IAASS-ISSB-S-1700-Rev-B March 2010

ISSB

INDEPENDENT SPACE SAFETY BOARD

SPACE SAFETY STANDARD

COMMERCIAL HUMAN-RATED SYSTEM

IAASS-ISSB
16580 Saturn Lane, Suite 100
Houston, TX 77058
USA

PREFACE

DATE: August, 2006

On December 23, 2004, President Bush signed into law the Commercial Space Launch amendments Act of 2004 (CSLAA). The CSLAA promotes the development of the emerging commercial space flight industry and makes the Department of Transportation and the Federal Aviation Administration (DOT/FAA) responsible for regulating commercial human space flight under 49 U.S.C. Subtitle IX, Chapter 701 (Chapter 701). The CSLAA requires that before receiving compensation from a space flight participant or making an agreement to fly a space flight participant, an RLV (Reusable Launch Vehicle) operator inform the space flight participant in writing that the U.S. Government has not certified the launch vehicle as safe for carrying crew or space flight participants. 49 U.S.C. § 70105(b)(5)(B). In addition, the RLV operator should have a placard displayed in the launch vehicle in full view of all space flight participants to warn that the launch vehicle does not meet aircraft certification standards.

The IAASS consider that the average space flight participant will not have the necessary background and technical experience to truly grasp the risk of space flight. Therefore the written consent required by law may end as a merely bureaucratic process. On the other hand the lack of an independent safety certification may be deter the participation of at least part of potential customers. Furthermore, due to the fact that the current CSLAA regime does not relieve the RLV operator of any responsibility for gross negligence, obtaining an independent safety certification is very much in the interest of the RLV operator in case of future litigations.

The FAA guidelines for *Commercial Suborbital Reusable Launch Vehicle Operations with Space Flight Participants* issued in February 2005, provide details about the overall process of written informed consent. It requires that an RLV operator should describe to each space flight participant the safety record of all launch or re-entry vehicles that have carried one or more persons on board, including both U.S. government and private sector vehicles. The safety record should not be limited to only the vehicles of a particular RLV operator. An RLV operator should also describe the safety record of its vehicle to each space flight participant. The RLV operator's safety record should include vehicle ground-test and flight-test information. This information should describe all safety-related anomalies or failures that occurred and corrective actions taken to resolve the anomalies or failures. The FAA guidelines consider that the development of commercial launch vehicles to carry space flight participants is in the embryonic or early stages. Consequently, newly developed launch vehicles will not have the extensive flight-test history or operational experience that exists for commercial airplanes. Because of the lack of flight-test and operational experience, the risks of the RLV operator's particular launch vehicle and of vehicles like it, including both government and private sector vehicles, should be disclosed. The US House Committee on Science report, H. Rep. 108-429, clarifies that Congress intended that all government and private sector vehicles to be included in this description. Because most human space flight to date has taken place under government auspices, the government safety record provides the most data. The RLV operator should provide a

record of all vehicles that have carried a person because they are the most relevant to what the RLV operators propose. Regardless of whether humans travelled to space on board a vehicle destined for a suborbital or orbital mission, those persons travelled on vehicles based on technology as new then as what may be developed now. It was therefore as risky. Likewise, because it was intended for a human on board, greater care was likely to have been taken in its design and construction. The same should be expected for commercial human space flight. Furthermore the RLV operator is required to provide space flight participants an opportunity to ask questions orally to acquire a better understanding of the hazards and risks of the mission.

The requirements in this document have been established on the basis of the safety experience accumulated in human spaceflight to date. By demonstrating design compliance with these requirements, the commercial human spaceflight operator will show to have taken into due consideration past experiences and best practices for the sake of making his spacecraft design and operations safe.

The International Association for the Advancement of Space Safety (IAASS) has established an Independent Space Safety Board (ISSB) to provide flight safety certification services to the emerging commercial human space industry on the basis of this document requirements. The ISSB is located in Houston (TX), and is composed by a multidisciplinary team of space safety experts.

TABLE OF CONTENTS

CHAPTER 1: GENERAL

CHAPTER 2: TECHNICAL REQUIREMENTS

CHAPTER 4: CERTIFICATION REQUIREMENTS

CHAPTER 1: GENERAL

100 PURPOSE

This document establishes the safety requirements applicable to the IAASS Certification of Commercial Human Rated Systems (CHS). This standard covers any human-rated system commercially developed and operated to perform sub-orbital or orbital flights, including transport vehicles such as capsules or winged bodies, commercial orbital stations, unmanned cargo transport vehicles intended to dock with a crewed station, and integrated systems (e.g.: capsule on launcher).

101 SCOPE

These requirements are intended to protect the flight personnel (i.e., crew and flight participants), ground personnel, the vehicle and relevant launcher or carrier, and any other interfacing system from CHS-related hazards. This document contains technical and system safety requirements applicable to CHS during ground and flight operations.

These requirements are applicable to the vehicle and to the integrated system, the CHS, (i.e., vehicle on its Launcher or Carrier, and relevant interfaces with control centers, launch pad, recovery system, etc.) for all phases of flight, 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 expendable launchers or winged carriers used to transport a vehicle during part of its mission are outside the scope of this standard. Furthermore all issues related to public safety are outside the scope of this standard, in particular during launch, air-carried and re-entry phases.

