal power conditions.

205.2.4 Inadvertent Memory Modification

The CS shall detect and recover from inadvertent memory modification during use.

205.2.5 Discriminating Valid Versus Invalid Inputs

The CS shall be capable of discriminating between valid and invalid inputs from sources external to the CS and remain or recover to a known safe state in the event of an invalid external input.

205.2.6 In-Flight Response to Loss of Function

The CHS shall automatically recover functional performance for those capabilities, which are identified through the safety analysis as requiring automatic recovery. The CHS shall automatically safe in less than the time to catastrophic or critical effect.

205.2.7 Separate Control Path (SCP)

When CS is used for controlling hazards of a must-not-work function, the CS shall use separate control path for each inhibit used to control a hazard.

205.2.8 Monitoring

The CS shall make available to crew and ground operator:

a) the data necessary and sufficient for the performance of manual system safing for identified hazard and
b) the status of monitored inhibits used to control hazards.

206 FIRE PROTECTION

206.1 General

A fire protection system comprised of fire detection, warning, and suppression devices shall be provided. The fire protection system shall encompass both hardware and flight personnel procedures for adequate control of the fire hazard within the internal volume of the CHS. The fire protection system shall incorporate test and checkout capabilities such that the operational readiness of the entire system can be verified by the flight personnel.

The fire protection system shall have redundant electrical power sources and shall incorporate redundant detection and warning capability and redundant activation of suppressant devices.

206.2 Fire Suppressant

Fire suppressant shall be compatible with CHS life support system. The fire suppressant shall not exceed 1-hour spacecraft maximum allowable concentrations (SMAC) levels in any isolated elements and shall be non-corrosive. Fire suppressant by-products shall be compatible with the space system contamination control capability.

206.3 Fire Detection and Annunciation

Fire detection annunciation and control of the fire protection system shall be provided to the crew.

CHAPTER 3 - SAFETY DESIGN REQUIREMENTS

300 GENERAL

The safety design requirements in this standard are applicable to a commercial human-rated space system (CHS) as determined by the safety analysis performed by the commercial developer/operator (CO). When a requirement which is identified as applicable by the safety analysis cannot be met, a noncompliance report shall be submitted to the Space Safety Institute (SSI) in accordance with Appendix C for resolution.

301 STRUCTURES

301.1 Structural Design

The structural design shall provide ultimate factors of safety equal to or greater than 1.5 for all mission phases. This includes loads incurred during operations for all CHS configurations or while changing configuration. A Structural Verification Plan shall be submitted for SSI SRP review and approval in accordance with Appendix C. When failure of structure can result in a catastrophic event, the design shall be based on fracture control procedures to prevent structural failure because of the initiation or propagation of flaws or crack-like defects during fabrication, testing, and service life. Requirements for fracture control are specified in NASA-STD-5019A. Safety critical fasteners shall be procured in accordance with aerospace standards. Safety critical fasteners shall be designed to include redundant features (e.g., torque and self-locking helicoids) to prevent inadvertent back-out.

301.2 Emergency Landing Loads

For air-carried vehicle, the structural design shall comply with the ultimate design load factors for emergency landing loads that are specified in the ICD's between the carrier and the vehicle. Structural verification for these loads may be certified by analysis only.

301.3 Windows Structural Design

Windows number shall be minimized, and all assemblies shall provide a redundant pressure pane. The pressure panes shall be protected from damage by external impact. The structural design of window panes in the pressure hull shall provide a minimum initial ultimate factor of safety of 3.0 and an end-of-life minimum factor of safety of 1.4. Window design shall be based on fracture mechanics considering flaw growth over the design life of the space system.

301.4 Design Allowables

Material design allowables and other physical properties to be used for the design/analysis of flight hardware shall be taken from DOT/FAA/AR-MMPDS-01. For all applications of metals, material "A" allowable shall be used. For non-metallic materials, material equivalent "A" allowables as defined in DOT/FAA/AR-MMPDS-01 shall be used.

301.5 Stress Corrosion

Materials used in the design of the CHS structures shall be rated for resistance to stress corrosion cracking (SCC) in accordance with tables in MSFC-HDBK-527F and MSFC-STD-3029A. Alloys with high resistance to SCC shall be used whenever possible and do not require SSI SRP approval. When failure of a part made from a moderate or low resistance alloy could result in a critical or catastrophic hazard, a Stress Corrosion Evaluation Form from MSFC-HDBK-527F must be included in the relevant hazard report. When failure of a part made from a moderate or low resistance alloy would not result in a hazard, rationale to support the non-hazard assessment shall be included in the stress corrosion hazard report. Approval of the hazard report shall constitute SSI SRP approval for the use of the alloy in the documented applications. Controls that are required to prevent SCC of components after manufacturing shall be identified in the hazard report.

301.6 Pressure Systems

301.6.1 Pressure Control

The maximum design pressure (MDP) for a pressurized system shall be the highest pressure defined by maximum relief pressure, maximum regulator pressure or maximum temperature. Transient pressures shall be considered. Design factors of safety shall apply to MDP. Where pressure regulators, relief devices, and/or a thermal control system (e.g., heaters) are used to control pressure, collectively they shall be two-FT from causing the pressure to exceed the MDP of the system. Pressure integrity shall be verified at system level.

301.6.2 Pressure Vessels

Safety requirements for CHS pressure vessels are listed in the paragraphs below. Particular attention will be given to ensure compatibility of vessel materials with fluids used in cleaning, test, and operation. Data requirements for pressure vessels are listed in Appendix C.

301.6.2.1 Metallic Pressure Vessels

Metallic pressure vessels shall comply with the pressure vessel requirements of ANSI/AIAA S-080A.

301.6.2.2 Composite Overwrapped Pressure Vessels (COPVs)

COPVs shall meet the pressure vessel requirements in ANSI/AIAA S-081B. A damage control plan and stress rupture life assessment shall be developed for each COPV.

301.6.2.3 Pressure Stabilized Vessels

The minimum required pressure shall be verified prior to the application of safety critical loads into the system. This verification shall include a single fault tolerant pressure decay monitoring technique which is implemented such that the system pressure decay characteristics can be certified to insure minimum design safety factors will exist at the time of subsequent structural load application.

301.6.3 Dewars

Dewar/cryostat systems are a special category of pressurized vessels because of unique structural design and performance requirements. Pressure containers in such systems shall be subject to the requirements for pressure vessels specified in paragraphs 301.6 and 301.6.2 as supplemented by the requirements of this section.

1) Pressure containers shall be leak-before-burst (LBB) designs where possible as determined by a fracture mechanics analysis. Containers of hazardous fluids and all non-LBB designs shall employ a fracture mechanics safe-life approach to assure safety of operation.
2) MDP of the pressure container shall be as determined in paragraph 301.6 or the pressure achieved under maximum venting conditions whichever is higher. Relief devices shall be sized for full flow at MDP.
3) Outer shells (i.e., vacuum jackets) shall have pressure relief capability to preclude rupture in the event of pressure container leakage. If pressure containers do not vent external to the dewar but instead vent into the volume contained by the outer shell, the outer shell relief devices shall be capable of venting at a rate to release full flow without outer shell rupture. Relief devices shall be redundant and individually capable of full flow.
4) Pressure relief devices which limit maximum design pressure shall be certified to operate at the required conditions of use. Certification shall include testing of the same part number from the flight lot under the expected use conditions.
5) Non-hazardous fluids may be vented into closed volumes if analysis shows that a worst case credible volume release will not affect the structural integrity or thermal capability of the system.
6) The proof test factor for each flight pressure container shall be a minimum of 1.1 times MDP. Qualification burst and pressure cycle testing is not required if all the requirements of paragraphs 301.6, 301.6.2 and 301.6.3 are met. The structural integrity for external load environments shall be demonstrated.

301.6.4 Pressurized Lines, Fittings, and Components

1) Pressurized lines and fittings with less than a 38 mm (i.e., 1.5-inch) outside diameter and all flex-hoses shall have an ultimate factor of safety equal to or greater than 4.0. Lines and fittings with a 38 mm (i.e., 1.5-inch) or greater outside diameter shall have an ultimate factor of safety equal to or greater than 1.5.
2) All line-installed bellows and all heat pipes shall have an ultimate safety factor equal to or greater than 2.5.
3) Other components (e.g., valves, filters, regulators, sensors, etc.) and their internal parts (e.g., bellows, diaphragms, etc.) which are exposed to system pressure shall have an ultimate factor of safety equal to or greater than 2.5.
4) Secondary compartments or volumes that are integral or attached by design to the above parts and which can become pressurized as a result of a credible single barrier failure shall be designed for safety consistent with structural requirements. These compartments shall have a minimum safety factor of 1.5 based on MDP. If external leakage would not present a catastrophic hazard to the system, the secondary volume shall either be vented or equipped with a relief provision in lieu of designing for system pressure.

301.6.4.1 Flow Induced Vibration

Flexible hoses and bellows shall be designed to exclude flow induced vibrations which could result in a catastrophic hazard to the CHS.

301.6.4.2 Burst Disks

When burst discs are used as the second and final control of pressure to meet the pressure control requirements of 301.6.1, they shall be designed to the following requirements:

a) Burst discs shall incorporate a reversing membrane against a cutting edge to insure rupture.
b) Burst disc design shall not employ sliding parts or surfaces subject to friction and/or galling.
c) Stress corrosion resistant materials shall be used for all parts under continuous load.
d) The burst disc design shall be qualified for the intended application by testing at the intended use conditions including temperature and flow rate.
e) Qualification shall be for the specific part number used, and it shall be verified that no design or material changes exist between flight assemblies and assemblies making up the qualification database.
f) Each flight assembly shall be verified for membrane actuation pressure either by, (1) use of special tooling or procedures to prevent cutting-edge contact during the test or, (2) demonstration of a rigorous lot screening program approved by the SSI Safety Review Panel.

301.7 Pressure Hull

The design of the pressure hull shall comply with the structural design requirements of paragraphs 301.1. The hull maximum design pressure (MDP) shall be determined as defined in paragraph 301.6. The ultimate factor of safety of hull design shall be equal to or greater than 2.0 for both the MDP and the maximum negative pressure differential the hull may be subjected to during normal and contingency operations or as the result of two credible failures. The pressure hull shall be designed to leak-before-burst criteria.

301.8 Depressurization and Re-Pressurization

Equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, re-pressurization, and the depressurized condition without resulting in a hazard.

301.9 Safety Critical Fasteners

CHS safety critical fasteners shall be designed to prevent back out under all environmental conditions.

302 MATERIALS

MSFC-HDBK-527F contains a listing of materials (both metals and nonmetals) with a "rating" indicating acceptability for each material's characteristic. For materials which create potential hazardous situations as described in the paragraphs below and for which no prior test data or rating exists, the CO shall present other test results for the SSI SRP review. The CHS material requirements for hazardous materials, flammability, and offgassing are as follows:

302.1 Hazardous Materials

Hazardous materials shall not be released in the vehicle internal volume or ejected near the CHS. Hazardous fluids must be contained, unless they can be (if necessary) safely vented or dumped. The CO shall submit to the SSI SRP an independent toxicological assessment for all hazardous materials of the CHS.

