Federal Aviation Administration

Recommended Practices for Human Space Flight Occupant Safety

Version 1.0

August 27, 2014

Federal Aviation Administration
Office of Commercial Space Transportation
800 Independence Avenue, Room 331
Washington, DC 20591

TC14-0037

Record of Revisions

Version	Description	Date
1.0	Baseline version of document	August 27, 2014

TABLE OF CONTENTS

A. INTRODUCTION

1.0 Purpose

The purpose of this document is to provide a compilation of practices that the Federal Aviation Administration (FAA) Office of Commercial Space Transportation (AST) believes are important and recommends for commercial human space flight occupant safety. The document is intended to enable a dialogue among, and perhaps consensus of, government, industry, and academia on practices that will support the continuous improvement of the safety of launch and reentry vehicles designed to carry humans.

The document can also be used to help identify subject areas that could benefit from industry consensus standards. There are a number of industry and government standards that address the subject areas covered in this document, but some subject areas may not have standards that are appropriate for the commercial human space flight industry. The development of industry consensus standards in these subject areas could have significant benefits for the safety of future commercial operations.

Lastly, the document may serve as a starting point for a future rulemaking project, should there be a need for such an effort at some point in the future. However, this document is not a regulation, and it has no regulatory effect.

2.0 Scope

The scope of this document includes suborbital and orbital launch and reentry vehicles. The document assumes that any orbital vehicle will stay in Earth orbit for a maximum of 2 weeks, and can return to Earth in under 24 hours if necessary. Orbital rendezvous and docking, flights longer than 2 weeks, extravehicular activity, and any flights beyond Earth orbit are not explicitly addressed. Future versions of this document may cover such additional human space flight operations and missions.

The recommended practices in this document cover the safety of occupants only, that is, flight crew and space flight participants. Public safety and mission assurance are not addressed. This document also takes a "clean sheet" approach to occupant safety, in that it assumes no other regulations act to protect occupants from harm, including AST's existing regulations in 14 CFR Chapter III.

Lastly, the recommended practices in this document cover occupants from the time they are exposed to vehicle hazards prior to flight until after landing when they are no longer exposed to vehicle hazards.

3.0 Development Process

Fifty years of human space flight have provided AST with a wealth of information to use in developing this document. AST reviewed existing government and private sector requirements and standards, including those from the National Aeronautics and Space Administration (NASA), the European Space Agency, and the International Association for the Advancement of Space Safety. AST used NASA's requirements and guidance for its Commercial Crew Program[1] as the primary guide for the development of this document. This is because, with some exceptions unique to the program, the Commercial Crew Program requirements and guidance provide comprehensive coverage of occupant safety. Our purpose was not to copy NASA's requirements, but to use them as a means to capture safety practices and judge whether they are, at a general level, appropriate for the commercial human space flight industry.

The recommended safety practices have been vetted with a wide audience, including the Commercial Space Transportation Advisory Committee (COMSTAC), NASA, the FAA's Civil Aerospace Medical Institute (CAMI), and the FAA's Center of Excellence for Commercial Space Transportation (COE). We held eight teleconferences with COMSTAC from the summer of 2012 to the spring of 2013 on various topics reflected in this document. We also received a number of comments from COMSTAC on a draft of this document. NASA reviewed and commented on the draft as well. We worked closely with CAMI on space flight medical issues and with the COE on various technical and medical issues related to suborbital human space flight safety.[2]

4.0 Level of Risk and Level of Care

4.1 Level of Risk

This document does not aim to achieve a single level of risk for commercial human space flight systems. Because of the wide variety of commercial human space flight activities that are likely to take place in the future, with differing destinations, purposes, and architectures, different risk levels may be appropriate in different situations. In addition, establishing a single level of risk may inadvertently limit innovation. Collectively, however, the application of these recommended practices will ensure that occupant safety is considered throughout the life cycle of a space flight system, and that occupants are not exposed to avoidable risks.

[1] Specifically, CCT-PLN-1120, CCT-REQ-1130, and CCT-STD-1150.
[2] In particular, the University of Colorado and the University of Texas Medical Branch.

4.2 Level of Care

Three levels of care are addressed in this document. First, the occupants of commercial human space flight vehicles should not experience an environment that would cause a serious injury or fatality, from the time they are exposed to vehicle hazards prior to flight until after landing when they are no longer exposed to vehicle hazards. This is a low bar, below the level of comfort that most space flight participants would want to experience.[3]

Second, the level of care for flight crew when performing safety-critical operations should be at the level necessary to perform those operations. For example, if planned translational forces will not result in serious injuries, but the flight crew needs lower forces in order to move their arms to perform a safety-critical operation, then an increased level of care is reflected in this document. Note that we have assumed that each member of the flight crew is safety-critical, and that space flight participants may be called upon to perform limited safety-critical tasks, such as emergency egress and restraining themselves in their seats.

The third level of care applies to emergencies. In emergencies, occupants should have a reasonable chance of survival. A number of recommended practices in this document address emergencies, and are listed in Table 1.

Table 1: Practices Addressing Emergencies

Recommended Practice	Section
Emergency Survival Equipment and Supplies	1.1.6
Emergency Response to Contaminated Atmosphere	1.2.9
Emergency Response to Loss of Cabin Pressure Integrity	1.2.10
Emergency Response – Abort and Escape	1.2.11
Emergency Occupant Location Post-Landing	1.3.13
Emergency Communication with Rescue Personnel	1.3.14
Emergency Control Markings	1.4.14
Emergency Equipment Access	1.4.15
Emergency Lighting	1.4.16
Emergency Vehicle Egress	1.4.17
Occupant Survivability Analysis	1.5.4
Emergency Operations Management	3.3.20
Emergency Survival Equipment Training	3.5.8

[3] If a failure occurs that leaves the system in a state where another failure may lead to a catastrophic situation, an operator following these recommended practices would end the flight early, providing the occupants the same level of care through the end of flight.

5.0 Structure and Nature of the Recommended Practices

5.1 Categories

The recommended practices are divided into three categories: design, manufacturing, and operations. This document is written to be neutral as to whether separate entities design, manufacture, and operate a human space flight system, or whether one entity does it all. However, we have attempted to write the document in a way that ensures safety concerns are addressed in an integrated fashion over the entire life cycle of a system.

The design and operations categories are further broken down into subcategories, as shown in Figure 1.