Note (1) : In case of a vehicle which during part of its flight operates as an aircraft (powered and non), the relevant civil aviation requirements and certification authority should in principle apply. In other words a vehicle operating also as an aircraft should require two complementary certification as space vehicle and aircraft respectively (being only the former one addressed by this standard).

Note (2): Requirements in this document referring to CHS apply to the composite (e.g.: vehicle integrated or launcher or carrier) as well as to the vehicle element operating separately.

101.1 Ground Operations and GSE Design. For additional safety requirements which are unique to ground operations and for requirements on GSE design, the CHS Operator (CO) shall refer to applicable national safety and health regulations as well as to spaceport ground safety regulations.

102 RESPONSIBILITY

102.1 **CHS Operator**. It is the responsibility of the CHS Operator to assure the safety of its vehicle and to implement the requirements of this document.

102.2 **Launcher or Carrier Operator.** It is the responsibility of the Launcher or Carrier to interface with the national regulatory body (ies) to obtain the necessary licenses. It is also the responsibility of the Launcher or Carrier operator to assure that interaction between the vehicle and the Launcher or Carrier, and the integrated system does not create a hazard for the general public and ground personnel.

103 IMPLEMENTATION

This document identifies the safety policy and requirements which are to be implemented by the CHS Operator (CO). The implementation of safety requirements by the CO will be assessed by the IAASS-Independent Space Safety Board (ISSB) during the safety review process and must be consistent with hazard potential. The ISSB assessment of safety compliance will include a complete review of the safety assessment reports (paragraph 401) and may include audits and safety inspections of flight hardware. The detailed interpretations of these safety requirements will be by the ISSB, and will be determined on a case-by-case basis consistent with the CHS actual architecture and hazard potential. The following supplementary documents are meant to assist the CO in complying with the requirements of this document.

103.1 **Implementation Procedure.** IAASS-ISSB-13830, will be published to assist the CHS Operator in implementing the system safety requirements and to define further the safety analyses, data submittals, and safety assessment review meetings.

103.2 **Interpretations of Requirements.** IAASS-ISSB-18798 will be issued as a collection of interpretations of the requirements in this document relative to specific CHS detailed designs.

104 MISSION SAFETY RISK

104.1 **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 a carrier only monitors two of three inhibits to a catastrophic hazardous function such 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.

104.2 Orbital Flights

104.2.1 Safety Risk. The probability of a catastrophic event for the flight personnel (i.e., flight crew and participants) during the entire mission shall not exceed 1.10^{-3}.

104.2.2 Micrometeoroids and Orbital Debris Risk (M/OD). For orbiting vehicles, the probability that the exposure to meteoroid and debris environment will not lead to penetration of or spall detachment (from M/OD critical items) shall be higher than 0.9946 over the mission.

104.3 Sub-Orbital Flights.

104.3.1 Safety Risk. The probability of a catastrophic event for the flight personnel during the entire mission shall not exceed $1 \cdot 10^{-4}$.

105 GLOSSARY OF TERMS AND ACRONYMS

For definitions applicable to this document, see Appendix A.

106 APPLICABLE DOCUMENTS

The documents which are referenced in this document is in Appendix B.

107 FIGURES AND TABLES

Figures and Tables referred to in the text are contained in Appendix C.

CHAPTER 2: TECHNICAL REQUIREMENTS

200 GENERAL

The following requirements are applicable to a CHS as determined by the safety analysis performed by the CO. When a requirement which is identified as applicable by the safety analysis cannot be met, a noncompliance report shall be submitted to the ISSB in accordance with IAASS-ISSB-13830 for resolution.

200.1 **Design to Tolerate Failures.** Failure tolerance is the basic safety requirement that shall be used to control most CHS hazards. The CHS must tolerate a minimum number of credible failures 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 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. Failure of de-orbiting an unmanned cargo spacecraft used for servicing an on-orbit crewed vehicle shall also be considered a critical hazard.

200.1b **Catastrophic Hazards.** Catastrophic hazards shall be controlled such that no combination of two failures 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 tolerance are called "Design for Minimum Risk" 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 will be identified in IAASS-ISSB 13830.

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 fault tolerance 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 Compatibility**. The CHS shall be designed to effectively utilize human capabilities, controls hazards and manage safety risk associated with human spaceflight, and provides, to the maximum extent practical, the capability to safely recover from hazardous situations.

200.6 **Handling Qualities**. The vehicle shall have handling qualities rating of 1 or 2 on the Cooper-Harper Scale in Figure 1 (see Appendix C) for tasks that can result in loss of flight personnel or loss of vehicle.

200.7 **Flight Data Use Capability.** To facilitate anomaly resolution and mishap/ incident investigation, the vehicle shall 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**

200.8a **Safe Without Services.** The vehicle should be designed to maintain fault tolerance or safety margins consistent with the hazard potential without Launcher or Carrier flight services.

200.8b **Critical Launcher or Carrier Services.** When Launcher or Carrier services are to be utilized to control vehicle hazards, the integrated system shall meet the failure tolerance requirements of paragraph 200.1 and adequate redundancy of the Launcher or Carrier services must be negotiated. The CO shall provide a summary of the hazards being controlled by Launcher or Carrier services in the safety assessment report (see paragraph 401), 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 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 system function whose loss could result in a critical hazard shall be one fault tolerant, whenever the hazard potential exists. No single credible failure or operator error shall cause loss of that function.