302.2 Fluid Systems

Particular attention shall be given to materials used in systems containing hazardous fluids. These hazardous fluids include gaseous oxygen, liquid oxygen, fuels, oxidizers, and other fluids that could chemically or physically degrade the system or cause an exothermic reaction. Those materials within the system exposed to oxygen (liquid and gaseous), both directly and by a credible single barrier failure, must meet the requirements of NASA-STD-6001B at MDP and temperature. Materials within the system exposed to other hazardous fluids, both directly and by a credible single barrier failure, must pass the fluid compatibility requirements of NASA-STD-6001B at MDP and temperature. Manufacturer's compatibility data on hazardous fluids may be used to accept materials in this category if approved by the SSI SRP.

302.3 Chemical/Biological Releases

Chemicals and biological materials which would create a toxicity (including irritation to skin or eyes) or cause a hazard to the CHS if released should be avoided. If such chemicals and biological materials cannot be avoided, adequate containment shall be provided by the use of an approved pressure vessel as defined in paragraph 301.6.2 or the use of two or three redundantly sealed containers, depending on the toxicological hazard for a chemical with a vapor pressure below 1034 hPa (absolute). The CO shall assure that each level of containment will not leak under the maximum use conditions (i.e., vibration, temperature, pressure, etc.).

302.4 Flammable Materials

Materials shall not constitute an uncontrolled fire hazard. The minimum use of flammable materials shall be the preferred means of hazard reduction. The determination of flammability shall be in accordance with NASA-STD-6001B. Guidelines for the conduct of flammability assessments are provided in NASA-JSC 29353B. A flammability assessment shall be documented in accordance with Appendix C.

302.5 Internal Air Pressurized Volumes

Materials used in the internal air pressurized volumes shall be tested in accordance with NASA-STD-6001B in the worst-case atmosphere (i.e., oxygen concentration). Fire propagation path considerations also apply.

302.6 Outside Materials

Materials used outside the vehicle shall be evaluated for flammability in an air environment at 1.4-1.7 psi. Propagation path considerations of NASA-JSC 29353B apply for material usages of greater than 1 pound (0.454 kg) and/or dimensions exceeding 12 inch (30.5 cm)

302.7 Material Outgassing

Materials used in the design and construction of the CHS hardware exposed to the vacuum environment shall have low outgassing properties, whenever outgassing products may be detrimental to safety critical devices and functions (e.g., fogging of optical sensors).

302.8 Material Offgassing

Usage in vehicle internal air pressurized volumes of materials which produce toxic levels of offgassing products shall be avoided. The vehicle internal volumes design shall assure that the offgassing load to the flight personnel will not exceed the spacecraft maximum allowable concentrations (SMAC's) of atmospheric contaminants at the time of ingress. Internal volumes will be tested for offgassing characteristics according to NASA-STD-6001B and shall include measurement of the internal atmosphere of a full scale, flight configured vehicle as a final verification of acceptability. Time periods prior to flight personnel ingress during which the system does not have active atmospheric contamination control must be considered.

All items in internal volumes (including payloads and cargo) are required to be subjected to offgassing test (black-box levels) for safety validation. Rigorous material control to ensure that all selected materials have acceptable offgassing characteristics is a possible alternative to black-box level testing, if agreed by SSI SRP.

302.9 Shatterable Materials

Material that can shatter should not be used in the habitable volume unless hazard controls (e.g., positive protection) is provided to prevent fragments from entering the vehicle environment**.**

303 ELECTRICAL/ELECTRONIC SYSTEMS

303.1 Circuit Overload Protection

Electrical power distribution circuitry shall be designed to include circuit protection devices to guard against circuit overloads which could result in distribution circuit damage, generation of excessive hazardous products in internal vehicle volumes, and to prevent damage to other safety critical circuits and interfacing systems and present a hazard to the flight personnel by direct or propagated effects. Electrical equipment shall be designed to provide protection from accidental contact with high voltage and generation of molten metal during mating de-mating of power connectors.

303.2 Fire Ignition Prevention

(a) circuit protective devices shall be sized such that steady state currents in excess of the derated values for wires and cables in NASA TM 102179 are precluded; (b) Wire/cable insulation constructions shall not be susceptible to arc-tracking. All selected wire/cable shall be tested for arc-tracking unless they are polytetrafluoroethylene (PTFE), PTFE aminate or silicone insulated wires; (c) Electrical faults shall not cause ignition of adjacent materials.

303.3 Electrical Systems Separation

Separate safing systems shall be used for nominal CHS system functions and for essential/emergency functions (e.g., fire protection, caution and warning, and emergency lighting, etc.). Essential/emergency functions shall be powered from a dedicated electrical power bus with redundant power sources**.**

303.4 Connectors

Bent pins or conductive contamination in an electrical connector will not be considered a credible failure mode if a post-mating functional verification is performed to assure that shorts between adjacent connector pins or from pins to connector shell do not exist. If this test cannot be performed, then the electrical design shall insure that any pin if bent prior to or during connector mating, cannot invalidate more than one inhibit and that conductive contamination is precluded by proper inspection procedures.

303.5 Batteries

Batteries shall be designed to control applicable 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 overpressure. Safety guidelines for batteries are contained in JSC 20793D.

303.6 Electromagnetic Compatibility

Electromagnetic compatibility between the various elements and electro-pyrotechnic devices shall be ensured.

303.7 Lightning

303.7.1 Lightning Protection

Lightning protection for operations in the Earth's atmosphere shall be designed into the CHS such that in the event of a lightning strike, flight hardware will not be damaged or affected to the extent that flight personnel safety is compromised.

303.7.2 Lightning to Launch Pad

The CHS electrical circuits may be subjected to electromagnetic fields due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard, the circuit design shall be hardened against the environment or insensitive devices (relays) shall be added to control the hazard.

303.7.3 Active Lightning Protection

An active lightning protection system (detection and lightning warning) providing a lightning forecast compatible with the time required to restore the involved system to a safe configuration, shall be implemented for operations involving a potential hazard with catastrophic or critical consequences.

303.8 Electrical Hazards

303.8.1 Exposure Threshold

Hardware and equipment shall be designed to protect the flight personnel from any incidental or intentional exposure above 32 V RMS, as the threshold for a catastrophic hazard.

303.8.2 Leakage Currents

For equipment specifically designed to contact the human body (e.g., medical devices, exercise equipment), electrical leakage currents caused by contact with exposed surfaces shall be kept below the levels specified in Table 1, Leakage Currents – Equipment Designed for Human Contact.

Table 1

<table>
<tr><th colspan="5">Maximum Current (mA RMS)</th></tr>
<tr><th rowspan="2">Body Contact</th><th rowspan="2">Frequency</th><th rowspan="2">Operating Condition</th><th colspan="2">Equipment Type</th></tr>
<tr><th>Isolated Equipment</th><th>Non-Isolated Equipment</th></tr>
<tr><td rowspan="4">External*</td><td rowspan="2">DC to 1 kHz</td><td>Normal</td><td colspan="2">0.1</td></tr>
<tr><td>Single Fault</td><td colspan="2">0.5</td></tr>
<tr><td rowspan="2">>1 kHz</td><td>Normal</td><td colspan="2">Lesser of (0.1 x frequency in kHz) or 5</td></tr>
<tr><td>Single Fault</td><td colspan="2">Lesser of (0.5 x frequency in kHz) or 5</td></tr>
<tr><td rowspan="4">Internal</td><td rowspan="2">DC to 1 kHz</td><td>Normal</td><td>0.01</td><td rowspan="4">Not Allowed</td></tr>
<tr><td>Single Fault</td><td>0.05</td></tr>
<tr><td rowspan="2">>1 kHz</td><td>Normal</td><td>Lesser of (0.01 x frequency in kHz) or 1</td></tr>
<tr><td>Single Fault</td><td>Lesser of (0.05 x frequency in kHz) or 1</td></tr>
<tr><td colspan="5">*For DC currents, there is a small risk of heating and tissue necrosis for prolonged duration of contact.</td></tr>
</table>

303.8.3 Grounding, Bonding, and Insulation

Grounding, bonding and insulation shall be provided for all electrical equipment to protect flight personnel from electrical hazards. The system shall be designed so that it does not generate electric arc or sparks during regular operating mode.

303.9 Electrical, Electronic, and Electromechanical (EEE) Parts

EEE parts used in safety-critical functions shall be selected, specified, screened, and qualified in accordance with the requirements for Level 1 of NASA EEE-INST-002.

304 MECHANISMS

304.1 Design Factors

Safety-critical mechanisms shall be sized to provide actuation forces which exceed the predicted worst-case resistance torques/forces by a factor of at least 2. The following minimum factors are applicable for the components of resistance:

a) Friction: 3
b) Hysteresis: 3
c) Spring: 1.2
d) Inertia: 1.1

When the contributing sources of the components of resistance are multiple and independent, these factors need only to be applied to the two worst sources in each category.

304.2 Lifetime Testing

The lifetime of safety critical mechanisms shall be demonstrated by test in an operationally representative environment, using the sum of the predicted nominal ground test cycles and the flight and in-orbit operation cycles. For the test demonstration, the number of the predicted cycles shall be multiplied by the following factors:

a) Ground Testing cycles x4 (with 10 as minimum number of cycles)
b) Flight and in-orbit cycles:
   - 1 to 10 actuations x10
   - 11 to 1000 actuations x4
   - 1001 to 10000 actuations x2
   - over 10000 actuations x1.25

A full output cycle or full revolution of the mechanism is defined as one actuation. In order to determine the lifetime to be demonstrated by test, an accumulation of actuations multiplied by their individual factors shall be used. Any element in the chain of actuation (motor, bearing, gear, etc.) has to be compliant with the maximum number of cycles applicable to any of the remaining elements in the chain.

305 RADIATION

305.1 Ionizing Radiation

A vehicle containing or using radioactive materials or that generate ionizing radiation shall be identified and approval obtained for their use by the relevant national regulatory body(ies).

305.2 Non-Ionizing Radiation

305.2.1 Natural Radiation Protection

The vehicle shall include the necessary radiation protection features (shielding, radiation monitoring, etc.) required to ensure that flight personnel' dose rates from naturally occurring space radiation are kept as low as reasonably achievable (ALARA). Exposure levels shall not exceed the limits defined in NASA-STD-3001 Volume 2.

305.2.1a Natural Radiation Event Warning

A radiation detection system shall be provided which continuously monitors the interior radiation levels of the vehicle, records the accumulated doses and provides clear notification of radiation conditions within space system.

305.2.2 RF Emission

The system shall protect the flight personnel from exposure to RF non-ionizing radiation beyond the limits in IEEE C95.1.

305.2.3 Use of Onboard Mass

The vehicle shall make optimal use of onboard mass as radiation shielding.

305.3 Windows Transmissivity

The transmissivity of the vehicle windows shall be based on protection of the flight personnel from exposure to excess levels of naturally occurring non-ionizing radiation. Exposure of the skin and eyes of flight personnel to non-ionizing radiation shall not exceed the Threshold Limit Values (TLV) for physical agents as defined by the American Conference of Governmental Industrial Hygienists (ACGIH) in Threshold Limit Values and Biological Exposure Indices. Window design shall be coordinated with other shielding protection design to comply with the ionizing radiation limits specified in NASA-STD-3001 Volume 2.

305.4 Emissions and Susceptibility

CHS emissions shall be limited to those levels identified in the ICDs with interfacing systems. Systems with unintentional radiation level (EMI) above the levels identified in ICDs will be assessed for hazardous impact. Safety critical equipment shall not be susceptible to the applicable electromagnetic environment.

305.5 Lasers

Lasers shall be designed and operated in accordance with ANSI-Z-136.1.