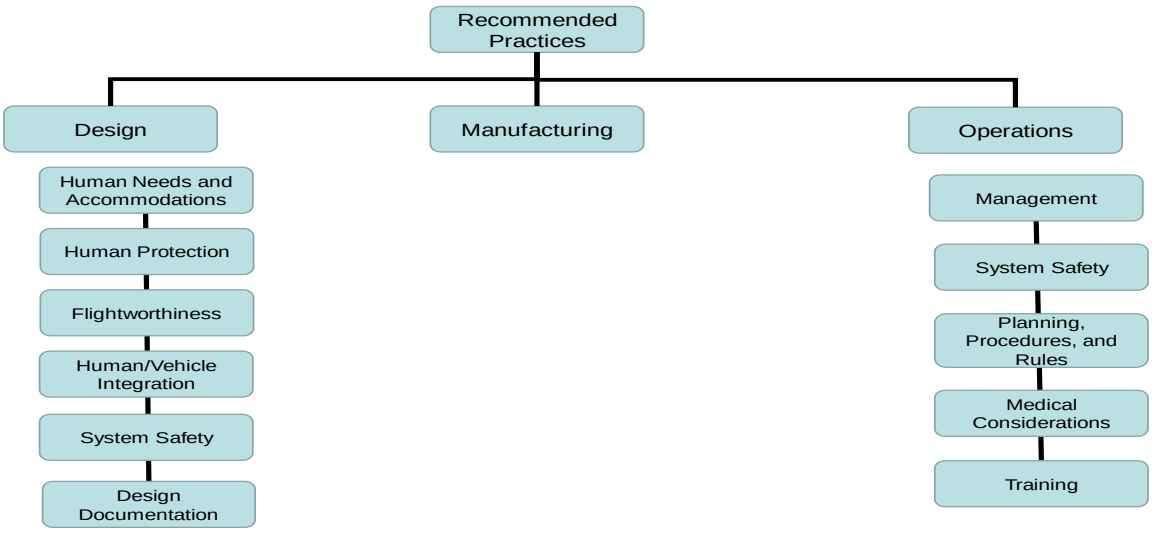

Figure 1: Recommended Practices Framework

The subcategories are defined as follows:

Design

Human Needs and Accommodations – This subcategory includes the steps necessary to accommodate specific human needs, such as consumables, human waste disposal, etc., that have no relation to specific mission tasks or physical stress, unless not met.

Human Protection – This subcategory includes the steps necessary to keep an occupant's physical or psychological stress at levels that can be considered safe for space flight participants, and sufficient for flight crew to execute the flight.

Flightworthiness – This subcategory identifies the minimum system capabilities necessary to maintain occupant safety.

Human/Vehicle Integration – This subcategory includes operational and design constraints necessary to integrate humans with a human space flight system.

System Safety – This subcategory includes engineering and management principles, criteria, and techniques to achieve acceptable risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

Design Documentation – This subcategory includes documentation related to the design of the human space flight system necessary to operate the system safely.

Operations

Management – This subcategory includes program controls necessary to ensure proper implementation of safety requirements.

System Safety – This subcategory includes system safety management and engineering principles, criteria, and techniques applicable during the operational phase of a system's life cycle.

Planning, Procedures, and Rules – This subcategory includes plans and procedures necessary to safety operate a human space flight system.

Medical Considerations – This subcategory includes medical needs and constraints for flight crew and space flight participants.

Training – This subcategory includes training needs of flight crew, space flight participants, ground controllers, and safety-critical ground operations personnel.

Note that recommended safety practices applicable to more than one category, such as configuration management, are written only once and then referred to in subsequent categories.

5.2 Performance and Process Based Practices

The recommended practices in this document are primarily performance based, stating a safety objective to be achieved, and leaving the design or operational solution up to the designer or operator. In addition, we have refrained from establishing hard numerical limits where possible because there is often no consensus on specific values, they can limit design flexibility, and they may not stand the test of time as technology advances.

A few process based practices are included in the document, including system safety, software safety, and payload safety. The performance based practices address hazards that are present regardless of system design and operation, while the system safety, software safety, and payload safety processes systematically address hazards that are unique to a particular design or operation.

5.3 Depth and Breadth of Practices

The recommended safety practices in this document are broadly written, and do not go into detail on any particular practice. Such details may be better addressed in industry standards.

This document also does not address how a designer or operator would verify that it meets each safety measure. Verification is a significant cost driver, and is an area that may be added to this document in the future.

5.4 "System" vs. "Vehicle"

Although definitions of terms are provided in the back of this document, it is particularly important to understand the distinction between "system" and "vehicle." This is because certain practices are specific to the vehicle, while other practices are applicable to the entire system. The two terms are defined as follows:

- System means an integrated composite of personnel, products, subsystems, elements, and processes that when combined together will safely carry occupants on a planned space flight.[4]

- Vehicle means that portion of a space flight system that is intended to fly to, operate in, or return from space. This includes any launch vehicle, carrier aircraft, equipment, and supplies, but excludes payloads.

An example of the use of "system" is found in section 1.3.1, Failure Tolerance to Catastrophic Events. AST recommends that the "system" should control hazards that can lead to catastrophic events with no less than single failure tolerance. "System" is used here because the vehicle and other parts of the space flight system, such as ground systems, procedures, and training, often work together to provide failure tolerance.

An example of the use of the term "vehicle" is found in a related section, 1.3.3, Separation of Redundant Systems. AST recommends that the "vehicle" should be designed to separate or protect redundant safety-critical systems and subsystems such that an unexpected event which

[4] Any narrower use of the word "system" will be clear in its usage (e.g., safety-critical system, or launch escape system).

damages one is not likely to prevent the other from performing its function. This practice is applied at the vehicle level as opposed to the system level because the vehicle is the part of the space flight system most susceptible to damage that could affect redundant systems.

6.0 Notable Omissions

Some notable omissions from the recommended practices include the following topics:

6.1 Medical Limits for Space Flight Participants

This document does not include any medical criteria that would limit who should fly in space as a space flight participant. Medical consultation for space flight participants is recommended to inform them of risks and to ensure they will not be a danger to other occupants. However, space flight participants should be free to make decisions about their own individual risk.

We do understand that flying members of the public outside the relatively healthy government astronaut population is new, and that commercial operators will be challenged to control hazards to space flight participants from other space flight participants with medical conditions. However, we have not included any performance standards in this document to address this issue.

6.2 Ionizing Radiation

Occupants exposed to ionizing radiation during space flight have an increased lifetime risk of cancer, and their progeny have an increased risk of inheriting genetic disorders. This is an inherent risk of space flight. An operator can minimize occupant exposure to radiation through such measures as shielding, the use of low inclination orbits, and avoiding space flight during extreme solar events. However, this document does not include ionizing radiation exposure limits because the recommended practices aim to avoid serious injuries or fatalities, not long-term health effects.

6.3 Integration of Occupant and Public Safety

This document does not attempt to address the integration of occupant and public safety. Actions that may be appropriate for occupant safety may have public safety implications and vice versa. This is an area of future work for AST.

7.0 This Document's Relation to NASA Requirements

Any space transportation system that complies with NASA commercial crew requirements would likely be consistent with the recommended safety practices in this document. NASA commercial crew requirements are much more exhaustive, and address mission assurance and other mission needs in addition to occupant safety. NASA also addresses verification and incorporates a number of government and industry standards that AST has yet to address.