201.1.2 **Functions Resulting in Catastrophic Hazards.**
A system function whose loss operation could result in a catastrophic hazard shall be two fault tolerant, whenever the hazard potential exists. No two credible failures, no two operator errors, or combination thereof shall cause loss of that function.

201.1.3 **Crewed Manual Flight Control.** The vehicle 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 vehicle 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 (e.g.: mission control) to perform functions that are required to keep the flight personnel alive.

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

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 (paragraph 201.2.3).

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 either near-real-time or real-time. Monitoring shall be available to the launch site when necessary to assure safe ground operations.

201.2.3(a) **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(b) **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.** The inhibits to a hazardous function may be controlled by a computer system used as a timer, provided the system meets all the requirements for independent inhibits.

201.3 **Failure Propagation.** The design shall preclude propagation of failures from the system to the interfacing systems and vice-versa.

201.3.1 **Isolate and Recover.** The system shall provide the capability to isolate and/or recover from faults identified during system development that would result in a catastrophic event.

201.3.2 **Inhibits / Barriers.** A power failure in the circuits of an inhibit (i.e., barrier or disabling device) shall not cause it to change state. A 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.

201.3.3 **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.

201.4 **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.

201.5 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.

201.5.1 Explosives and Pyrotechnics.

201.5.1.1 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 MIL-STD-1576.

201.5.1.2 Initiators. NASA Standard Initiators are the preferred initiators for all safety critical explosive pyrotechnic functions. MIL-STD-1576 qualification and acceptance test requirements, or equivalent, apply if other initiators are used.

201.5.2 Explosive / Pyrotechnic Operated Devices.

201.5.2.2 Debris Protection. Pyrotechnic devices that are to be operated in proximity of the Launcher, Carrier or another 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).

201.5.2.3 Must Function 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. The data required for ISSB review are specified in IAASS-ISSB 13830. 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.

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.

201.5.2.4 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.

201.5.2.5 Traceability. The CO shall maintain a list of all safety critical pyrotechnic initiators installed or to be installed on the system, giving the function to be performed, the part number, the lot number, and the serial number.

201.5.2.6 Shielding & 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 crewed vehicle.

201.5.2.7 Use of Safe and Arm (S&A) Devices. All solid propellant rocket motors shall be equipped with an S&A device that provides a mechanical interrupt in the pyrotechnic train immediately downstream of the initiator. The S&A device shall be designed and tested in accordance with provisions of MIL-STD-1576. 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 CHS; and the initiator shall meet the requirements of paragraph 201.5.1.2. The S&A shall be in the safe position during the launch or carry phase. There shall be a capability to resafe 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(b).

The S&A devices shall be designed and tested in accordance with the provisions of MIL-STD-1576. In determining compliance with paragraph 201.2.3(b), the S&A device in the "safe" position shall be counted as one of the required inhibits.

201.5.2.7a Safe and Arm Design. S&A devices shall be designed to meet the following requirements:

1. 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.).
2. The setting status report is representative of the real state, "armed" or "safe", and may be remote;
3. The "armed" or "safe" state is displayed by an indicator physically linked to the disabling device;
4. They may be remotely controlled, but manual disarming is always possible;
5. The assembly of the initiator is physically impossible if the device is not in "safe" position.

201.5.3 Propulsion Systems.

201.5.3.1 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 201.5.3.1(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).

201.5.3.1(a) Safe Distance Criteria. The hazard of engine firing close enough to inflict damage to the Launcher, Carrier or interfacing orbital system due to heat flux, contamination, and/or perturbation of the Launcher, Carrier, or interfacing orbital 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 (see Appendix C). For large thruster systems with greater than 10 pounds total thrust, the collision hazard with the Launcher, Carrier or Interfacing 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.

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

201.5.3.1(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 201.5.3.1(c) and 201.5.3.1(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.

201.5.3.1(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.

201.5.3.1(c) **Electrical Inhibits.** If the vehicle is closer to the Launcher, Carrier or interfacing orbital 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 201.5.3.1(b)(1), 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.

201.5.3.1(d) **Monitoring.** At least two of the three required independent electrical inhibits shall be monitored by the flight crew until final separation of the CHS system 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 and 201.2.3(a). One of the monitors shall be the electrical inhibit or mechanical position of the isolation valve. Monitoring will not be required if the CHS qualifies for the unpowered bus exception of paragraph 201.2.3(b).

If the isolation valve will be opened prior to the system 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.

201.5.3.2 **Adiabatic/Rapid Compression Detonation.** If the vehicle is attached to the Launcher, Carrier or interfacing orbital system, the inadvertent opening of isolation valves in a hydrazine (N2H4) 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 ISSB 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.

201.5.3.3 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-failure tolerant 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-6001) or on data furnished by the manufacturer and approved by the ISSB.

Propellant temperatures less than the material/fluid compatibility limit, but greater than 110 ^{O}C (200 degrees Fahrenheit) must be approved by the ISSB. The use of inhibits, cutoff devices, and/or crew safing actions may be used to make the system two failure tolerant to overheating. Monitoring of inhibits (paragraphs 201.2.3 and functions resulting in catastrophic hazards) or of propellant temperature will be required.

201.5.3.4 Propellant Leakage. A system shall be two failure tolerant 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 failure tolerant.

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.

201.5.3.5 Hazardous Impingement and venting. The vehicle attitude control shall be designed to prevent hazardous thrusters' impingement on the Launcher, Carrier or Interfacing Orbital 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 vehicle.

201.5.4 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.