305.6 Optical Requirements

Optical instruments shall prevent harmful light intensities and wavelengths from being viewed by operating and flight personnel. Quartz windows, apertures or beam stops and enclosures shall be used for hazardous wavelengths and intensities. Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems shall be below the Threshold Limit Values (TLV) for physical agents as defined by the ACGIHA in Threshold Limit Values and Biological Exposure Indices.

306 ENVIRONMENT AND HABITABILITY

306.1 General

A safe and habitable internal environment shall be provided within the CHS throughout all operational phases with human on board. Habitability requirements should comply with NASA-STD-3001 Volume 2.

306.2 Life Support System

The CHS life support system shall be able to provide the following functions in any configuration (e.g., open/closed hatches to different habitable volumes or interfacing system) in response to metabolic consumption and loss of cabin atmosphere to space:

a) Monitor total pressure in the range of 0 to 1100 hPa absolute with an accuracy of ±0.7 hPa absolute and report cabin atmospheric pressure once per minute. The system shall alert the crew within 1 minute when the cabin atmosphere pressure drops below 960 hPa absolute for longer than three minutes.

b) Controlled release of gaseous nitrogen and gaseous oxygen into the habitable volume for maintenance and restoration of habitable volume pressure, and to maintain the habitable volume pressure in response to loss of atmosphere to space.
   Remote and manual on/off control of introduction of gaseous nitrogen and gaseous oxygen into the internal atmosphere at a flow rate for each of 0.045 to 0.090 kg per min respectively.
   Capability to maintain cabin total pressure at greater than 972.16 hPa (i.e., 1.4-1.1 psia). This maintenance of cabin pressure shall not cause nitrogen partial pressure to exceed 799.79 hPa (i.e., 11.6 psia), or cabin total pressure to exceed 1027.32 hPa (i.e., 14.9 psia).
c) Capability to maintain oxygen partial pressure above 195.12 hPa (i.e., 2.83 psia). This maintenance of oxygen partial pressure shall not cause the oxygen partial pressure to exceed 230.97 hPa (i.e., 3.35 psia) or 24.1 percent by volume.
d) Control the maximum internal-to-external differential pressure of the space system to less than 1048 hPa (i.e., 15.2 psia). Venting of atmosphere to space shall not occur at less than 1034.21 hPa (i.e., 15.0 psia).
e) Monitor atmosphere temperature over the range of 15.5 to 32.2 °C (i.e., 60 to 90 °F) with an accuracy of ±0.5 °C (i.e., 1 °F).
f) Detect combustion products over specified ranges.
g) Monitor the atmosphere of carbon dioxide partial pressure over a range of 0 to 20 hPa (i.e., 15 mmHg) with an accuracy of ±1% of full scale.
h) Remove gaseous contaminants to maintain contaminant concentrations in the atmosphere below acceptable limits, which are defined as less than or equal to the Spacecraft Maximum Allowable Concentration (SMAC) levels.

306.3 Contamination Control

Specific design and mission provisions shall be made for contamination control of the vehicle internal volume. The internal environment shall be monitored and assessed for particulate, molecular and microbiological contamination SMAC's of atmospheric contaminates are specified in Tables 2 and 3.

Table 2

Spacecraft maximum allowable concentrations						
		Potential Exposure Period				
Chemical		1 h	24 h	7 d	30 d	180 d
Acetaldehyde	mg/m^3	20	10	4	4	4
Acrolein	mg/m^3	0.2	0.08	0.03	0.03	0.03
Ammonia	mg/m^3	20	14	7	7	7
Carbon Dioxide	mm Hg	10	10	5.3	5.3	5.3
Carbon monoxide	mg/m^3	60	20	10	10	10
1,2-Dichloroethane	mg/m^3	2	2	2	2	1
2-Ethoxyethanol	mg/m^3	40	40	3	2	0.3
Formaldehyde	mg/m^3	0.5	0.12	0.05	0.05	0.05
Freon 113	mg/m^3	400	400	400	400	400
Hydrazine	mg/m^3	5	0.4	0.05	0.03	0.005
Hydrogen	mg/m^3	340	340	340	340	340
Indole	mg/m^3	5	1.5	0.25	0.25	0.25
Mercury	mg/m^3	0.1	0.02	0.01	0.01	0.01
Methane	mg/m^3	3800	3800	3800	3800	3800
Methanol	mg/m^3	40	13	9	9	9
Methyl ethyl ketone	mg/m^3	150	150	30	30	30
Methyl hydrazine	mg/m^3	0.004	0.004	0.004	0.004	0.004
Dichloromethane	mg/m^3	350	120	50	20	10
Octamethyltrisiloxane	mg/m^3	4000	2000	1000	200	40
2-Propanol	mg/m^3	1000	240	150	150	150
Toluene	mg/m^3	60	60	60	60	60
Trichloroethylene	mg/m^3	270	60	50	20	10
Trimethysilanol	mg/m^3	600	70	40	40	40
Xylene	mg/m^3	430	430	220	220	220

Table 3

Combustion product detection	
Compound	Range (ppm)
Carbon Monoxide (CO)	5 to 400
Hydrogen Chloride (HCL)	1 to 100
Hydrogen Cyanide (HCN)	1 to 100
Hydrogen Fluoride (HF) / Carbonyl Fluoride (COF_2)	1 to 100

306.4 Acoustic Noise

The flight personnel shall be provided with an acoustic environment that will not cause injury or hearing loss, interfere with voice or any other communications, cause fatigue, or in any other way degrade overall human/machine system effectiveness. Acoustic noise limits are specified in NASA-STD-3001 Volume 2.

306.5 Vibration

The vehicle vibration environment shall not cause injury, fatigue, or in any other way degrade human/machine system effectiveness (e.g., instrument reading). The vibration exposure limits are specified in NASA-STD-3001 Volume 2.

306.6 Internal Mechanical Hazards

The vehicle internal design shall protect the flight personnel from sharp corners and edges, during all flight operations. Requirements on sharp corner and edges are specified in NASA-STD-3001 Volume 2. There shall be no sharp edges in structures in areas where cables are installed to avoid any possibility of damaging cables. Protrusions greater than 3.05 mm (0.12 inch) of threads of screws/bolts in the vehicle habitable volumes, are also sharp edges to be controlled.

306.7 External Mechanical Hazards

All surfaces, and edges shall be smooth, rounded, and free of burrs. In addition, the following criteria apply:

a) vehicle external equipment and structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with Table 4;
b) materials less than 2.032 mm (0.08 inch) thick, with exposed edges that are uniformly spaced, not to exceed 12.7 mm (0.5 inch) gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.0762 mm (0.003 inch);
c) all latching devices shall be covered in a manner that does not allow gaps or overhangs that can catch fabrics or pressure suit appendages, or shall be designed in a manner to preclude the catching of fabrics and pressure suit appendages;
d) all lap joints in sheet metal and mismatching of adjacent surfaces shall be mated within 0.03 inch (0 8 mm) of flat surface at edges or shall be butted or recessed. All exposed edges must be smooth and radiused 0.06 inch (1.5 mm) minimum, chamfered 45°, or shall be covered with an appropriate material to protect EVA gloves;

Table 4

Edge, Corner and Protrusion Criteria – Edge and In-Plane Corner Radii

Application	Radius				Remarks	Figure II.2-5 Referenced
	Outer		Inner			
	in.	mm	in.	mm		
(a) Openings, panels, covers (corner radii in plane of panel)	0.25	6.4	0.12	3.0	Preferred	
	0.12	3.0	0.06	1.5	Minimum	
(b) Exposed corners:	0.50	13.0	–	–	Minimum	(a)
(c) Exposed edges: (1) 0.08 in. (2.0 mm) thick or greater	0.04	1.0	–	–		(b)
(2) 0.02 to 0.08 in. (0.5 to 2.0 mm) thick	Full Radius		–	–		(c)
(3) less than 0.02 in. (0.5 mm) thick	Rolled or Curled					(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.

e) sheet metal structure, box and cabinet three-plane intersecting corners shall be spherical welded or have formed radii unless comers are protected with covers;
f) All screwheads and bolt heads shall face the outside of the structure, if possible. Where nuts, nut plates, and threads are exposed, the nuts, nut plates and threads are exposed, the nuts, not plates and threads shall be covered in a secure manner. Recessed heads or the use of recessed washers is recommended. Overall height of heads shall be within 0.125 inch (3.2 mm) or covered unless more than 7 head diameters apart from center to center. Height of roundhead or oval head screws is not limited. Screwheads or bolt heads more than 0.25 inch (6.4 mm) deep must be recessed or be covered with a fairing, except those intended to be EVA crew interfaces.
g) Rivet heads shall face out on all areas accessible to crewmember and shall protrude no more than 0.06 inch (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 inch (3.1 mm), or 0.50 inch (12.7 mm) of unset and diameter if more than 0 12 inch (3.1 mm), a fairing shall be installed over them. This applies to explosive, blind, or pull rivets, etc. LJnset ends of rivets must have edges chamfered 45° or ground off to a minimum radius of 0.06 inch (1.5 mm).
h) a maximum gap of 0.02 inch (0.5 mm) shall be allowed only between one side of a fastener head and its mating surface.
i) torque-set, slotted, or Phillips head screws must be covered with tape or other protective materials or be individually deburred before flight

306.8 Thermal Hazards

During normal operations, the flight personnel shall not be exposed to contact with objects at high or low surface temperature extremes. Any object to which the bare skin of the flight personnel is exposed shall not cause epidermis/dermis interface temperature to exceed the pain threshold upper limit of 44 °C (111.2 °F), or the pain threshold lower limit of 10 °C (50 °F). Because the thermal properties of the object in contact will drive the heat transfer from the surface to the skin (and vice versa for the cold case), and the temperature that the epidermis/dermis interface will reach, the Maximum/Minimum Permissible Temperature (TPM) for unintentional contact (less or equal to 1 second) or intentional contact shall be calculated with the method in NASA-STD-3001 Volume 2. Protection shall be provided against continuous skin contact with surfaces above or below the TPM. Safeguards such as warning labels, protective devices or special design features to protect the flight personnel from contact with objects at temperatures outside the TMP safe limits, shall be provided for both nominal and contingency operations.

306.9 Illumination

The lighting illumination level provided throughout the space system shall permit planned crew activities without injury. A backup/secondary lighting system shall be provided consistent with emergency egress requirements or in case of failure of the primary lighting system.

306.10 Hatches

The space system hatch design shall be compatible with emergency flight personnel. Hatches between different habitable modules shall provide a capability to allow a visual inspection of the interior of the space system prior to hatch opening and flight personnel ingress. All operable hatches that could close and latch inadvertently, thereby blocking an escape route, shall have a redundant (backup) opening mechanism and shall be capable of being operated from both sides.

External pressure hatches (i.e., interfacing directly to space vacuum) shall be self-sealing (i.e., inward opening). Hatches shall have a pressure difference indicator clearly visible to the flight personnel operating the hatch and a pressure equalization device. All hatches shall nominally be operable without detachable tools or operating devices and shall be designed to prevent inadvertent opening prior to complete pressure equalization. Hatches at docking locations shall provide the capability to verify that the environment is within the oxygen, nitrogen and carbon dioxide levels as well as within the SMAC levels (of selected compounds) provide visual inspection of the interior of the pressurized volume prior to crew ingress into an unmanned cargo transportation spacecraft.

306.11 Access to Moving parts

Moving parts such as fans, belt drives, and similar components that could cause flight personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices.