8.0 Future Versions

This document will evolve as industry evolves. At a minimum, AST plans to modify this document in the future to incorporate new knowledge we gain either from feedback we receive or from industry experience. We may also enhance the manufacturing section, and add verification statements to each practice.

B. RECOMMENDED PRACTICES

1.0 DESIGN

1.1 Human Needs and Accommodations

1.1.1 Atmospheric Conditions

a. The vehicle should provide atmospheric conditions to all occupants adequate to protect them from serious injury and allow safety-critical operations to be performed.

b. The flight crew or ground controllers should be able to monitor and control the following atmospheric conditions in the inhabited areas:

    1. Composition of the atmosphere and any revitalization;

    2. Pressure, temperature, and humidity;

    3. Contaminants that include particulates, and any harmful or hazardous concentrations of gases, vapors, and combustion byproducts; and

    4. Ventilation and circulation.

    Direct monitoring and control may not be necessary if analysis and testing demonstrates they are not needed to protect the occupants from serious injury or to allow safety-critical operations to be performed.

Rationale: Occupants may become ill or incapacitated if the habitable environment is either contaminated or otherwise degraded. In addition, an ill or incapacitated occupant may divert the flight crew's attention from the performance of safety-critical operations, thus endangering occupant safety. For example, very low oxygen partial pressure constitutes a severe hazard, resulting in impaired judgment and ability to concentrate, shortness of breath, nausea, and fatigue, thus affecting crew performance and potentially resulting in a serious injury or fatality. Likewise, hazardous concentrations of gases or vapors that build up during the course of a space flight due to metabolic or other processes occurring in the cabin, or contaminants for which a source is present in the cabin (and could be further exacerbated by a lack of ventilation and circulation), can have the same result. In addition, high humidity is a factor in the formation of condensation, which could lead to the growth and proliferation of harmful bacteria and fungi. Therefore, the capability to monitor and control these atmospheric conditions is necessary to protect occupants from harm.

Note, however, that direct monitoring and control may not be necessary in all vehicle concepts, such as suborbital flights of limited duration. For example, trace contaminants may be controlled passively by the design of the system, and not actively monitored or controlled by the flight crew or the ground.

1.1.2 Food and Water

Any food and water provided to the occupants for consumption should be handled, stored, and dispensed to protect against illness or serious injury.

Rationale: Occupants may become ill or incapacitated if food and water are contaminated. In addition, ill or incapacitated flight crew may not be able to perform their safety-critical operations. An ill or incapacitated occupant may also divert the flight crew's attention from the performance of safety-critical operations, thus endangering occupant safety.

1.1.3 Flight Crew Rest

For orbital flight, the vehicle should provide accommodations and an environment for flight crew sleep.

Rationale: Crew rest is an important component to ensuring the safety of the occupants aboard a vehicle. A fatigued crew can make mistakes that put the occupants at risk. Allowing the flight crew to have the opportunity to rest during an orbital flight should help avoid mistakes that could be attributed to crew fatigue. Depending on the vehicle design, there may be enough habitable volume to allow the flight crew to rest in a sleeping bag or, with less volume, the flight crew may need to be restrained in their seats. Operationally, the amount of noise and light in the habitable volume could impact the flight crew's opportunity to rest. Tethering locations, pillows, blankets, earplugs, or other items may be helpful to allow the flight crew to rest.

1.1.4 Body Waste and Vomitus Management

The system should manage body waste and vomitus to protect all occupants from serious injury and allow safety-critical operations to be performed. For orbital missions, this should include supplies for personal and habitable volume hygiene, containment, isolation, stowage, odor control, and labeling for waste containers.

Rationale: Occupants may become ill or incapacitated if the habitable environment is either contaminated or otherwise degraded by occupant body waste and vomitus. In addition, ill or incapacitated flight crew may not be able to perform their safety-critical operations. Errant body waste and vomitus may also divert the flight crew's attention from the performance of safety-critical operations, thus endangering occupant safety. Because orbital flights are longer than suborbital flights, containment, isolation, stowage, odor control, and other considerations are recommended to help ensure the safety of occupants.

1.1.5 Biological Waste and Wet Trash Management

For orbital flight, the system should manage biological waste and wet trash to protect all occupants from serious injury. For orbital missions, this should include supplies, containment, isolation, stowage, odor control, and labeling for waste containers.

Rationale: Occupants may become ill or incapacitated if the habitable environment is either contaminated or otherwise degraded by biological waste or wet trash. In addition, ill or incapacitated flight crew may not be able to perform their safety-critical operations. If not properly contained, biological waste or wet trash contents could damage equipment, injure crew members, or transmit disease.

1.1.6 Emergency Survival Equipment and Supplies

The vehicle should include emergency survival equipment and supplies that provide a reasonable chance of survival of all occupants for post-landing emergencies. Unless unnecessary for the design reference mission, the emergency survival equipment and supplies should include items from each of the following categories:

a. First aid;

b. Water, water collection, and water purification;

c. Fire starter;

d. Shelter;

e. Floatation device;

f. Food;

g. Signaling equipment;

h. Navigation; and

i. Survival tools.

Rationale: In a post-landing emergency situation, emergency survival equipment and supplies provide for occupant safety and improve an occupant's chance of survival. The emergency survival equipment and supplies should provide readily-accessible survival rations and equipment to support occupant needs while awaiting rescue. Since emergency landing locations and conditions are often unpredictable, an operator should use the design reference mission as a basis for determining which items should be included as emergency survival equipment and supplies. For example, on a suborbital flight, if no over-water flight will occur, there is no need for equipment necessary for survival on water. Orbital flights however, should address the needs to survive in many different environments, such as the ocean.

1.2 Human Protection

1.2.1 Acceleration Protection

The vehicle should be designed to limit occupant exposure to transient and sustained linear and angular acceleration such that occupants are protected from serious injuries and safety-critical operations can be performed successfully.

Rationale: High transient and sustained linear and angular acceleration can increase the risk of occupant incapacitation, or a serious injury or fatality. High rates and extended periods of acceleration in the Gz-axis can significantly increase the risk of short-term incapacitation due to cerebral hypoxia. When a flight crew has been weightless and then experiences accelerations during reentry in the Gz-axis, loss of color vision, tunnel vision, and loss of consciousness can occur, which could prevent the crew from performing their safety-critical operations. Long periods of acceleration can also have psychological effects that can impair decision-making.

The vehicle may still experience periods of high acceleration during reentry or approach to landing. However, countermeasures for the flight crew, such as a G-suit or specific crew seating configurations, can prevent vehicle acceleration from impairing the flight crew.

1.2.2 Vibration Protection

The vehicle should be designed to limit occupant exposure to vibration such that occupants are protected from serious injuries and safety-critical operations can be performed successfully.