201.5.5 Planned Deployment/Extension Functions.

201.5.5.1 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 CHS system 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.

201.5.6 RF Transmitters. Allowable levels of radiation from CHS shall be defined in the vehicle to Launcher or Carrier or other interfacing vehicles ICDs.

201.5.7 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 habitable volumes.

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

201.5.8 On-Orbit Rendezvous and docking.

201.5.8.1 Safe Trajectories. The trajectory of an active vehicle during rendezvous and proximity operations 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 stays 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 stays outside the keep-out sphere (KOS) for a minimum of 4 orbits;

c) during any retreat out of the Approach Ellipsoid, the vehicle shall maintains a positive relative range rate until it is outside the Approach Ellipsoid and thereafter it shall stays outside the Approach Ellipsoid for a minimum of 24 hours.

201.5.8.2 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 interfacing CHS system.

201.5.8.3 Collision Avoidance Maneuver. The active vehicle shall implement collision avoidance manoeuvre strategies in addition to safe free drift trajectories, as a mean to avoid collision with a passive CHS system in case of contingencies up to docking.

201.5.9 Hazardous Commands

201.5.9.1 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 CHS system flight and operations 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 201.5.

201.5.9.2 **Command Fault Tolerance Approach.** The computer system (CS) shall be designed such that no combination of two failures, or two operator actions, or one of each will cause a catastrophic hazardous event, or no single failure or operator action will cause a critical hazardous event.

201.5.9.2a **Catastrophic Loss of Capability Hazard.** Where loss of a capability could result in a catastrophic hazard, the computer system shall provide two independent and unique command messages to deactivate any function within a failure tolerant capability.

201.5.9.2b **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.

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

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

201.5.9.4a **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.

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

201.5.9.6 **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.

201.5.9.7 **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.

201.5.9.8 **Removal of Software Controlled Inhibits.** Command messages to change the state of inhibits shall be unique for each inhibit.

201.5.9.9 **Unique Command for Inhibit Removal.** A unique command message shall be required to enable the removal of inhibits.

201.5.9.10 **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.

201.5.9.11 **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 ISSB 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 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.

202.5 **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 hardlines, 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.

202.6 **Unassisted Emergency Egress.** The CHS system shall provide the capability for unassisted flight personnel emergency egress to a safe haven during Earth pre-launch activities.

203 ABORT, ESCAPE, NEUTRALISATION AND SAFE HAVEN

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 or 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 or spaceport 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 an abort when an impending catastrophic failure is detected.

203.4 **Abort Sequencing**. If a range safety destruct system is incorporated into the launcher design, the vehicle shall automatically initiate the Earth ascent abort sequence when range safety destruct commands are received onboard, with an adequate time delay prior to destruction of the launch vehicle to allow a successful abort.

203.5 **Neutralisation**. The Launcher shall be equipped with an on-board intervention system to ensure the protection of the population flown over while not penalising the safety of the flight personnel. The on-board intervention system can be triggered from the ground or by an on-board automated system.

203.5.1 **Controlled Neutralisation.** A radio-commanded order from the ground causes execution of the neutralisation function.

203.5.2 **Instantaneous Automatic Neutralisation.** An automatic on-board system can be used to trigger the neutralisation function, when a non nominal stage separation or a stage rupture occurs. This function can also be triggered by an on-board automated device, in the event of drift from the specified conditions.

203.5.3 **Delayed Automatic Neutralisation.** An on-board automatic system can be used to trigger the neutralisation function with a specified time lag to neutralise a stage after nominal separation, without generating any risk on the upper stages and crewed vehicle, and before impact on the ground, and ensuring the dispersal of remaining propellant.

203.5.4 **Inhibition Of On-board Receiver Equipment.** This equipment shall be inhibited when in the course of the mission the neutralisation function is not longer required.

203.5.5 **Timing for neutralisation.** The time selected for neutralisation shall be determined to allow successful flight abort while ensuring the safety of the population on ground.

203.6 **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.

203.7 **Crewed Overriding Automation/Control**. The vehicle 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 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 **Crashworthiness Capabilities.** The vehicle design shall 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 ISSB.

205.2.1 **Safe State.** The computer system (CS) shall safely arrive to a known safe state when:

1) initializing a function,
2) performing an orderly shut down of a function upon receipt of a termination command or detection of a termination condition
3) 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 vs. 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 **On-orbit 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 habitable vehicle. 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 vehicle habitable volume life support hardware. 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.

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

CHAPTER 3: VEHICLE SAFETY DESIGN REQUIREMENTS

301 STRUCTURES

301.1 **Structural Design.** The structural design shall provide ultimate factors of safety equal to or greater than 1.5 for all vehicle mission phases. This includes loads incurred during vehicle and Launcher or Carrier operations for all CHS configurations or while changing configuration. A Structural Verification Plan shall be submitted for ISSB review and approval. 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-5003. 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.** 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 MIL-HDBK-5G. For all applications of metals, material "A" allowable MIL-HDBK-5G shall be used. For non-metallic materials, material equivalent "A" allowables as defined in MIL-HDBK-5G 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-527/JSC 09604 and MSFC-STD-3029. Alloys with high resistance to SCC shall be used whenever possible and do not require ISSB 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-527/JSC 09604 must be attached to the applicable stress corrosion hazard report contained in the safety assessment report (see paragraph 401). 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 ISSB 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 and closure shall be documented in the verification log (see paragraph 406.2).