306.12 Communications

The vehicle shall provide the capability for direct voice communication between crewed vehicles (2 or more) during proximity operations.

307 SAFE RETURN AND LANDING

307.1 Winged System

The civil aviation airworthiness regulations and certification requirements may apply for such use, as determined by the relevant national civil aviation authority

307.2 Capsule Recovery

307.2.1 Capsule Environment

The CHS shall maintain a safe and habitable environment for the crew inside the spacecraft after Earth landing until the arrival of the landing recovery team or rescue forces.

307.2.2 Capsule Localization

The CHS shall provide recovery forces with the location of the spacecraft after return to Earth.

308 HAZARDOUS OPERATIONS

308.1 Hazard Identification

The CO shall assess all CHS flight (and ground) operations and determine their hazard potential. The hazardous operations identified shall be assessed in the applicable flight (or ground) safety assessment report. (Note: Those ground operations (e.g., arm plug installation in a CHS pyrotechnic system, final ordnance connection, etc.) which place the CHS in a configuration of increased hazard potential shall be accomplished as late as practicable during the CHS processing flow at the spaceport).

308.2 Access to Moving Parts

Moving parts such as fans, belt drives, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices

CHAPTER 4 - CERTIFICATION REQUIREMENTS

400 SYSTEM PROGRAM REQUIREMENTS

The following requirements are applicable to the CHS flight safety certification by the Space Safety Institute.

401 SAFETY ANALYSIS

A safety analysis shall be performed in a systematic manner on the CHS, its elements, related software, and flight operations to identify hazardous subsystems and functions. The safety analysis shall be initiated early in the design phase and shall be kept current throughout the development phase. A safety assessment report which documents the results of this analysis, including hazard identification, classification, and resolution, and a record of all safety-related failures, shall be prepared, maintained, and submitted in support of the safety assessment reviews conducted by the SSI Safety Review Panel. Detailed instructions for the safety analysis and safety assessment reports are provided in Appendix C.

402 HAZARD REDUCTION

Hazards are classified according to potential as critical or catastrophic hazards. Action for reducing hazards shall be conducted in the following order of precedence:

402.1 Safety-by-Design

The major goal throughout the design phase shall be to insure inherent safety through the selection of appropriate design features, which eliminates as much as possible the hazards. Damage control, containment, and isolation of potential hazards shall be included in design considerations.

402.2 Safety Devices

Hazards which cannot be eliminated through design selection shall be reduced and made controllable through the use of automatic safety devices as part of the system, subsystem, or equipment.

402.3 Warning Devices

When it is not practical to preclude the existence or occurrence of known hazards or to use automatic safety devices, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal, coupled with emergency controls of corrective action for operating personnel to safe or shut down the affected subsystem. Warning signals and their application shall be designed to minimize the probability of wrong signals or of improper reaction to the signal.

402.4 Special Procedures

Where it is not possible to reduce the magnitude of an existing or potential hazard through design or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of flight personnel safety.

403 SAFETY ASSESSMENT REVIEWS AND SAFETY CERTIFICATION

Safety assessment reviews will be conducted by the SSI Safety Review Panel to determine compliance with the requirements of this document, excluding any aspect of public safety and ground personnel safety which are regulated by national bodies and by the spaceport safety authority. An initial contact meeting will be held at the earliest appropriate time and will be followed by formal review meetings spaced throughout the development phase. The depth, number, and scheduling of reviews will be negotiated with the CO and will be dependent on complexity, technical maturity, and hazard potential.

404 SAFETY COMPLIANCE DATA

Safety compliance data packages shall be prepared by the CO.

404.1 Data

The data listed below shall be submitted as part of the data package for the phase III flight safety review.

a) A safety assessment report (safety data package) for CHS design and flight and ground operations.
b) CHS safety verification tracking log for verifications that cannot be concluded before phase III safety review.
c) Approved noncompliance reports (waivers and deviations).
d) A summary and safety assessment of all safety related failures and accidents applicable to CHS processing, test, and checkout.
e) A list of all pyrotechnic initiators installed or to be installed on the CHS, giving the function to be performed, the part number, the lot number, and the serial number. Submittal of this list may be delayed to be concurrent with the submittal of the flight safety certification statement.
f) A log book template for each limited life item which will be kept current over the CHS lifetime.

404.2 Post-Phase III Compliance

When the flight certification statement of paragraph 404 is submitted, it shall be included with an updated CHS safety verification tracking log that documents the closeout of all required safety verification. The verification tracking log and the certification statements shall reflect the final configuration of the CHS that includes all post phase III safety activity.

405 VERIFICATION

Test, analysis, inspection and demonstration are common techniques for verification of design features used to control potential hazards. The successful completion of the safety process will require positive feedback of completion results for all verification items associated with a given hazard. Reporting of results by procedure/report number and date is required.

405.1 Mandatory Inspection Points (MIP's)

When procedures and/or processes are critical steps in controlling a hazard and the procedure and/or process results will not be independently verified by subsequent test or inspection, it will be necessary to insure the procedure/process is independently verified in real-time. Critical procedure/process steps shall be identified in the appropriate hazard reCOrt as MIP's requiring independent QA observation.

405.2 Verification Tracking

Safety verification tracking (see Appendix C) is required to properly status the completion steps associated with hazard report verification items.

406 REUSABLE SYSTEMS

406.1 Recertification of Safety

Reusable systems shall be recertified safe and shall meet all the safety requirements of this document. Caution should be exercised in the use of previous safety verification data for the new flight.

406.2 Previous Flight Safety Deficiencies

All anomalies during the previous flight shall be assessed for safety impact. Those anomalies affecting safety critical systems shall be reported and corrected. Rationale supporting continued use of the affected design, operations or hardware shall be provided for SSI Safety Review Panel review and approval.

406.3 Limited Life Items

All safety critical age sensitive equipment shall be refurbished or replaced to meet the requirements of the new flight.

406.4 Refurbishment

Safety impact of any changes, maintenance or refurbishment made to the hardware or operating procedures shall be assessed and reported in the safety assessment reviews. Hardware changes include changes in the design, changes of the materials of construction, etc.

407 MISHAP/INCIDENT/MISSION FAILURES INVESTIGATION AND REPORTING

Mishap/incident/flight failures investigation and reporting will be handled under the provisions of the applicable national regulations.

APPENDIX A - GLOSSARY OF TERMS AND ACRONYMS

ABORT. A specific action or sequence of actions initiated by an on-board automated function, by crew, or by ground control that terminates a flight process.

ACGIHA. American Conference of Governmental Industrial Hygienists.

ADIABATIC COMPRESSION DETONATION. 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.

AE. Approach Ellipsoid.

AI. Approach Initiation.

AIAA. American Institute of Aeronautics and Astronautics.

ANOMALY. The unexpected performance of intended function.

ANSI. American National Standards Institute.

ASE. Airborne Support Equipment.

CATASTROPHIC EVENT. Loss of life, life threatening or permanently disabling injury or occupational illness, loss of system, loss of an interfacing crewed flight system, loss of launch site facilities. Severe detrimental environmental effects.

CDR. Critical Design Review.

CERTIFICATE OF SAFETY COMPLIANCE. A formal written statement by the CHS Operator attesting that the CHS is safe and that all safety requirements for this document have been met and, if not, what waivers and deviations are applicable.

CHS ELEMENT. Subsystems, equipment and any other subset of a CHS.

CHS. A human-rated system commercially developed and operated to perform suborbital, orbital, or interplanetary flights. In this document, the requirements referring to the CHS apply to the intergraded configuration (i.e., vehicle integrated on launcher or carrier) and to the vehicle after separation.

CITE. Cargo Integration Test Equipment.

CO. Commercial Human-rated System Developer/Operator.

COMPUTER SYSTEM. A computer system is the composite of hardware and software components.

CONTROL. A device or function that operates an inhibit is referred to as a control for an inhibit and does not satisfy inhibit requirements. The electrical devices that operate the flow control devices in a liquid propellant propulsion system are exceptions in that they are referred to as electrical inhibits. The term “control" is also used in this document to indicate any measure aimed to hazard reduction (e.g., redundancies, safety factors, etc.) (see Hazard Control).

COPV. Composite Overwrapped Pressure Vessel.

CORRECTIVE ACTION. Action taken to preclude occurrence of an identified hazard or to prevent recurrence of a problem.

CREDIBLE. A condition that can occur and is reasonably likely to occur. For the purposes of this document, failures of structure, pressure vessels, and pressurized lines and fittings are not considered credible failure modes if those elements comply with the applicable requirements of this document.

CRITICAL EVENT. Temporarily disabling but not life-threatening injury; occupational illness. Major damage to interfacing flight system(s); Major damage to ground facilities, public or private property. Major detrimental environmental effects. Also an event that leads to the need to use a contingency procedure.

DEVELOPER/OPERATOR (CO). The company which develops and/or operates the CHS.

DEVIATION. Granted use or acceptance for more than one flight of a CHS aspect which does not meet the specified requirements. The intent of the requirement should be satisfied, and a comparable or higher degree of safety should be achieved.

DFMR. Design for Minimum Risk.

EEE. Electrical, Electronic, and Electromechanical (parts).

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.

EMERGENCY. Any condition which can result in flight personnel injury or threat to life and requires immediate corrective action, including predetermined flight personnel response.

FACTOR OF SAFETY. The factor by which the limit load is multiplied to obtain the ultimate load. The limit load is the maximum anticipated load or combination of loads, which a structure may be expected to experience. Ultimate load is the load that a system shall be able to withstand without failure.

FAILURE/FAULT TOLERANCE. The number of failures/faults which can occur/exist in a system or subsystem without the occurrence of a hazard. Single failure/fault tolerance would require a minimum of two failures/faults for the hazard to occur. Two-failure/fault tolerance would require a minimum of three failures/faults for a hazard to occur.

FAILURE. The event when a required function is terminated. The unacceptable performance (exceeding the acceptable limits) of an intended function.

FAULT. The inability of a system, subsystem, component or part to perform its required function under specified conditions for a specified duration. A fault is hence a state.

FDS. Fire Detection and Suppression.

FINAL SEPARATION. Final separation is achieved when the last physical connection between the vehicle and its launcher or carrier is severed and the vehicle becomes autonomous.

FIRE EVENT. Localized or propagating combustion, pyrolysis, smouldering or other thermal degradation processes, characterized by the potentially hazardous release of energy, particulates or gasses.

FLIGHT ABORT. An abort of a flight wherein the CHS, or the vehicle returns to a landing site.

FLIGHT CREW. Any flight personnel onboard the CHS engaged in flying the CHS and/or managing resources onboard, e.g., commander, pilot.

FLIGHT PERSONNEL. Flight crew and space flight participant.

FRR. Flight Readiness Review.

FT. Failure/Fault Tolerant.

GFE. Government Furnished Equipment.

GROUND CONTROL PERSONNEL. With respect to spaceflight monitoring, the term includes any personnel supporting the flight from a console in a flight control center or other support area.

GSE. Ground Support Equipment.

HAZARD CONTROL. Design or operational feature used to reduce the likelihood of occurrence of a hazardous effect.

HAZARD DETECTION. An alarm system used to alert the crew to an actual or impending hazardous situation for which the crew is required to take corrective or protective action.

HAZARD. The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of an 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 flight personnel or vehicle. 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 such as the removal of a required safety inhibit to a hazardous function.