Rationale: Depending on the vibration amplitude and frequency, excessive vibration can increase the risk of occupant incapacitation, or a serious injury or fatality. Excessive vibration can also lead to lack of concentration, psychological effects that can impair decision-making, and distorted communications, such that safety-critical operations may be affected and, as a result, threaten occupant safety.

1.2.3 Radiation Protection

The vehicle should be designed to limit occupant exposure to the following types of radiation such that occupants are protected from serious injuries and safety-critical operations can be performed successfully:

a. Radiofrequency non-ionizing radiation; and

b. Near infrared, visible, and ultraviolet radiation.

Rationale: Exposure to excessive radiation can significantly increase the risk of occupant incapacitation, or a serious injury or fatality. It can also significantly increase the risk of momentary incapacitation of flight crew, such that safety-critical operations may be affected and, as a result, threaten occupant safety.

a. Exposure to radiation from sources such as a LiDAR or similar system can lead to temporary or permanent blindness. Exposure to radiation from sources such as C-band, S-band, or Ku-band

systems can lead to injuries in soft tissues. Cumulative exposure during a flight to non-ionizing radiation can also cause incapacitation or serious injury.

b. *In low Earth orbit, near infrared radiation raises the internal temperature of the eye and can lead to lens, cornea, and retina damage. Extended exposure to visible radiation may increase the risk of macular degeneration disease where an affected person loses central vision. Ultra Violet-A and Ultra Violet-B radiation have damaging effects on exposed soft tissues, such as skin and eyes.*

1.2.4 Noise Exposure Protection

The vehicle should be designed to limit occupant exposure to noise such that occupants are protected from serious injuries and safety-critical operations can be performed successfully.

Rationale: Excessive sound pressure (noise) can increase the risk of occupant incapacitation, serious injury, or fatality. Excessive sound pressure can also lead to lack of concentration, psychological effects that can impair decision-making, and distorted communications, such that safety-critical operations may be affected and, as a result, threaten occupant safety.

1.2.5 Mechanical Hazards Protection

The vehicle should be designed to protect occupants from serious injuries and to ensure no interference with the successful performance of safety-critical operations due to:

a. Moving parts;

b. Entrapment;

c. Stored potential energy;

d. Burrs;

e. Pinch points;

f. Sharp edges;

g. Sharp items; and

h. Temperature.

Rationale: The vehicle, including its hardware and equipment, should be designed to protect against a serious injury or fatality caused by occupant contact with mechanical hazards, an occupant becoming trapped or snagged by fixed or loose items, and from the release of stored energy.

a. *An occupant's ability to perform safety-critical operations could be hampered by moving parts, such as gears, that could catch on an occupant's clothing or hair and cause a serious injury or*

fatality. Historically, covers or panels have been used as preventive measures to minimize the risk.

b. *Entrapment can occur in places where loose cables or other restraint devices, such as tethers, straps, or nets get in the way of an occupant's path. An occupant's clothing, fingers, or toes could become trapped or snagged. Additionally, entrapment can occur if the occupant is unable to unfasten their seat restraint. Any entrapment could result in a serious injury.*

c. *Items with stored potential energy (e.g., springs) could become projectiles in a microgravity environment and result in a serious injury to an occupant.*

d. *The removal of burrs can help to prevent an occupant from receiving a serious injury.*

e. *Pinch points can cause serious injury to an occupant, but may exist for the nominal function of equipment (i.e., equipment panels). Serious injury may be avoided by locating pinch points out of the occupant's reach or providing guards to eliminate the potential to cause injury.*

f. *An occupant's ability to perform safety-critical operations could be hampered by surfaces with sharp edges. Sharp edges are hazards and may distract from or impair the performance of safety-critical operations.*

g. *Functionally sharp items (e.g., syringes, scissors, knives) are intentionally sharp and should be prevented from causing serious injury when not being used for their intended purpose.*

h. *An occupant's ability to perform safety-critical operations could be hampered by the temperature of the interface (e.g., a touchscreen that is too hot to touch). Extreme touch temperatures, both hot and cold, can cause pain and distract from the performance of safety-critical operations.*

1.2.6 Orthostatic Protection

The vehicle should provide orthostatic intolerance countermeasures to the extent necessary for occupants to perform safety-critical operations.

Rationale: Post-landing orthostatic intolerance, the inability to maintain blood pressure while in an upright position, is a medical condition associated with human exposure to microgravity during space flight. Although the physiological mechanisms are not completely understood, countermeasures are needed to ensure occupant safety. Symptoms and signs of orthostatic intolerance include dizziness, lightheadedness, confusion, fainting, and impaired consciousness. This may result in an inability to operate controls, complete safety-critical tasks, or egress from the space vehicle without assistance. Historical NASA studies have shown that post-landing orthostatic intolerance is a frequent consequence of space flight, and countermeasures have been needed to allow occupants to egress the vehicle. Thus, without appropriate mitigation strategies, a flight crew suffering the effects of orthostatic intolerance could jeopardize safe and successful reentry, landing, and egress, particularly in the event of an emergency before first responders are available.

1.2.7 Medical Equipment and Supplies

The vehicle should have first aid and medical equipment and supplies for treatment of injuries or medical emergencies that might occur during flight, consistent with the design reference mission and the number of occupants.

Rationale: Injuries to astronauts have been common during space flights to date, including musculoskeletal injuries, abrasions, contusions, lacerations, foreign objects in the eye, and burns. As such, it should be expected that medical injuries may be sustained during future space flights. Having first aid and medical equipment on board, consistent with the design reference mission and the number of occupants, provides a means to apply first aid to an injury and help prevent any injuries sustained in flight from evolving into a more serious injury. For example, a suborbital flight operator may be able to very quickly provide medical assistance due to the very short duration of flight. However, an orbital mission in most cases will require a much longer period of time to return an occupant in need of medical attention. Therefore, having medical equipment and supplies onboard is necessary to address the injury or medical emergency until post-landing medical attention can be provided.

1.2.8 Fire Event Detection and Fire Suppression

a. The system should have the ability to detect a fire event within the habitable volume and alert the occupants.

b. The vehicle or an occupant should have the ability to extinguish a fire in the habitable volume.

Rationale: In enclosed spaces, fire significantly threatens occupant safety, and alerting the occupants to the presence of a fire allows for quick action to mitigate the hazardous effects. Automatic detection is often preferable, such as with a smoke detector. However, for small habitable volumes and short duration flights, human senses may suffice to detect a fire event. Firefighting capability may be achieved using a fire suppression system integrated with the vehicle, portable fire extinguishers, or both.

1.2.9 Emergency Response to Contaminated Atmosphere

In order to respond to a contaminated atmosphere, the vehicle should provide equipment and provisions to limit occupant exposure to the contaminated atmosphere such that occupants are protected from serious injuries and safety-critical operations can be performed successfully. The equipment and provisions should:

a. Provide breathable air and eye protection for each occupant;

b. Provide voice communication between the flight crew and the ground controllers; and

c. Provide voice communication between the flight crew and the space flight participants.