301.6 **Pressure Systems.** 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-fault tolerant from causing the pressure to exceed the MDP of the system. Pressure integrity shall be verified at system level.

301.6.1 **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. The MDP as defined in paragraph 301.6 shall be substituted for all references to maximum expected operating pressure (MEOP) in the pressure vessel standards. Data requirements for pressure vessels are listed in IAASS-ISB-13830.

301.6.1a **Metallic Pressure Vessels.** Metallic pressure vessels shall comply with the pressure vessel requirements of ANSI/AIAA S-080, as modified by subparagraphs (a), (b) and (c) below.

(a) Approach "B" of figure 2 is not acceptable.

(b) Non-destructive evaluation (NDE) of safe-life pressure vessels shall include inspection of welds after proof testing.

(c) A proof test of each flight pressure vessel to a minimum of 1.5 x MDP and a fatigue analysis showing a minimum of 10 design lifetimes may be used in lieu of testing a certification vessel to qualify a vessel design that in all other respects meets the requirements of this document and ANSI/AIAA S-080.

301.6.1b **Composite Overwrapped Pressure Vessels (COPVs).** COPVs shall meet the pressure vessel requirements in ANSI/AIAA S-081A. A damage control plan and stress rupture life assessment shall be developed for each COPV.

301.6.2 **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 301.6.1 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, 301.6.1 and 301.6.2 are met. The structural integrity for external load environments shall be demonstrated.

301.6.3 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.

301.7 **Pressure Hull.** The design of the habitable volume 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 Repressurization**

301.8.1 **Pressure differential tolerance.** 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.

302 MATERIALS

MSFC-HDBK-527/JSC 09604 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 ISSB review. The CHS material requirements for hazardous materials, flammability, and offgassing are as follows:

302.1 **Hazardous Materials.** Hazardous materials shall not be released or ejected near human systems (interfacing or in close proximity). The CO shall submit to the ISSB, independent toxicological assessments for all hazardous materials of the vehicle’s habitable volume.

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-6001 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-6001 at MDP and temperature. Manufacturer's compatibility data on hazardous fluids may be used to accept materials in this category if approved by the ISSB.

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 vehicle and other human systems (interfacing or in close proximity) 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 301.6.1 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 SSO 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-6001. Guidelines for the conduct of flammability assessments are provided in NSTS 22648. A flammability assessment shall be documented in accordance with IAASS-ISSB-13830.

302.5 **Habitable Areas.** Materials used in habitable areas shall be tested in accordance with NASA-STD-6001 in the worst case atmosphere (i.e., oxygen concentration). Fire propagation path considerations also apply.

302.6 **Outside Habitable Areas.** Materials used outside the vehicle shall be evaluated for flammability in an air environment at 14.7 psi. Propagation path considerations of NSTS 22684 apply for material usages of greater than 1 pound (0.454kg) and/or dimensions exceeding 12 inches (30.5cm)

302.7 **Material Outgassing.** Materials used in the design and construction of the vehicle 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).

302.7a **Material Offgassing in Habitable Volumes.** Usage of materials which produce toxic levels of offgassing products shall be avoided in habitable volumes. The vehicle design shall assure that the offgassing load to the crewed compartment will not exceed the spacecraft maximum allowable concentrations (SMAC's) of atmospheric contaminants at the time of ingress. Habitable volumes will be tested for offgassing characteristics according to NASA-STD-6001 and shall include measurement of the internal atmosphere of a full scale, flight configured CHS 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.

The items in such volumes (e.g., cargo, payloads) are required to be subjected to offgassing tests (black-box levels) for safety validation. Rigorous material control to insure that all selected materials have acceptable offgassing characteristics is a negotiable alternative to black-box level testing. The offgassing test shall be used for the black-box level offgassing test.

303 ELECTRICAL SYSTEMS

303.1 **General.**
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 habitable 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 faults shall not cause ignition of adjacent materials. 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.

Circuit protective devices shall be sized such that steady state currents in excess of the derated values for wires and cables in IAASS-ISSB 18798 are precluded. 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 in accordance with IAASS-ISSB 18798.

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.

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

303.3 **Electrical System.** Separate safing systems shall be used for nominal space system functions and for essential/emergency functions (e.g., the 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 **Lightning Protection.** Electrical circuits may be subjected to electromagnetic fields due to a lightning strike. 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.

303.4.1 **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.

303.5 **Electromagnetic Compatibility.** Electromagnetic compatibility between the various elements and electro-phyrotechnic devices shall be ensured.

303.6 **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 20793.

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 insure that crew members' dose rates from naturally occurring space

radiation are kept as low as reasonably achievable (ALARA). Exposure levels shall not exceed the limits defined in Figure 5.7.2.2.1-2 of NASA-STD-3000.

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 vehicle shall protect the flight personnel from exposure to RF non-ionizing radiation beyond the limits in the latest version of IEEE C95.1, “IEEE Standard for Safety Levels with Respect to Human Exposure to Radio-Frequency Electromagnetic Fields, 3 kHz to 300 GHz” standard for RF non-ionizing radiation exposure limits.

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 paragraph 305.1.

305.4 **Emissions and Susceptibility.** Vehicle’s emissions shall be limited to those levels identified in the ICDs with interfacing systems. Space systems with unintentional radiation level (EMI) above the levels identified in ICDs will be assessed for hazardous impact. Space systems 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 (2007).