HAZARDOUS FUNCTIONS. Hazardous functions are operational events (e.g., motor firings, appendage deployments, active thermal control, etc.) whose inadvertent operations or loss may result in a hazard.

HUMAN PRESSURIZED VOLUME. Any module in which a person can enter and perform activities in a shirt-sleeve environment.

HUMAN-RATED. A human-rated space system is a system that accommodates human needs, effectively utilizes human capabilities, controls hazards with sufficient certainty to be considered safe for human operations, and provides, to the maximum extent practical, the capability to safely recover the crew from hazardous situations.

IAASS. International Association for the Advancement of Space Safety.

ICD. Interface Control Document.

INDEPENDENT INHIBIT. Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

INHIBIT. 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.).

INTERLOCK. A design feature that ensures that any conditions perquisite for a given function or event are met before the function or event can proceed.

ITAR. International Traffic in Arms Regulations.

KOS. Keep-Out Sphere.

LBB. Leak-Before-Burst.

M/OD. Meteoroid/Orbital Debris.

MDP. Maximum Design Pressure.

MIP. Mandatory Inspection Points.

MISHAP/INCIDENT. An unplanned event which results in personnel fatality or injury; damage to or loss of the system, environment, public property or private property; or could result in an unsafe situation or operational mode. A mishap refers to a major event, whereas an incident is a minor event or episode that could lead to a mishap.

MONITOR. Device use to ascertain the safety status of the space system functions, devices, inhibits, and/or parameters.

MUA. Material Usage Agreement.

NASA. National Aeronautics and Space Administration.

NCR. Noncompliance Report.

OFFGASSING. The emanation of volatile matter of any kind from materials inside the vehicle internal air pressurized volumes.

OPERATOR ERROR. Any inadvertent action by either flight or ground personnel that could eliminate, disable, or defeat an inhibit, redundant system, or other design features that is provided to control a hazard. The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or a wrong keystroke or an inadvertent switch throw.

PDR. Preliminary Design Review.

PRESSURE VESSEL. A container designed primarily for pressurized storage of gases or liquids and: (1) contains stored energy of 19.30 kJ (i.e., 14,240 foot-pounds) (0.0045 kg trinitrotoluene equivalent) or greater based on adiabatic expansion of a perfect gas; or (2) will experience a design limit pressure greater than 6894.75 hPa (i.e., 100 psia); or (3) contains a fluid in excess of 1034.21 hPa (i.e., 15 psia) which will create a hazard if released.

PTFE. Polytetrafluoroethylene.

RCS. Reaction Control System.

REAL-TIME MONITORING (RTM). Real-time monitoring is defined as immediate notification to the crew. RTM shall be accomplished via the use of the space system failure detection and annunciation system.

REUSABLE SYSTEMS. Reusable systems are those CHS elements which are made up of hardware items that are foreseen for reuse.

RISK. Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity.

SAFE HAVEN. A functional association of capabilities and environments that is initiated and activated in the event of a potentially life-threatening anomaly and allows human survival until rescue, the event ends, or repair can be affected.

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 the function of critical equipment.

SAFETY ANALYSIS. The technique used to systematically identify, evaluate, and resolve hazards.

SAFETY-CRITICAL. An item is safety-critical if the failure or defective design could cause a risk to human life. (Note: Mission-critical refers instead to a loss of capability leading to possible reduction in mission effectiveness).

SAFETY-CRITICAL FUNCTIONS. A safety critical function is a function whose proper performance is essential to system operation such that it does not pose an unacceptable level of risk. Safety critical functions are either “must-work” and/or “must-not-work” functions. For instance, “must work” safety critical functions are those functions that must work to ensure flight personnel survival in the space environment (e.g., life support system). “Must-not-work” functions are those that can cause catastrophic consequences if inadvertently activated (e.g., rocket motor firing at the wrong moment). A “must work” function in a phase of the flight make become a “must-not-work” function in another phase of the flight and vice versa.

SAFING. An action or sequence of actions 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).

SMAC. Spacecraft Maximum Allowable Concentration (SMAC) is the max concentration of a gas, vapor or fume that a human may be safely exposed to over a designated period of time.

SPACE FLIGHT PARTICIPANT. Any human on board the space system while in flight that has no responsibility to perform any mission task for the system, it is also referred to as space passenger.

SPACE SYSTEM ELEMENT. A subset of a space system (e.g., crewed vehicle, launcher).

SRP. System Safety Review Panel.

SSI. Space Safety Institute.

STRUCTURE. Any assemblage of materials which is intended to sustain mechanical loads.

TLV. Threshold Limit Value.

TPM. Maximum/Minimum Permissible Temperature (TPM) of an object inside the vehicle internal volume.

VEHICLE. A vehicle, referred to in this standard, is a spacecraft, capsule or winged system designed to transport humans and/or cargo (accessible by humans) on orbital sub-orbital, or interplanetary flight.

APPENDIX B - APPLICABLE DOCUMENTS

The latest revision and changes of the following documents form a part of this document to the extent specified herein. In the event of conflict between the reference documents and the contents of this document, the contents of this document will be considered superseding requirements.

AIAA-S-113, Criteria for Explosive Systems & Devices on Space & Launch Vehicles

American Conference of Governmental Industrial Hygienists (ACGIH), Threshold Limit Values and Biological Exposure Indices

ANSI/AIAA S-080A, Space Systems – Metallic Pressure Vessels, Pressurized Structures, and Pressure Components

ANSI/AIAA S-081B, Space Systems Composite Overwrapped Pressure Vessels (COPVs)

ANSI-Z-136.1, American National Standard for Safe Use of Lasers

AS-9100, Quality Management Systems - Requirements for Aviation, Space and Defense Organizations

DOT/FAA/AR-MMPDS-01, Metallic Materials Properties Development and Standardization (MMPDS)

IAASS-SSI-1700-01, Safety Management System - Requirements for Space Organizations (TO BE ISSUED)

IEEE C95.1, "IEEE Standard for Safety Levels with Respect to Human Exposure to Radio-Frequency Electromagnetic Fields, 3 kHz to 300 GHz"

ISO 24113, "Space systems -- Space debris mitigation requirements"

JSC 20793D, Crewed Space Vehicle Battery Safety Requirements

MSFC-HDBK-527F, Materials Selection List for Space Hardware Systems

MSFC-STD-3029A, Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments

NASA EEE-INST-002, Instructions for EEE Parts Selection, Screening, Qualification, and Derating (maintained by GSFC)

NASA JSC 29353B, Flammability Configuration Analysis for Spacecraft Applications

NASA-STD-3001, NASA Space Flight Human System Standard. **Volume 1A**, Crew Health; **Volume 2A**, Human Factors, Habitability, and Environmental Health

NASA-STD-5019A, Fracture Control Requirements for Spaceflight Hardware

NASA-STD-6001B, Flammability, Offgassing, and Compatibility Requirements and Test Procedures

NASA-STD-8719.13B, Software Safety

NASA TM 102179, Selection of Wires and Circuit Protective Devices for STS Orbiter Vehicle Payload Electrical Circuits

NSTS 08060, Space Shuttle System Pyrotechnic Specification

APPENDIX C - SAFETY REVIEW PROCESS AND DATA SUBMITTAL REQUIREMENTS

C-1 GENERAL

The CO is responsible for assuring the safety of its system and for complying with the safety technical requirements of this standard. To this end, the CO must accomplish the following:

- Perform a Safety Analysis as Part of the Design
- Document Compliance with the Technical Safety Requirements
- Present the Documentation to the SSI Safety Review Panel (SRP)

C-1.1 Performance of Safety Analysis as Part of Design

To demonstrate that the system design and operations meet the technical safety requirements of this standard, the CO shall perform a safety analysis. The primary objectives of the safety analysis process are to identify the hazards applicable to a system and its operations, and their causes, and to assure that the hazard controls (i.e., design solutions and operational procedures) and relevant verifications are adequate and in compliance with the safety technical requirements. The safety analysis shall begin during the project concept phase and shall be refined and expanded as the design matures. For situations in which system hardware will be installed or reconfigured in-flight or in which the system will be in-flight for an extended time, safety analyses shall consider the necessity of in-flight maintenance operations, and in-flight verification/reverification of hazard controls.

C-1.1.1 Level of Analysis

In order to identify the hazards applicable to a system, the CO shall conduct safety analyses both at system and subsystem levels. Each system and subsystem shall be evaluated to determine the applicability of each technical safety requirement.

For hardware developed for or provided to the CO, the CO shall:

a) Obtain the appropriate safety data from the supplier or conduct an independent safety analysis.
b) Conduct a safety analysis of the interfaces between the subject hardware and other elements.

C-1.1.2 Analysis Techniques

Depending on the complexity of the system, the CO should use established primary and supporting analytical techniques (e.g., Preliminary Hazard Analysis, Sneak Circuit Analysis, Fault-Tree Analysis, Operational Hazard Analysis, Failure Modes and Effects Analysis) to obtain the data necessary to complete, present, and support system hazard reports.

C-1.2 Documenting Compliance with Safety Technical Requirements

The safety analysis results shall be documented in the Safety Data Package (SDP), which includes the description of the system and its operations, and the system hazards reports. The hazard reports are the key part of the SDP and are used to systematically and formally document the compliance of the system with the safety technical requirements.

The flight SDP submittal must contain all flight hazard reports. Each hazard report must be signed and dated by the CO program manager prior to submittal. Hazard reports must be prepared using forms recommended by the SSI or agreed equivalent.

The CO is responsible for retaining and maintaining the original hazard reports after approval.

C-1.3 Safety Reviews and Meetings

Review meetings may be formal, or out-of-board as deemed appropriate by the SSI SRP Chairman. Safety reviews may take place in person, via teleconference, or by correspondence.

C-1.3.1 Formal Safety Review Meeting

Formal safety review meetings constitute a gathering of the safety review panel, representatives of the CO, and the appropriate supporting technical staff. Usually, safety review meetings are held at phases 0, I, II, III levels that corresponds to the project phases that conclude with conceptual, preliminary, and critical design reviews, and qualification/certification and acceptance reviews. Following a technical discussion during the meeting, the SSI SRP Chairman will provide a disposition for each hazard report. This disposition may take one of the following forms: (1) approved as written, (2) approved with modification, (3) approved with an action to be performed by the CO and/or SSI SRP, and (4) not approved. Successful completion of each safety review phase is documented by approval of all Hazard Reports by the SSI SRP Chairman. Splinter meetings with experts teams may be held concurrently with a safety review meeting to discuss detailed technical concerns. The results are then reported to the safety review panel for information and/or disposition.

C-1.3.2 Out-of-Board Meeting

Out-of-board meetings do not require the full safety panel. Attendees may include the Panel Chairman, safety representative(s), representatives of the CO, and others necessary to address the issues that may be involved.

C-1.3.3 Technical Interchange Meeting (TIM)

The review panel and/or associated technical staff may convene upon request in order to assist in interpreting safety requirements or to coordinate safety analyses/issues prior to safety reviews. Requests for flight safety TIMs should be coordinated with the SSI SRP Executive Secretary.

C-2 PHASED SAFETY REVIEWS

C-2.1 Phase 0 Safety Review

The objectives of the Phase 0 Safety Review are to:

a) Assist the CO in identifying hazards, hazard causes, and applicable safety requirements early in the development of the system.
b) Adequately describe the hazard potential.
c) Answer questions regarding the interpretation of the safety requirements or the implementation procedures of this standard.
d) Provide guidance to the CO for preparing the safety data required for subsequent safety reviews.