Rationale: In an emergency situation, fire, toxic off-gassing, and chemical leaks can degrade the vehicle's atmospheric conditions, increasing the risk of occupant incapacitation, or a serious injury or

fatality. In addition, such emergencies are difficult to manage by the flight crew due to the potential of inhalation or eye injuries. The use of a self-contained breathing apparatus, for example, can protect occupants from the hazard, and allow the flight crew to manage the emergency.

The ability to verbally communicate with the ground while wearing emergency gear provides the crew with an additional resource to respond to the emergency. The ability to verbally communicate within the vehicle while wearing emergency gear enhances situational awareness and increases safety by allowing multiple occupants to coordinate activities necessary to resolve the on-going emergency.

1.2.10 Emergency Response to Loss of Cabin Pressure Integrity

In the event cabin pressure integrity is lost, the vehicle should be designed to prevent incapacitation of flight crew and serious injury of occupants by providing:

a. Enough pressurant gases to maintain cabin pressure; or

b. A pressure suit or other equivalent system that makes available environmental control and life support capability for the occupants.

Rationale: Space flight takes place in an extreme environment such that without protection from the environment's extremely low pressures and wide ranging temperatures, life cannot be sustained. Full and partial pressure suits have historically been used to protect the human from these elements when cabin pressure failures occur. With improvements in technology, reliability, and redundancy in environmental control and life support systems, the use of emergency systems such as pressure suits may not always be required. In some cases, such as short suborbital flights, enough gas or cryogenic fluid can be stored to sustain minimal cabin pressure in the event of a leak for the period of time that it would take to return the vehicle back to atmospheric conditions that can sustain life.

1.2.11 Emergency Response – Abort and Escape

The system should provide the capability to abort, escape, or both, during pre-flight and ascent.

Rationale: The capability to respond to an imminent catastrophic hazard (e.g., loss of thrust, loss of attitude control, vehicle explosion, etc.) can provide occupants with a reasonable chance of survival. Escape includes safely returning the occupants to Earth in a portion of the space flight system normally used for reentry and landing, or by the removal of the occupants from the portion of the space flight system normally used for reentry and landing. While a successful abort or escape may not be possible for every imaginable event, history has shown that having the capability to abort, escape, or do both, significantly enhances occupant safety.

1.3 Flightworthiness

1.3.1 Failure Tolerance to Catastrophic Events

a. The system should control hazards that can lead to catastrophic events with no less than single failure tolerance.

b. When failure tolerance adds complexity that results in a decrease in overall system safety or when failure tolerance is not practical (e.g., it adds significant mass or volume), an equivalent level of safety should be achieved through design for minimum risk.

Rationale: Failure tolerance can mitigate hazards leading to catastrophic events and improve the overall system safety. In cases where the risk remains high after applying single failure tolerance, additional redundancy may be appropriate. Additionally, the overall system reliability is a significant element used in the determination of the level of redundancy. Redundancy alone without sufficient reliability does not improve the overall system safety.

Note that failure tolerance applies not only to "must work" functions, such as preventing over-pressurization burst of the crew compartment, but also to "must not work" functions, such as ensuring crew compartment pressure relief valves do not open inadvertently or leak excessively.

Where failure tolerance is not the appropriate approach to control hazards, specific measures should be employed to achieve an equivalent level of safety. This is commonly known as "design for minimum risk." Measures that may achieve an equivalent level of safety include demonstrated reliability, design margin, and other techniques that compensate for the absence of failure tolerance.

1.3.2 Limitations on Failure Tolerance

The system should provide failure tolerance capability without:

a. Using extravehicular activity;

b. Relying upon in-flight maintenance of safety-critical equipment under time-critical situations;

c. Using emergency equipment; or

d. Using a launch escape system.

Rationale: Effective failure tolerance should not rely on time consuming and potentially dangerous crew intervention. Where redundancy is required to satisfy failure tolerance requirements, the redundancy should be built into the system and not rely on in-flight maintenance under time-critical situations or extravehicular activities to replace a failed component or avionics unit. An additional component that is on board a space flight vehicle but not designed to be a functional operating part of the system without in-flight maintenance under time-critical situations would not be considered to meet this recommended practice.

Emergency equipment and escape systems should be reserved only for emergency situations to mitigate the effects of a hazard, when the first line of defense, in the form of failure tolerance, cannot prevent the occurrence of the hazardous situation. Emergency systems and equipment, such as fire suppression systems, fire extinguishers, emergency breathing masks, pressure suits, and ballistic unguided reentry capability, are not considered part of the failure tolerance capability.

1.3.3 Separation of Redundant Systems

The vehicle should separate or protect redundant safety-critical systems and subsystems such that an unexpected event that damages one is not likely to prevent the other from performing its function.

Rationale: Physical separation or protection of redundant systems reduces the likelihood that an unexpected event that damages one system will prevent the other from performing its function. Occupant safety can be improved with a design that protects against a common cause event that would lead to failure of redundant systems. Physical separation of systems is not always possible, but this should be a design goal for any new systems or subsequent improvements to an existing system. For systems with significant heritage and demonstrated performance, it may not be necessary to physically separate existing redundant safety-critical systems.

1.3.4 Isolate and Recover from Faults

The system should detect and isolate faults in safety-critical systems, and recover any lost function to continue safe operations.

Rationale: A safety-critical function should continue in the presence of a fault. Detecting and isolating a fault prevents further propagation of the hazard. The system should recover functionality by activating the associated redundant system in time to prevent a catastrophic event. The isolation of faults should not interfere with the implementation of failure tolerance.

1.3.5 Structural Design

The vehicle structure should be designed to withstand the maximum expected operating environment throughout the life cycle of the vehicle, and have margin sufficient to account for design tolerances and uncertainties due to the environment, structural modeling, material properties, and manufacturing processes.

Rationale: Maintaining structural integrity is a fundamental safety aspect of human space flight. Uncertainties and variability always exist in predictions of structural performance. Loads are often variable and inaccurately known. Strengths are variable and sometimes inaccurately known for certain failure modes or certain states of stress; structural models embody assumptions that may introduce inaccuracies. Other uncertainties may result from quality of manufacture, operational conditions, inspection procedures, and maintenance practices. Thus, sufficiently bounding the uncertainties and adding additional margin will help avoid a structural failure.

1.3.6 Electrical Systems

The vehicle's electrical circuitry and electrical power distribution, including mating and demating of electrical connectors, should be designed to:

a. Prevent electrical shock hazard to occupants;

b. Fail safe;

c. Prevent the generation of molten material;

d. Prevent electrical wires from overheating; and

e. Protect circuitry from floating debris.

Rationale: Improperly designed electrical systems could lead to a fire, serious injury, or damage to safety-critical systems such that the occupants are unnecessarily put at risk.