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 ENVIRONMENTAL CONTROL AND HABITABILITY

306.1 **General.** A safe and habitable internal environment shall be provided within the CHS throughout all crewed operational phases. Habitability

requirements should comply with NASA-STD-3000 and 3001.

306.2 **Life Support System.** The vehicle's 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 one 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.

c) 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.

d) Capability to maintain cabin total pressure at greater than 972.16 hPA (i.e., 14.1 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).

e) 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.

f) 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).

g) Monitor atmosphere temperature over the range of 15.5 to 32.2 degrees Centigrade (i.e., 60 to 90 degrees F) with an accuracy of +/- 0.5 degree Centigrade (i.e., 1 degree F).

h) Detect combustion products over specified ranges.

i) 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.

l) 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 **Payload/Cargo Leakage.** Payload/cargo flown in the vehicle habitable volume shall meet the containment requirements of paragraph 302.3. Payload/cargo configurations during unmanned operations are not restricted; however, The crewed compartment shall be environmentally safe for crew ingress during any revisit. Safe conditions for entry may be established by review of the containment design features, proof of adequate atmospheric scrubbing for the chemical involved, vacuum evacuation, use of equipment capable of detecting toxic chemicals prior to crew exposure, or other techniques suitable for the particular experiment involved.

306.4 **Contamination Control.** Specific design and mission provisions shall be made for contamination control in the vehicle and interfacing subsystems. For internal environments monitoring of particulate, molecular and microbiological contamination shall be assessed. SMAC's of atmospheric contaminates are specified in Table 1 and Table IV.

306.5 **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.

306.6 **Vibrations.** The vehicle vibrations environment shall not cause injury, fatigue, or in any other way degrade human / machine system effectiveness (e.g., instrument reading).

306.7 **Mechanical Hazards.** The vehicle system and equipment design shall protect the flight personnel from sharp edges, protrusions, etc. during all flight operations. Translation paths and adjacent equipment shall be designed to minimize the possibility of entanglement or injury to flight members. There shall be no sharp edges in structures in areas where cables are installed to avoid any possibility of damaging cables.

306.8 **Thermal Hazards.** During normal operations, the flight personnel shall not be exposed to high or low surface temperature extremes. Protection shall be provided against continuous skin contact with surfaces above 49 degrees Centigrade or below 4 degrees Centigrade. Safeguards such as warning labels, protective devices or special design features to protect the crew from surface temperatures outside these 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 shall apply for such use, as determined by the relevant national civil aviation authority

307.2 **Capsule and hybrid Recovery System** (Reserved)

308 HAZARDOUS OPERATIONS

308.1 **Hazard Identification.** The CHS Operator shall assess all 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.

308.2 **Exposure to Risk.** 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 .

308.3 **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 GENERAL

The following requirements are applicable to the CHS and its elements development.

401 SAFETY ANALYSIS

A safety analysis shall be performed in a systematic manner on the CHS, its elements, related software, and ground 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 IAASS-ISSB in accordance with paragraph 404. Detailed instructions for the safety analysis and safety assessment reports will be provided in IAASS-ISSB/ ISS-13830.

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 **Design for Minimum Hazard.** 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 personnel safety.

403 SAFETY ASSESSMENT REVIEWS AND SAFETY CERTIFICATION

Safety assessment reviews will be conducted by the ISSB 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 for CHS design and flight and ground operations. See paragraph 401.

b. A CHS safety verification tracking log.

c. Approved 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, and inspection 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 report as MIP's requiring independent QA observation.

405.2 **Verification Tracking Log.** A safety verification tracking log (see IAASS-ISSB-13830) 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 ISSB 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 (paragraph 404). 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.

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.

ACGIHA. American Conference of Governmental Industrial Hygienists.

ANSI. American National Standards Institute.

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. A human-rated system commercially operated to perform suborbital or orbital flights. It includes as element, vehicles such as capsules or winged bodies, performing transportation to/from orbit operations. It includes also orbital stations. A vehicle is a CHS element and may be for a part of its flight a payload for a launcher (expendable launch vehicle) or for a winged carrier. In this document, the requirements refereeing to the CHS apply to the intergraded configuration (i.e.: vehicle integrated on launcher or carrier and to the vehicle after separation).

CHS ELEMENTS. Vehicle, subsystems, equipment and any other item which are subsets of a CHS.

CHS OPERATOR (CO). The company which provides commercial human transportation services and on-orbit operations services. Also a company which provides commercial unmanned cargo transportation services to on-orbit crewed vehicle.

CO. Commercial Human-rated System Operator.

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).

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.

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.

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

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**.**

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.

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 payload shall be able to withstand without failure.

FAILURE. The inability of a system, subsystem component or part to perform its required function under specified conditions for a specified duration.

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

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, smoldering 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.

GSE. Ground Support Equipment.

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

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.

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.

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.

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.

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

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.

ISSB. Independent Space Safety Board.

KOS. keep-out Sphere.

LBB. Leak-before-burst.

MEOP. Maximum Expected Operating 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.

M/OD. Meteoroid / Orbital Debris.

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

NEAR REAL TIME MONITORING. Near-real-time monitoring (NRTM) is defined as notification of changes in inhibit or safety status on a periodic basis.

OFFGASSING. The emanation of volatile matter of any kind from materials into habitable areas.

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.

PTFE. Polytetrafluoroethylene.

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.

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.

RCS. Reaction control 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. 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.

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.

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

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).

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).