The following data are required for the phase 0 SDP:

1) Conceptual system description (including subsystems) and mission scenario.
2) Description of safety-critical subsystems and their operations.
3) Hazard Reports.

The description of the system and its operation must be of sufficient detail to permit identification of all subsystems that may create hazards. Emphasis should be given to those subsystems that store, transfer, or release energy. The descriptions of the safety-critical subsystems must be of sufficient detail to identify the hazards in terms consistent with the conceptual design level.

The purpose of a phase 0 hazard report is to document and scope the specific hazards identified. It is intended to be a working document for discussion and critique at the phase 0 safety review and will not require signatures. A hazard report must be prepared for each hazard identified in the safety analysis. The hazards contained on the phase 0 hazard report must reflect the system conceptual design and operations existing at the time of the phase 0 review. For phase 0, the CO may identify hazard controls, verification methods, or status of verifications.

C-2.2 Phase I Safety Review

The purpose of the phase I safety review is to obtain SSI SRP approval of the updated safety analysis that reflects the preliminary design and operations scenario of the system. At this point, the CO shall present a refined safety analysis that identifies all hazards and hazard causes inherent in the preliminary design; evaluates all hazards for means of eliminating, reducing, or controlling the risk; and establishes preliminary safety verification and in-flight verification/reverification methods. The CO shall provide a preliminary identification of the system interfaces and of the hazards presented by these interfaces.

The following data are required for the phase I SDP:

1) Updated system description (including subsystems) and mission scenario.
2) Updated descriptions of safety-critical subsystems and their operations, including schematics and block diagrams with safety features, inhibits, and controls identified. Identify any safety-critical subsystem that is computer controlled, and identify the functional architecture associated with that computer control.
3) Updated and additional (if any) flight hazard reports.
4) A summary list (in the SDP system description) of launcher or carrier-provided critical services, and an explanation (in the appropriate hazard reports) of how those services are used to control and/or monitor system hazards.
5) A presentation of the Fire Detection and Suppression (FDS) implementation approach.
6) Discussion of design features supporting verification/reverification of hazard controls in-flight and associated constraints.
7) A tabulated list of tentative toxic materials and support data.
8) A list of all battery types, their uses, manufacturer, and applications.
9) A preliminary description of all pyrotechnic devices and their functions.
10) If applicable, preliminary in-flight maintenance safety

The CO shall prepare phase I hazard reports for each hazard identified as a result of the safety analysis for the preliminary design and operations scenario of the system. Hazard reports shall be added to or deleted from those agreed to during phase 0 to reflect the updated safety analysis. Rationale for deleting a hazard report agreed upon at phase 0 shall be presented during the phase I review.

For phase I, the CO shall identify hazard controls for each hazard cause identified at phase 0. A direct correlation between each hazard cause and the corresponding hazard control(s) must be clearly shown on the report. Sufficient supporting information detailing each hazard control must be provided as annex to the hazard report.

Verifications should include the types of tests, analyses, inspections, or demonstrations to be used to verify each hazard control, including all launcher or carrier-provided services or interfaces, both prelaunch and in-flight. A direct correlation between each verification method and the corresponding hazard control must be clearly shown on the report. Each verification item should be independent and have a designator that allows for individual tracking of verification status.

Manufacturing/assembly procedures/processes that are critical in controlling hazards that cannot or will not be verified by subsequent inspection or test must be verified during the manufacturing/assembly process. An independent verifier, as specified by the CO, shall attest to proper completion of the procedure/process. Critical procedures/processes, which require special monitored verification (Mandatory Inspection points [MIPs]), shall be identified in preliminary fashion.

C-2.3 Phase II Safety Review

The purpose of the phase II safety review is to obtain SSI Safety Review Panel approval of the updated SDP that reflects the CDR-level design and operations scenario of the system. The phase II safety analysis identifies all hazards and hazard causes; defines and documents implementation of means for eliminating, reducing, or controlling the risks; and documents finalized, specific safety verification and in-flight verification/reverification methods (test plans, analysis, inspection requirements, etc.). System interfaces, mission operations, procedures, and timelines that were not addressed during the phase I safety review shall be assessed for safety hazards. The system interfaces to be assessed shall include those between the launcher or carrier and the system and among the various components that make up the system. Newly identified hazards shall be documented in additional hazard reports.

The following data are required from the CO for phase II review:

1) Updated system description (including subsystems) and mission scenario.
2) Updated descriptions of safety-critical subsystems and their operations, including schematics and block diagrams with safety features and inhibits identified. Provide electrical schematics that clearly identify the required number of independent inhibits, controls, and monitoring provisions. Present a summary of the test and analytical efforts required to verify the intended performance of all safety-critical hardware. For a computer-based control system that is used to prevent critical or catastrophic hazards, provide the following data/descriptions: (a) functional architecture; (b) expected interactions; (c) results of unexpected interactions; (d) protections for common cause failures; (e) development process for databases, hardware, software, and hardware/software.
3) Updated and additional (if any) flight hazard reports.
4) Update of the FDS implementation approach. Include information on use of forced air flow, wire derating, circuit protection, materials usage, parameter monitoring (fan speeds, temperatures, current, etc.) and responses to an out-of-limit condition, and suppression approach.
5) Verification methods associated with hazard controls that require in-flight verification and/or reverification and the applicable approach (include rationale, constraints, and detailed methodology).
6) An updated tabulated list of planned toxic materials and support data.
7) Updated list of all battery types, their uses, manufacturer, and applications.
8) List of all pyrotechnic devices, their functions, chemical composition, critical components inspection plan, verification plan, and aging degradation evaluation plan.
9) List of hazard controls that require crew procedures and/or training.
10) A record of test failures, anomalies, and accidents involving qualification or flight hardware. Include a safety assessment for items which may affect safety.
11) The status of all action items assigned to the CO during phase I.
12) Detailed in-flight maintenance safety assessment.
13) Status of all action items assigned to the CO during phase I.

The CO shall prepare the phase II hazard reports by revising the phase I hazard reports to reflect the completed system design and operational procedures. If the system design changes from phase I to phase II so that a phase I hazard report may be deleted, present a brief statement of rationale for deleting the report in the phase II SDP.

Address all critical procedures/processes, including the plan for verification. Verifications shall refer to specific test (or analysis) procedures and summarize pass/fail criteria to be used. Specify the schedule for the completion of each specific verification test, analysis, or inspection.

C-2.4 Phase III Safety Review

The purpose of the phase III safety review is to obtain SSI SRP approval of Hazard Reports and safety compliance data that reflects the safety verification findings. The focus of this review is to assess safety verification testing and analysis results. If verifications critical for establishing the acceptability of the fundamental design of the system for safety are not completed prior to the phase III review, then subsequent reviews may be required prior to hazard report approval. All verifications that are open at the time of the phase III SDP submittal must be included in a dedicated tracking data base.

The following data are required for the phase III SDP:

1) Final as-built system description (including subsystems) and mission scenario.
2) Updated descriptions that define the final configuration of the safety-critical subsystems and their operations, including schematics and block diagrams with the as-built system safety features and independent inhibits, controls, and monitoring provisions identified. Address applicable features and constraints relating to in-flight verification/reverification of hazard controls. For a computer-based control system that is used to prevent critical/catastrophic hazards, provide verifications for the following: (a) functional architecture; (b) expected interactions; (c) results of unexpected interactions; (d) protections for common cause failures; (e) flight article databases, hardware, software, and hardware/software operate as designed.
3) Updated and additional (if any) flight hazard reports, including support data that reflect the final configuration of the as-built system and planned use. For systems that have catastrophic hazard potential, document the verification program.
4) Final summary list and explanation of launcher or carrier-provided critical services.
5) Finalized FDS implementation approach. Include information on use of forced air flow, wire derating, circuit protection, materials usage, parameter monitoring (fan speeds, temperatures, current, etc.) and responses to an out-of-limit condition.

6) Updated (and additional, if required) verification methods associated with hazard controls that require in-flight verification and/or reverification and the applicable approach (include rationale, constraints, and detailed methodology).
7) Final tabulated list of toxic materials and support data.
8) Final list of all battery types, their uses, manufacturer, and applications.
9) Final list of all pyrotechnic devices installed or to be installed on the system. The list will identify for each cartridge the function to be performed, the part number, the lot number, and the serial number.
10) Updated list of hazard controls that require crew procedures and/or training.
11) An updated record of test failures, anomalies, and accidents involving qualification or flight hardware or baselined flight software if the software is used for hazard control. Include a safety assessment for items which may affect safety.
12) Status of all action items assigned to the CO through phase II.
13) Identification of flight safety non-compliances (NCRs). Safety NCRs must be approved as either a waiver or a deviation before the phase III safety review can be completed. A signed copy of each approved safety waiver and/or deviation shall be included in the phase III SDP attached to the appropriate hazard report.
15) Final/updated in-flight maintenance safety assessment.

If the system design is changed from phase II to phase III, so that a phase II hazard report may be deleted, provide in the phase III SDP a brief statement of rationale for deleting the report.

Verifications completed by phase III shall be indicated as such on the hazard report. This information shall summarize the results of the completed tests, analyses, and/or inspections and refer to particular test reports by document number, title, and date. Open verification moved to the tracking data base.

C-2.5 Schedule of Safety Reviews

The schedule of formal phase 0, I, and II system safety reviews generally relates to the system development schedule. Phase 0 is held during the concept phase or at the start of system design. Phase I is near the Preliminary Design Review (PDR); phase II is near the Critical Design Review (CDR). Scheduling of safety reviews immediately before or after a project design reviews depends on the CO confidence on the outcome of those reviews. For example, if there are doubts about the approval by the SRP of hazard controls to be presented at phase I, it would be wise to schedule the safety review before the PDR. The CO should set the review schedule to obtain maximum benefit to system development based on the results of the safety reviews. Phase III is associated with completion of system safety verifications and/or the start of ground processing at the spaceport. When establishing a timeline for phase III, the CO should allow enough time to close potential issues that may result from the phase III review. The timing and completion of the phase III review and safety certification are critical to the launch schedule.

C-2.6 Safety Review Completion Criteria

C-2.6.1 Documentation of Phase Completion

During a formal meeting, the SSI SRP Chairman will make an official announcement that the safety phase is complete or incomplete (open). This announcement will be recorded and distributed by the SSI SRP in the official meeting minutes. Incomplete phases are usually attributable to overdue/open action items or unsigned (open) hazard reports. The SSI SRP will issue official correspondence to document closure of open action items/signature of open hazard reports that occurs after the phase review. The correspondence that closes the last open action item/hazard report for that phase will include a statement that the safety phase is considered complete.

C-2.6.2 Completion Criteria for Phase I, II, and III

Successful completion of phase I and II reviews is accomplished by obtaining approval (Panel Chairman's signature) of hazard reports at the appropriate phase level and closure of applicable phase I/II action items.

After submission of all required data, the criteria for successful completion of the safety review process at the phase III level are as follows:

a) All system hazard reports are signed by the CO Program Manager and the SSI SRP Chairman at the phase III level.
b) All Non-compliance Reports (NCRs) are approved.
c) Safety review action items are formally closed in the safety review meeting minutes or documented closed in separate correspondence.

Approval of the phase III safety data by the SSI SRP is with the understanding that the data represent the actual design and operations of the system. Should safety issues arise after the safety process is complete, the safety panel reserve the right to request additional data deemed necessary to reassess the system.