1.3.7 Vehicle Stability

A vehicle whose safe flight requires a certain attitude during one or more phases of flight, should be either inherently statically and dynamically stable in that orientation during that phase or phases, or controllable to a safe attitude.

Rationale: Maintaining a safe attitude is a fundamental safety aspect of human space flight. When a vehicle requires maintenance of a specific attitude, maintenance of that attitude may be accomplished with either an inherently (through vehicle shape and center of gravity location) stable design (statically and dynamically) or using control systems such as thrusters and aero surfaces. Either method should account for nominal flight, dispersed conditions, and loss of failure tolerance. For vehicles utilizing control systems to maintain a safe attitude, they should have sufficient control authority available to initiate or counter a translation or rotation in the presence of disturbances or perturbations.

Not all phases of flight may require a specific attitude to be safe. For example, the Vostok capsule was designed to reenter in any attitude, having a spherical design with thermal protection on all sides. Some control of the capsule orientation was possible by repositioning heavy equipment to offset the vehicle's center of gravity, which was done to maximize the cosmonauts' chance of surviving the g-forces.

1.3.8 Materials and Processes

a. The vehicle should be designed to ensure that materials are compatible and do not result in a hazard under the expected operating environment.

b. For habitable volumes, the materials should not cause a toxic atmosphere, act as an ignition source, cause an explosive or flammable gas, or generate particulates that could lead to serious injury or incapacitating illness.

Rationale: Poor material choices may lead to a hazard that unnecessarily puts occupants at risk. Proper selection or testing of materials during design prevents unsafe conditions related to flammability, off-gassing, and fluid compatibility. More stringent material selection is necessary in the habitable volume because the occupants are susceptible to additional hazards such as a toxic atmosphere or particulates. The expected operating environment includes nominal and non-nominal scenarios (e.g., vacuum, high temperatures, high humidity, cabin gases, etc.). Compatibility should account for material-to-material

interactions (e.g., different thermal properties from different materials may induce thermal stress), as well as whether a material is compatible with the environment (e.g., reduced cabin pressure may result in out-gassing that leads to a hazard).

1.3.9 Natural and Induced Environments

Safety-critical systems should be designed to operate in all expected natural and induced environments.

Rationale: The environment (natural and induced) impacts the design and operation of a system and, if not accounted for properly, can have detrimental effects on safety. An understanding of the environment is necessary to identify the design and operational limitations of the system. For example, certain natural environments (e.g., temperature, humidity, and lightning) and induced environments (e.g., propulsion-related thermal loads, acoustic shock, electromagnetic interference, and vibration) should be taken into account to avoid exceeding any system capability.

1.3.10 Probability of No Penetration by Micrometeoroids or Orbital Debris

For orbital flight, the vehicle should be designed and operated to minimize the probability of a safety-critical penetration by a micrometeoroid or orbital debris.

Rationale: Micrometeoroids and orbital debris (MM/OD) creates a significant on-orbit and reentry risk for a space flight vehicle. For example, NASA probabilistic risk assessments for Space Shuttle and Constellation estimated the risk to be about 30% of the total mission risk. For MM/OD that cannot be detected or avoided, shielding mitigates damage to safety-critical systems that could result in the loss of a vehicle or endanger the occupants. In addition to shielding, operational attitudes are often used to reduce exposure of critical surface area to the MM/OD environment. Because it is not technically feasible to detect or shield against all debris, it is not possible to completely avoid the possibility of a safety-critical penetration. Shielding and operations are used to reduce the risk to an acceptable level.

1.3.11 Qualification Testing

The design of the vehicle's safety-critical systems should be functionally demonstrated at conditions beyond the maximum expected operating environment. The environmental test levels selected should ensure that the design is sufficiently stressed to demonstrate that system performance is not degraded due to design tolerances, manufacturing variances, and uncertainties in the environment.

Rationale: Qualification testing of safety-critical systems is necessary to demonstrate that the system has sufficient margin in the design to account for potential hidden design errors and quality variations in manufacturing. Qualification testing of safety-critical systems demonstrates that they meet program performance and functional expectations throughout the full range of environmental conditions and operational modes anticipated in the product's service life.

1.3.12 Flight Demonstration

a. Prior to any flight with a space flight participant, the integrated performance of a vehicle's hardware, software, and operational procedures should be demonstrated by successfully executing a flight consistent with the nominal design reference mission.

b. Further flight demonstration should be conducted for any subsequent safety-critical modification that needs flight testing to verify integrated system performance.

Rationale: A flight demonstration is a one-time test that verifies vehicle flightworthiness. This demonstration does not test the entire operating envelope, but sufficiently exercises the system capabilities, software, operations, and procedures necessary to safely execute a nominal flight carrying space flight participants. The demonstration should represent the expected flight operations and mission profile as much as possible in order to exercise the integrated system.

Major modifications such as a new propulsion system, additional stages, outer mold line changes, structural changes, aerodynamic surfaces changes, and changes in launch and reentry trajectory profiles may be significant enough to warrant another demonstration flight prior to flying space flight participants.

1.3.13 Emergency Occupant Location Post-Landing

The vehicle should:

a. Have a portable transmitter to provide occupant location to rescue personnel post-landing; and

b. Be equipped with visual aids to assist rescue personnel.

Rationale: In an unforeseen or emergency situation, the vehicle may not land at its preplanned location. Experience has shown that providing rescue personnel with information as to the vehicle's location increases their probability of being found, thereby increasing their chance of survival. A portable transmitter, such as an Emergency Locator Transmitter, that is independent of vehicle systems (e.g., power, antenna) allows the locator to remain with the occupants if they must leave the vehicle area. Visual aids such as flashing lights, sea dye, smoke, or high contrast portions of the vehicle assist rescue personnel in locating the vehicle.

1.3.14 Emergency Communication with Rescue Personnel

Post-landing, the vehicle should be capable of communicating with rescue personnel on an International Air Distress (IAD) frequency.

Rationale: In an unforeseen or emergency situation, communicating with rescue personnel improves the occupants' probability of being rescued, thereby increasing their chance of survival. Communicating on an International Air Distress (IAD) frequency (121.5, 243, or 406 MHz for voice communication) follows search and rescue standards and allows for worldwide coverage. Human space flight history provides

numerous examples of vehicles failing to land at their preplanned landing location, and of those searching to find them.

1.4 Human/Vehicle Integration

1.4.1 Physical Considerations

The vehicle should be designed such that any safety-critical operation requiring human interaction with the vehicle can be physically performed by an occupant, with the occupants, vehicle, and equipment in flight configuration. At a minimum, the following factors should be taken into account:

a. Occupant anthropometry;

b. Strength limits;

c. Range of motion limits;

d. Ergonomics;

e. Acceleration limits;

f. Vibration limits;

g. Noise limits;

h. Vision limits; and

i. Tactile limits.