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

TLV. Threshold Limit Value.

VEHICLE. A vehicle is refereed to in this document as a the capsule or air-carrier detached space system designed to transport humans for either orbital and/or sub-orbital 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.

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
MSFC-HDBK-527/JSC 09604, Materials Selection List for Space Hardware Systems.	301.5, 302
NASA-STD-8719.13B, Software Safety	205.1
ANSI/AIAA S-080, Space Systems – Metallic Pressure Vessels, Pressurized Structures, and Pressure Components.	301.6.1a
ANSI/AIAA S-081, Space Systems – Composite Overwrapped Pressure Vessels (COPVs).	301.6.1.6
NSTS 22648, Flammability Configuration Analysis for Spacecraft Applications.	302.4
NSTS 08060, Space Shuttle System Pyrotechnic Specification.	201.5.2.3
ANSI-Z-136.1, American National Standard for Safe Use of Lasers.	305.5
American Conference of Governmental Industrial Hygienists (ACGIH), Threshold Limit Values and Biological Exposure Indices.	305.3, 305.6
JSC 20793, Manned Space Vehicle Battery Safety Handbook.	303.6
IEEE C95.1, "IEEE Standard for Safety Levels with Respect to Human Exposure to Radio-Frequency Electromagnetic Fields, 3 kHz to 300 GHz"	305.2.2
NASA-STD-3000 and 3001, Man-Systems Integration Standards.	305.2.1, 306.1

DOCUMENT NUMBERS AND TITLES	REFERENCED IN PARAGRAPH
MIL-HDBK-5G	301.4
IAASS-ISSB13830, Safety Review and Data Submittal Requirements.	103.1, 200, 200.2, 201.5.2.3, 301.6.1 302.4, 401, 406.2
IAASS-ISSB 18798, Interpretations of CHS Safety Requirements.	103.2, 303.1
MIL-STD-1576, Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems.	201.5.1.1, 201.5.1.2 201.5.2.7
NASA-STD-6001, Flammability, Odor, Offgassing, and Compatibility Requirements and Test Procedures for Materials in Environments that Support Combustion. (formerly NHB 8060.1C)	201.5.3.3, 302.2, 302.4, 302.5, 302.7a
NASA-STD-5003, Fracture Control Requirements for Payloads Using the Space Shuttle.	301.1
MSFC-STD-3029, Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments.	301.5