C-2.7 Post Phase III Safety Activity

C-2.7.1 Configuration Control

When changes to the design, configuration, or operations of the system are required subsequent to phase III safety review, the CO shall assess those changes for possible safety implications, including the effect on all interfaces. The assessment shall be forwarded to the SSI SRP for review and approval. New or revised hazard reports and support data shall be prepared where applicable and submitted for approval. The need for delta phase III safety reviews will be determined by the SSI SRP Chairman. Satisfactory completion of these activities is mandatory prior to the start of affected ground activities or launch.

Any test failures, anomalies, or accidents involving system flight hardware or software that occurs between the completion of phase III and launch must be promptly reported to the SSI SRP. Safety impacts, if any, should be identified.

C-2.4.2 Documentation of Safety Process Completion

Final flight safety approval is documented by the SSI SRP Chairman's signature on the Certificate of Flight Readiness (CoFR) for the planned flight.

C-3 SUPPORTING TECHNICAL DATA

This section addresses SDP data submittals related to various technical disciplines to support hazard reports, required by the SSI SRP for either Design for Minimum Risk or Failure Tolerant design. This supporting data shall be submitted in one of the following manners: (a) attached to the hazard report, (b) as part of the SDP, or c) submitted separately to the SSI SRP Executive Secretary.

C-3.1 Structures

C-3.1.1 Phase I

a) Proposed Structural Verification Plan.
b) Propose Fracture Control Plan.
c) Methodology for assurance of fastener integrity.

C-3.1.2 Phase II

a) Final Structural Verification Plan, including: (1) summary of design loads derivation leading to critical load cases, and (2) math model verification plan.
b) Fracture control status (including parts categorization).
c) Identification of Material Usage Agreements (MUAs) on structural materials, the failure of which would cause a hazard (including, but not limited to, stress corrosion, hydrogen embrittlement, and materials compatibility).

C-3.1.3 Phase III

a) Summary of verification tests/analyses/inspections results.
b) Fracture control summary report.
c) Approved MUAs.
d) Documentation of compliance with fastener integrity program.

C-3.2 Pressurized Systems

C-3.2.1 Phase I

a) Preliminary pressurized system (vessels, lines, fittings, components) schematic and operating parameters (e.g., temperature, pressure and other environmental conditions).
b) Preliminary summary of the derivation of system MDP(s).
c) Preliminary list of all system working fluids, their complete chemical composition, amounts, potential hazards (e.g., flammability, explosion, corrosion, toxicity) and hazard category (e.g., catastrophic, critical, non-hazard).
d) Summary of pressure vessel(s) design and qualification approach.
e) Damage control plan and stress rupture life assessment (COPVs only).
f) Fracture control plan.
g) Proposed pressurized system(s) verification approach for controls to ensure pressure integrity.
h) For fluids whose leakage is hazardous also include:
i) Proposed pressurized system(s) verification approach including controls to prevent leakage (e.g., levels of containment, DFMR). For the DFMR approach to protect against leakage that may cause a catastrophic hazard include: (1) identification of mechanical fitting and leakage certification approach for wetted areas. Consider all environments where leakage is hazardous, (2) preliminary identification of fusion and bi-metallic joints within the system.

C-3.2.2 Phase II

a) Complete and updated pressurized system schematic(s) and operating parameters, addressing all pressurized hardware.
b) Complete summary of the derivation of system MDP(s) Complete table of pressurized system hardware, MDP(s), proof pressure, ultimate pressure, resulting proof and ultimate safety factors and method of determining the safety factors (e.g., test, analysis, vendor data).
c) Updated list of all system working fluids, their complete chemical composition, amounts, identified hazards and hazard category.
d) Status on pressure vessel(s) design and qualification.
e) Fracture control status.
f) Identification of MUAs on pressurized system materials the failure of which would cause a hazard (including, but not limited to, stress corrosion, hydrogen embrittlement, and materials compatibility [including working and cleaning fluids]).
g) Final pressurized system(s) verification approach for controls to ensure pressure integrity including a summary of qualification and acceptance test plans and analyses.
h) For fluids whose leakage is hazardous also include: final pressurized system(s) verification approach including controls to prevent leakage (e.g., levels of containment, DFMR). Include a summary of qualification and acceptance test plans and analyses. For the DFMR approach to protect against leakage that may cause a catastrophic hazard include: (1) summary of certification test plans and analyses to prevent leakage of wetted mechanical fittings, (2) identification of system fusion joints and their method of NDE. Identification of system bi-metallic joint(s), manufacturer and certification data, and (3) complete list of wetted materials and their compatibility rating with system and cleaning fluids. Define credible single barrier failures which may release fluid into a volume that is not normally wetted and provide a summary of maximum worst case temperatures which were considered.

C-3.2.3 Phase III

a) Final pressurized system schematic(s) and operating parameters, addressing all pressurized hardware.
b) Final MDP derivation summary and table of pressurized system hardware.
c) Final list of all system working fluids, their complete chemical composition, amounts, hazards and categories.
d) Certification of pressure vessel(s) design, including qualification and acceptance test results.
e) Fracture control summary report.
f) Approved MUAs.
g) For safe-life and limited-life pressure vessels, document existence of a Pressure Log, including log number.
h) Summary of results from verification tests/analyses/inspections for controls to ensure pressure integrity.
i) For fluids whose leakage is hazardous also include: summary of results from verification tests/analyses/ inspections/demonstrations for controls to prevent leakage. For the DFMR approach to protect against leakage that may cause a catastrophic hazard include: (1) summary of results from certification tests and analyses on wetted mechanical fittings, (2) final list of system fusion joints and results from NDE. Final list of system bi-metallic joint(s), manufacturer(s) and certification data, (3) final list of wetted materials and their compatibility rating with system and cleaning fluids.

C-3.3 PYROTECHNIC DEVICES

C-3.3.1 Phase I

List of pyrotechnic devices and the functions performed.

C-3.3.2 Phase II

a) Detailed drawings of devices.
b) Chemical composition of any booster charge(s).
c) Inspection plan(s) for critical components.
d) Plan for evaluation of aging degradation.
e) Verification plan summary, including acceptance and qualification approach(s) (including margin demonstration).

C-3.2.2.3 Phase III

Summary of verification tests/analyses/inspections/demonstrations results.

C-3.4 MATERIAL FLAMMABILITY, TOXICITY, AND COMPATIBILITY

C-3.4.1 Phase I

a) Approach used to assure materials compatibility.
b) Tabulated list of tentative toxic materials and support data.

C-3.4.2 Phase II

a) Materials compatibility status.
b) Toxicological evaluation of test sample materials.
c) Offgassing test plan.
d) Preliminary flammability assessment.

C-3.4.3 Phase III

a) Final materials compatibility status.
b) Update to toxicological evaluation of test sample materials.
c) Flammability Assessment including a summary of flame propagation controls.
d) Offgassing test summary.

C-3.5 IONIZING RADIATION

C-3.5.1 Phase I

Ionizing Radiation Source Data Sheet.

C-3.5.2 Phase II

Updated Ionizing Radiation Source Data Sheet.

C-3.5.3 Phase III

Approved Ionizing Radiation Data Sheet.

C-3.6 NON-IONIZING RADIATION

C-3.6.1 Phase I

List of equipment that generates non-ionizing radiation (Radio Frequency (RF), light sources, lasers, etc.).

C-3.6.2 Phase II

Updated list of equipment that generates non-ionizing radiation, including expected nominal operational characteristics of all non-ionizing radiation sources.

C-3.6.3 Phase III

Final list of equipment that generates non-ionizing radiation, including actual nominal operational characteristics of all non-ionizing radiation sources.

C-3.7 SYSTEM COMMANDING

C-3.7.1 Phase I

List of hazardous commands and implementation.

C-3.7.2 Phase II

Updated list of hazardous commands and detailed implementation plan.

C-3.7.3 Phase III

Verification of implementation plan.

C-3.8 ELECTRICAL/ELECTRONIC SUBSYSTEMS

C-3.8.1 Phase I

a) Preliminary power distribution schematic(s) showing wire sizing and circuit protection.
b) Preliminary bonding and grounding diagram/plan.
c) Preliminary diagram of safety-critical subsystems, that indicate inhibits, controls, and monitors.
d) Preliminary verification approach for electrical safety-critical subsystems.
e) Identify any usage of launcher or carrier electrical service to control a hazard.

C-3.8.2 Phase II

a) Updated power distribution schematic(s) showing wire sizing and circuit protection.
b) Final bonding and grounding diagram.
c) Updated schematics of safety-critical subsystems that indicate inhibits, controls, monitors, and orbiter interfaces.
d) Verification approach (test pass/fail criteria) for each hazard control/monitor performed by avionics.

C-3.8.3 Phase III

a) As-built power distribution schematic(s) that show wire sizing and circuit protection.
b) Summary of verification tests/analyses/inspection results for bonding and grounding.
c) As-built schematics of safety-critical subsystems that indicate inhibits, controls, monitors, and launcher or carrier interfaces.
d) Summary of test results and summary of test procedures, including system organization testing and/or fully integrated testing.

C-3.9 COMPUTER SYSTEMS

This section applies only to system computer systems used to control hazardous functions (when they implement more than one control).

C-3.9.1 Phase I

a) Identify computer system hazard controls.
b) Describe the function(s) controlled by computer systems that prevent a hazard from occurring or control a hazardous function.
c) Describe the development process (including verification) of software/hardware and computer-based control.

C-3.9.2 Phase II

a) Describe the independence of computer and non-computer methods of hazard control.
b) Update the description of computer system hazard controls, and the function(s) controlled by computer systems that prevent a hazard from occurring or control a hazardous function.
c) Summarize the functional testing of the software/hardware and describe the verification approach for the computer-based hazard control system.

C-3.2.9.3 Phase III

Provide a summary of results of computer-based hazard control verification activity, including summaries of any failures/errors of the baselined flight software used for hazard control.

C-3.10 MECHANISMS IN CRITICAL APPLICATIONS

C-3.10.1 Phase I

a) Identification of safety-critical mechanisms.
b) Identification of areas of applicability of holding or operating force or torque margin requirements and planned verification approach (test or analysis).
c) Fracture control plan.

C-3.10.2 Phase II

a) Verification approach for each safety-critical mechanism, including qualification and acceptance tests and analyses.
b) List of MIPs.
c) Fracture control status (including parts categorization).

C-3.10.3 Phase III

a) Report of verification tests/analyses/inspection results.
b) Fracture control summary report.
c) Report of verification tests/analyses/inspection results.
d) Fracture control summary report.

C-3.11 SOLID ROCKET MOTORS

C-3.11.1 Phase I

a) Preliminary schematic showing electrical inhibits, controls and monitoring provisions to prevent premature firing.
b) Preliminary characteristics of the solid rocket motor.

C-3.11.2 Phase II

a) Updated schematic showing electrical inhibits, controls, and monitoring provisions to prevent premature firing, including power sources, inhibit control command sources and static control devices. Independence of inhibits shall be clearly depicted.
b) Updated characteristics of SRM, including motor manufacturer, total mass and type of propellant, propellant formulation/ingredients, motor/propellant explosive classification, and case description.
c) Cutaway diagram of the initiator.
d) Diagram of the safe-and-arm device, indicating design and operation.