Rationale: Ignoring human-to-vehicle interface issues can have adverse and unpredictable effects on an occupant's ability to perform safety-critical operations. History with space flight systems has demonstrated a large variability in the occupants that execute flight operations. Without accommodation of these variables, i.e., measurements and proportions of the human body and other factors, safety-critical operations may become hindered, causing serious injury to the occupant.

The flight crew's ability to successfully actuate controls in their intended flight configuration and environment (e.g., vertical launch configuration, space suited crew, and loaded crew compartment) is extremely important during dynamic phases of flight. Considerations include hand controls, seat dimensions, hatch or entry opening size, the distance from the seat to controls, and handle dimensions.

a. Failure to take into account human physical characteristics when designing systems or equipment can place unnecessary demands and restrictions upon an occupant.

b. *Vehicle hardware and equipment that is not operable with the lowest anticipated strength for operations and flight configurations, may not allow an occupant to perform a safety-critical operation efficiently and effectively.*

c. *The range of motion of an occupant is important for ensuring an occupant is able to perform safety-critical operations, whether or not the occupant is wearing a pressure suit.*

d. *Inadequate human-vehicle interface design could preclude an occupant from performing a safety-critical operation. Using data from occupant anthropometry, an ergonomic design of the work environment can be made safer and more comfortable for an occupant, thereby positively affecting the outcome of a safety-critical operation.*

e. *Control interfaces (e.g., control stick pivot axis) that are designed to be operable by the flight crew during vehicle acceleration and deceleration are important for ensuring the flight crew is able to perform safety-critical operations.*

f. *Proper occupant restraints are safety-critical in vehicle vibration scenarios where flight crew is operating controls. Furthermore, relevant displays that are designed with legibility in mind (e.g., analog versus digital displays, and larger graphics and text) enhance the execution of safety-critical operations during flight phases where vehicle vibration scenarios occur.*

g. *Loud noises for extended durations in the habitable volume can distract occupants, resulting in mistakes during safety-critical operations, and can defeat the effectiveness of audible cueing.*

h. *Inadequate font size, viewing angle, parallax, legibility, and lighting conditions can result in mistakes during safety-critical operations.*

i. *If pressurized suits are worn by occupants, the ability to use the sense of touch is diminished, as a gloved hand may not have the dexterity to operate certain safety-critical vehicle interfaces.*

1.4.2 System Health, Status, and Data

For a safety-critical function allocated to the ground controllers or flight crew, the system should provide the health, status, and engineering data necessary to perform the function. At a minimum, the ground controllers or flight crew should be able to determine if a level of failure tolerance is lost in a safety-critical function.

Rationale: To make informed decisions and perform anomaly resolution during a flight, the flight crew or a ground controller requires accurate vehicle health, status, and engineering data. Conducting safety-critical operations without necessary data could result in catastrophic consequences. A safe operation depends on accurate information.

1.4.3 Manual Override of Automatic Functions

The system should allow the flight crew or ground controllers to manually override any automatic safety-critical function, provided the override of the function will not directly cause a catastrophic event.

Rationale: During certain unforeseen events, the capability to manually override automatic functions may prevent serious injury to the occupants. Without this functionality, an automatic function could have an undesirable effect and result in serious injury to the occupants. Engineering judgment and historical events (e.g., engine sensor failure in STS-51F overridden to prevent shutdown) show that this functionality is important and should not be overlooked during the design of the system. As long as an override of an automatic function is feasible and will not directly cause a catastrophic event, the flight crew or ground controllers should have this capability. Allocation of specific override capability to the flight crew, ground controllers, or both, can depend on vehicle design and operations. For example, using manual control during an automated powered flight needs to be assessed against the risk of manual control during powered flight, but the simple override of a sensor may provide flexibility in unanticipated situations.

1.4.4 Detection and Annunciation of Faults

The system should detect and annunciate safety-critical vehicle system faults to the flight crew, within the time necessary for the flight crew to take any action necessary to address the consequences of the fault.

Rationale: To make decisions, and perform anomaly resolution during a flight, the flight crew needs to be alerted whenever a safety-critical system experiences a fault. Without this detection and annunciation, the flight crew would not be aware of the vehicle state of health and would lack insight on whether the flight crew needs to recover a safety-critical system or end the flight early. A detection and annunciation system decreases the cognitive load on the flight crew and allows the flight crew to concentrate on safety-critical operations.

1.4.5 Voice Communication with the Vehicle

The system should provide two-way voice communication between the ground controllers and the flight crew from pre-launch through post-landing occupant egress.

Rationale: Communication between the ground controllers and flight crew is beneficial, as it provides operational insight to the ground and enhances the ability of the flight crew to resolve anomalies should they occur. The intent of this practice is to ensure communications availability during safety-critical operations. Having 100% coverage is not always practical, therefore this practice is not meant to imply continuous communication for all phases of flight. In addition, this practice may not be necessary if there is no one on the ground with safety-critical responsibilities.

Historically, the ascent and reentry phases of human space flight have been the time frame of greatest risk for occupants. Previous space flights have shown that for powered ascent, there are a multitude of

timely systems responses that ground controllers can assist with, leading to the need for communications that can be accommodated by ground or space based communication assets. By contrast, for reentry, due to its dynamic conditions and communications dropouts, the need for continuous communication is less than that for ascent. Safety-critical events during reentry (e.g., separations, parachute deployment, and key navigation events) and the final phase of landing where the risk is the highest may warrant voice communication between the ground controllers and flight crew.

1.4.6 Occupant Communication

The vehicle should be designed such that occupants with a safety-critical role can communicate orally with each other during safety-critical operations.

Rationale: Oral communications is instrumental for effective communications during safety-critical operations. For effective communications, the message must be heard and be intelligible. Loud environments can become a communication barrier, thereby interfering with the message being conveyed. Limiting background noise, intermittent noise, or sound pressure levels helps enable effective voice communication. Providing volume control or noise canceling in an electronic communication device also helps. While noise can be an important barrier to communications, there can also be other barriers, including occupant location and the use of pressure suits. If an electronic communication device is not used, the habitable volume sound levels should be limited to allow for occupant communication.

1.4.7 Views for Flight Crew Operations

For a safety-critical operation requiring an external view by the flight crew, the vehicle should provide a window with a direct, non-electronic, through-the-hull view and the unobstructed field-of-view necessary to perform the operation.

Rationale: Providing a window with a direct, unobstructed field-of-view may be essential for a safety-critical operation, such as landing the vehicle, as well as to maintain flight crew situational awareness and safety. A window provides for a real-world view without technological advances to provide the same capability in a window-less vehicle. Other operations that benefit from this practice, aside from landing the vehicle, include on-orbit vehicle piloting, stellar navigation, and vehicle anomaly detection and inspection. To provide an unobstructed view, window fogging and visual obscurities should be prevented. In the future, windowless vehicles may become prevalent and this practice could evolve to allow for such technological advances.

1.4.8 Inadvertent Actions

No single inadvertent flight crew or ground controller action should result in an event causing serious injuries to occupants.