APPENDIX C: FIGURES AND TABLES

Figure 1.– NASA Copper-Harper Rating Scale

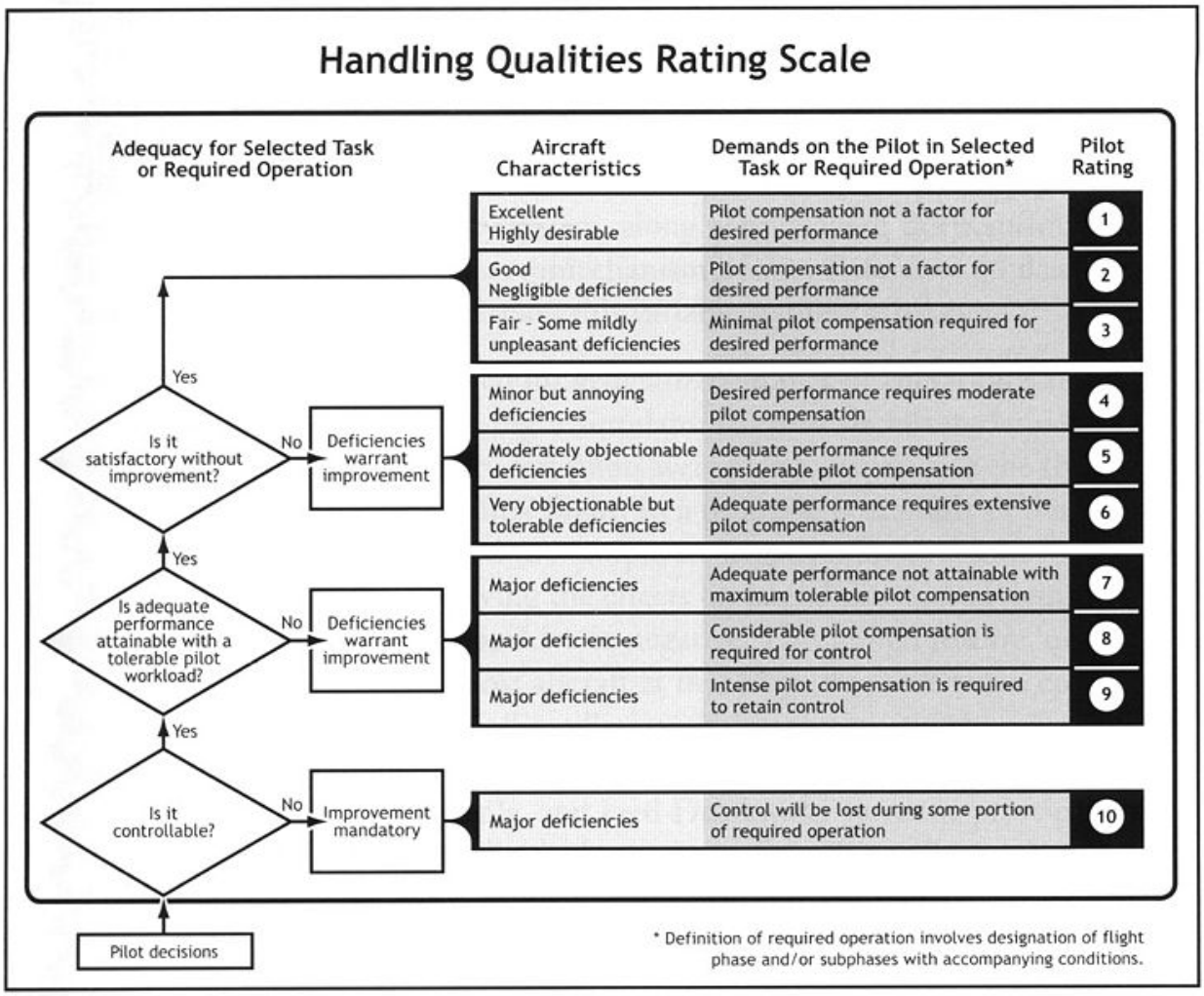

Figure 2.- Safe distance for firing liquid propulsion thrusters.

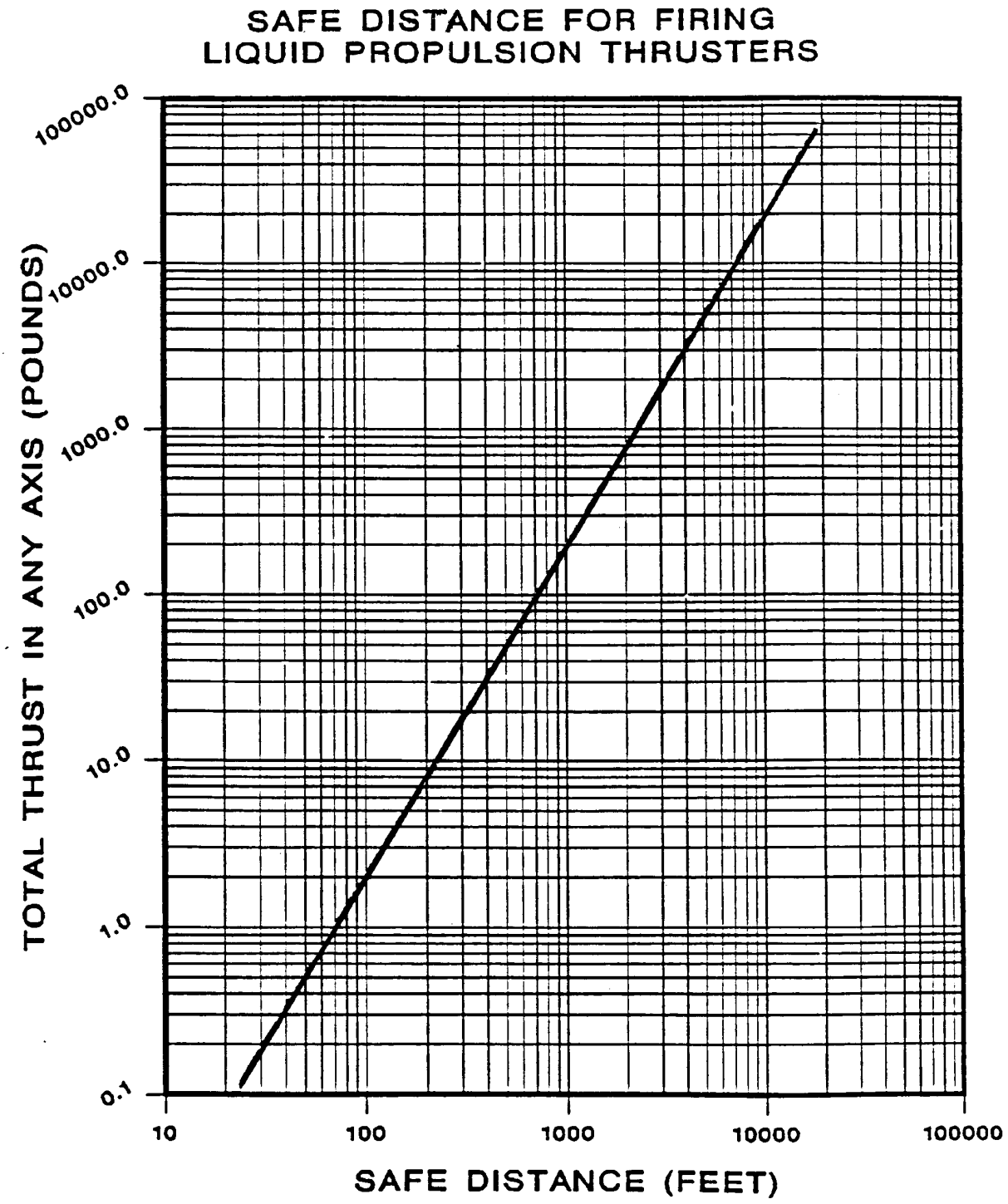

TABLE 1. Spacecraft maximum allowable concentrations						
		Potential Exposure Period				
Chemical		1 h	24 h	7 d	30 d	180 d
Acetaldehyde	mg/m^3	20	10	4	4	4
Acrolein	mg/m^3	0.2	0.08	0.03	0.03	0.03
Ammonia	mg/m^3	20	14	7	7	7
Carbon Dioxide	mm Hg	10	10	5.3	5.3	5.3
Carbon monoxide	mg/m^3	60	20	10	10	10
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 2. 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