C-3.11.3 Phase III

a) Final schematic showing electrical inhibits, controls, and monitoring provisions to prevent premature firing, including power sources, inhibit control command sources, and static control devices. Independence of inhibits shall be clearly depicted.
b) Final characteristics of SRM, including motor manufacturer, total mass and type of propellant, propellant formulation/ingredients, motor/propellant explosive classification and case description.
c) A table listing the inhibits, when last cycled (actuated), and the final pre-launch state.
d) Final cutaway diagram of the initiator.
e) Updated diagram of the safe-and-arm device, indicating design and operation.

C-3.12 BATTERIES

C-3.12.1 Phase I

a) Preliminary list of type and number of battery cells, cell size (capacity), cell chemistry, cell manufacturer, and model number.
b) State whether in-flight battery charging is intended.

C-3.12.2 Phase II

a) Updated list of type and number of battery cells, cell size (capacity), cell chemistry, cell manufacturer, and model number.
b) Circuit diagram including charging circuit.
c) Charging characteristics and procedures, e.g., pulse charging, charge rate, trickle charge rate, and method of charge termination.
d) Drawings for battery boxes that indicates materials of construction, absorbent material, venting provisions, minimization of hydrogen accumulation from aqueous electrolyte batteries, protective coatings on battery box interiors and on exposed cell terminals, and cell physical retention techniques.
e) Verification plan, including qualification and acceptance tests.
f) Diagram of charging devices, characteristics, and implementation procedures.
g) Fracture control approach for battery cells where leakage causes a catastrophic hazard and for nickel-hydrogen batteries.

C-3.12.3 Phase III

a) Final list of type and number of battery cells, cell size (capacity), cell chemistry, cell manufacturer, and model number.
b) Final circuit diagrams, including charging circuit.
c) Final charging characteristics and procedures.
d) As-built drawings for battery boxes that indicates materials of construction, absorbent material, venting provisions, minimization of hydrogen accumulation from aqueous electrolyte batteries, protective coatings on battery box interior and on exCOsed cell terminals, and cell physical retention techniques.
e) Results of verification tests, analyses, and inspections.
f) Fracture control summary.

C-3.13 FLUID PROPULSION SYSTEMS

C-3.13.1 Phase I

a) Preliminary propulsion system schematic(s) and operating parameters (e.g., temperature, pressure, other environmental conditions, number of thrusters).
b) Preliminary summary of the derivation of system MDP(s).
c) Preliminary list of all system working fluids, their complete chemical composition, amounts, potential hazards (e.g., flammability, explosion, corrosion, toxicity) and hazard category (e.g., catastrophic, critical, non-hazard).
d) Summary of pressure vessel(s) design and qualification approach.
e) Fracture control plan.
f) Safe distance assessment and planned thrust level(s) used to determine it.
g) Preliminary schematic(s) showing flow control devices, their electrical inhibits and monitoring provisions to prevent premature firing. Proposed verification approach for controls to prevent premature firing.
h) Proposed propulsion system(s) verification approach for controls to ensure pressure integrity.

i) For fluids whose leakage is hazardous also include proposed propulsion system(s) verification approach including controls to prevent leakage.
j) To protect against leakage that may cause a catastrophic hazard include: (1) identification of mechanical fitting and leakage certification approach for wetted areas. Consider all environments where leakage is hazardous, (2) preliminary identification of fusion and bi-metallic joints within the system.

C-3.13.2 Phase II

a) Complete and updated propulsion system schematic(s) and operating parameters, addressing all pressurized hardware.
b) Complete summary of the derivation of system MDP(s). Complete table of propulsion system hardware, MDP(s), proof pressure, ultimate pressure, resulting proof and ultimate safety factors, and method of determining the safety factors (e.g., test, analysis, vendor data).
c) Updated list of all system working fluids, their complete chemical composition, amounts, identified hazards, and hazard category.
d) Status on pressure vessel(s) design and qualification.
e) Fracture control status.
f) Identification of MUAs on propulsion system materials the failure of which would cause a hazard (including, but not limited to, stress corrosion, hydrogen embrittlement, and materials compatibility [including working and cleaning fluids]).
g) Updated safe distance assessment and planned thrust level(s) used to determine it.
h) Updated schematic(s) showing flow control devices, and their electrical inhibits and monitoring provisions to prevent premature firing. Independence of inhibits shall be clearly depicted. Provide cut-away diagrams of the flow control devices. Final verification approach for controls to prevent premature firing.
i) Final propulsion system(s) verification approach for controls to ensure pressure integrity, including a summary of qualification and acceptance test plans and analyses.
j) For fluids whose leakage is hazardous also include: final propulsion system(s) verification approach, including controls to prevent leakage. Include a summary of qualification and acceptance test plans and analyses. To protect against leakage that may cause a catastrophic hazard, include: (1) summary of certification test plans and analyses to prevent leakage of wetted mechanical fittings, (2) identification of system fusion joints and their method of NDE. Identification of system bi-metallic joint(s), manufacturer, and certification data, (3) complete list of wetted materials and their compatibility rating with system and cleaning fluids. Define credible single barrier failures which may release fluid into a volume that is not normally wetted and provide a summary of maximum worst case temperatures considered.

C-3.13.3 Phase III

a) Final propulsion system schematic(s) and operating parameters, addressing all pressurized hardware.
b) Final MDP derivation summary and table of propulsion system hardware.
c) Final list of all system working fluids, their complete chemical composition, amounts, hazards, and categories.
d) Certification of pressure vessel(s) design, including qualification and acceptance test results.
e) Fracture control summary report.
f) Approved MUAs as defined.
g) For safe-life and limited-life pressure vessels, document existence of a Pressure Log, including log number.
h) Final safe distance assessment.
i) Final schematic(s) showing flow control devices, and their electrical inhibits and monitoring provisions to prevent premature firing. Summary of results from verification tests/analyses/inspections for controls to prevent premature firing.
j) Summary of results from verification tests/analyses/inspections for controls to ensure pressure integrity.
k) For fluids whose leakage is hazardous also include summary of results from verification tests/analyses/inspections for controls to prevent leakage. To protect against leakage that may cause a catastrophic hazard, include: (1) summary of results from certification tests and analyses on wetted mechanical fittings, (2) final list of system fusion joints and results from NDE. Final list of system bi-metallic joint(s), manufacturer(s), and certification data, (3) final list of wetted materials and their compatibility rating with system and cleaning fluids.

C-3.14 SEALED CONTAINERS (STRUCTURES)

C-3.14.1 Phase I

a) List the name of each sealed container.
b) Provide preliminary identification of MDP, fluid(s), materials of construction for container enclosure, stored energy due to pressure, and environmental conditions.
c) Confirm/show sealed container meets design requirements. NASA-STD-5019A.

C-3.14.2 Phase II

a) List the name of each sealed container and verify that information furnished at Phase I is still valid. If not, identify and explain changes.
b) Provide preliminary summary of analyses and tests for each sealed container as required by pressure ratings and verification methods.

C-3.14.3 Phase III

a) List the name of each sealed container and verify that information furnished at Phase II is still valid. If not, identify and explain changes.
b) Provide final identification of MDP, fluid(s), materials of construction for container enclosure, stored energy due to pressure, and environmental conditions.
c) Provide final acceptance rationale for each sealed container including a summary of any required analyses and tests.

C-3.15 SENSITIVE DATA

C-3.15.1 Submittal of Proprietary Data

If proprietary data are submitted in the SDP, the transmittal letter must include the following statement: *This system safety data package contains proprietary data on the following pages: [list the appropriate page numbers]. [Insert name of the CO] acknowledges awareness and acceptance of the SSI policies and methods of processing proprietary data. [Insert name of the CO] also will provide any additional protective measures it deems necessary over and above that provided by the panels during meetings.*

The transmittal letter and the first page of the SDP must identify the specific pages that contain proprietary information. Insert the word “PROPRIETARY” at the top and bottom of each page that contains proprietary data.

In addition to the proper submittal of proprietary information, the CO should be aware of the following while attending SSI safety reviews, technical interchange meetings (TIMs), and action item closure meetings:

1) SSI SRP meetings are not conducted in secure facilities. Thus, when it is necessary to recess meetings (e.g., lunch and breaks), the COs will be responsible for protecting any proprietary data distributed during the meeting (other than that logged and distributed by SSI as part of the SDP).
2) If any proprietary data are to be presented or discussed during the meeting, prior to the meeting the CO will notify the SSI SRP Executive Secretary who will then make arrangements to monitor attendance, close the doors, and post a sign noting that access to the meeting is controlled.
3) The CO will be responsible for retrieval and disposition of any proprietary material distributed at the meeting (other than that logged and distributed by SSI as part of the SDP), with the exception that two copies of proprietary material distributed by the CO at the meeting will be retained by the SSI SRP in a protected file.

When the SSI SRP receives proprietary data included in the SDPs, such data will be handled in a manner that will protect the interests of the CO. These procedures include tracking distributed materials, protecting files, and restricting reproduction. In order to exercise reasonable care in protecting proprietary data in connection with the system safety review process, the SSI will ensure that proprietary data are distributed only to persons who have a need to review such data in support of panel functions. Furthermore, distributed data that is returned to the SSI SRP Executive Secretary after use will be destroyed via the SSI secure disposal process.

C-3.15.2 Submittal of Copyrighted Data

System documentation submitted to SSI is reproduced and distributed to the members of the SSI SRP and to associated technical support personnel. Accordingly, copyrighted data shall not be included in the submitted documentation unless the CO: (1) identifies such copyrighted data, and (2) grants to the SSI, or acquires on behalf of the SSI, a license to reproduce and distribute the data to these necessary recipients.

C-3.15.3 Submittal of Export Control Data

Export control data submittal requirements apply to U.S. COs only. Non-U.S. COs are not required to provide the U.S. export control classification of their safety data packages. In the event that a non-U.S. SDP requires a U.S. export control classification, SSI export control resources will be used to classify the SDP.

C-4 SYSTEM SAFETY NONCOMPLIANCES

The CO shall document each noncompliance with the technical safety requirements of this standard. The CO must develop the acceptance rationale that explains the design features and/or procedures used to conclude that the noncompliant condition is safe.

Approval of an NCR for the design or operation of one element, subsystem, or component of the system will not relieve the CO of the responsibility to meet the requirement in any other element, subsystem, or component of the system.

C-4.1 Safety NCR Submittal and Processing

a) The CO should submit the NCR as soon as it is determined that the safety requirement cannot be met.
b) All NCRs should be coordinated with the SSI SRP prior to submittal.
c) The NCR must be approved before the SSI SRP will approve the associated hazard report(s).
d) The SSI SRP will ensure that the NCR is processed through the appropriate Safety Authority.

C-4.2 Types of Safety NCRs

Non-compliance Reports NCRs will be approved as either waivers or deviations. The SSI SRP will determine the type of NCR.

C-4.2.1 Waivers

Waivers are granted for noncompliant conditions that do not meet specific requirements. Waivers have an effectivity of one flight only. The CO has the responsibility to correct the noncompliant condition prior to re-flight of the same system or system element, or prior to the flight of subsequent systems of the same series. The CO shall state the desired effectivity on the NCR form. After expiration of the waiver's effectivity and prior to re-flight of the same system or system element, or prior to the flight of subsequent systems of the same series, the CO has the responsibility to correct the noncompliant condition.

C-4.2.2 Deviations

Deviations are granted for noncompliant conditions that do not meet specific requirements in the exact manner specified; however, the system design, procedure, or configuration satisfies the intent of the requirement by achieving a comparable or higher degree of safety. Deviations may be approved for unlimited use. The effectivity is the applicable flight number or increment number and subsequent flight or increment numbers.