Rationale: In the unforgiving environment of space flight, an inadvertent flight crew or ground controller action could lead to serious injuries to occupants. Inadvertent actions or errant switch activation could occur due to a number of factors such as limited crew experience, gloved hands, ambiguous procedures, the flight environment (e.g., vibration), a stressed operational environment, and inadvertent bumping of

controls. For example, an inadvertent hatch opening and subsequent cabin depressurization while in the vacuum of space would lead to serious injuries to occupants. Preventing the hatch from opening, in this example, should be part of the vehicle design. In the Space Shuttle, NASA used switch guards, covers, and physically separated controls from other controls to prevent accidental activation.

Accidental activation of commands using a computer display can be prevented with an "arm-fire" mechanism. From the ground controller perspective, using an "arm-fire" method to initiate events could prevent serious injuries to occupants.

1.4.9 Flight Crew Loads

Safety-critical vehicle systems (e.g., switches, knobs, handles) should be designed to withstand intentional flight crew input loads without losing a safety-critical function.

Rationale: This design practice should apply to intentional forces imparted on hardware by a flight crew member as opposed to unintentional or accidental forces (e.g., kicking). Humans may exert high forces when operating controls, such as attempting to open a hatch for emergency egress. The resulting damage to equipment could make it impossible to perform safety-critical operations. Therefore, safety-critical systems should be designed to withstand foreseeable forces exerted by a flight crew member without breaking or sustaining damage that would render the hardware inoperable. This practice also applies to hardware that may be inadvertently used as a mobility aid or restraint.

1.4.10 Instrumentation Displays

Instrumentation should display safety-critical information that is readable in the environment of intended use.

Rationale: Safety-critical information that is displayed in a manner that accommodates varying conditions (e.g., vehicle vibration, sunlight, darkness) decreases the potential for errors. Some factors that should be accounted for when designing instrumentation displays are: the use of color, redundant coding for individuals whose color vision is deficient, luminance, contrast, ambient illumination, resolution, display update rate, vehicle vibration, and viewing angle.

1.4.11 Control of Glare and Reflection

Glare and reflection on windows and displays should not interfere with flight crew performance of safety-critical operations.

Rationale: Internal and external sources of light can create glare or reflections that can interfere with the flight crew's performance of safety-critical operations. The sun, Earth, and any solar arrays, external reflective material, camera lights, and internal habitable volume lighting are just some of the sources that can result in glare or reflections on windows and displays. Glare or a reflection can obscure or distort a display image, thereby creating a distraction for the flight crew.

The design and operation of the vehicle should plan for these vehicle orientations and allow for safe operations by blocking or eliminating glare and reflection. By varying the orientation of a launch or

reentry vehicle, instances in which the sun will shine directly on windows or displays creating glare or reflections can be minimized.

1.4.12 Handling Qualities

The vehicle should be controllable to the extent necessary to allow the flight crew to perform their safety-critical operations.

Rationale: Vehicle handling qualities should be sufficient to allow the flight crew to operate and control the vehicle while performing safety-critical operations. Inadequate vehicle handling qualities could overburden the flight crew with considerable piloting operations, thereby lessening the flight crew's ability to perform safety-critical operations. Handling quality rating systems (e.g., the Cooper-Harper rating scale) are often used to assess vehicle design and flight controllability.

1.4.13 Workload

The flight crew and ground controllers should be able to perform safety-critical operations under expected physical and cognitive workload.

Rationale: Inadequately designed user interfaces tend to increase the physical and cognitive workload of the user. An increase in the physical and cognitive workload may result in errors. It is important to ensure that flight crew and ground controller physical and cognitive workload does not result in errors related to safety-critical operations. In practice, workload assessment tools are used to assess flight crew and ground controller interfaces, operations, workload, and error rates.

1.4.14 Emergency Control Markings

The vehicle should provide clearly marked emergency controls that are distinguishable from non-emergency controls.

Rationale: In an emergency situation, quickly identifying emergency controls and not confusing them with non-emergency controls may prevent serious injury to occupants. Coding helps occupants identify appropriate controls or mechanisms, allowing faster reaction times in an emergency situation. Coding of controls and mechanisms also helps avoid the accidental accessing of an emergency control.

1.4.15 Emergency Equipment Access

The vehicle should be designed such that the flight crew can access equipment involved in the response to an emergency situation within the time required to respond to the hazard.

Rationale: In an emergency situation, having timely access to emergency equipment gives the flight crew an opportunity to address the emergency and increases the likelihood of occupant survival. The design should take into account emergency scenarios requiring access to equipment. The location and proximity of emergency equipment to the flight crew impact accessibility and response time.

1.4.16 Emergency Lighting

For orbital flights, and suborbital flights at night, the vehicle should have:

a. Emergency lighting for occupant egress and operational recovery in the event of a general power failure; and

b. A flashlight, or other personal lighting device, for each flight crew member, readily available at all times.

Rationale: In an emergency situation, emergency lighting aids in survival of the occupants. The emergency lighting system could include unpowered illumination sources that provide markers or orientation cues for occupant egress. A flashlight or other low-cost personal lighting device can assist each flight crew member in a lights-out condition to address an unforeseen or emergency situation.

1.4.17 Emergency Vehicle Egress

The vehicle should be designed to:

a. Allow occupants to visually determine hazards outside the vehicle on the primary egress path without the use of vehicle electrical power;

b. Allow the hatch to be opened without the use of tools, from the inside by a single occupant, and from the outside by ground personnel and rescue personnel;

c. Allow all occupants to physically egress within the time required to avoid a serious injury in the event of an emergency on the ground; and

d. Provide for unassisted egress of the occupants.

Rationale: Ensuring that occupants are able to egress the vehicle to the launch platform or post-landing surface in the event an emergency occurs during the pre-launch or the post-landing timeframe could be essential to allowing them to survive or avoid serious injury during such an event. This practice assumes the occupants are able to function in a 1-g environment.

In an emergency situation:

a. Visual observation of the environment outside the vehicle allows the occupants to determine the conditions or obstructions, such as the presence of fire or debris, and determine if it is safe to egress the vehicle. Visually determining hazards outside the vehicle without needing vehicle electrical power, such as through a window, protects occupants from failure scenarios involving the loss of electrical power.

b. Having a hatch that is operable by a single occupant, without the use of tools, is important in an emergency scenario where the vehicle must be egressed in a timely manner. Lost or damaged tools, preventing the hatch from being opened, could result in a serious injury or fatality. Allowing the hatch to be opened by ground or rescue personnel would help in an emergency situation where occupants are incapacitated or in a deconditioned state.

c. *In an emergency, having an egress path that allows egress of all occupants in enough time to protect from pre-launch and post-landing hazards is necessary to avoid serious injuries or fatalities.*

d. *Unassisted egress is needed in the event that no one is available to assist occupants to avoid serious injuries.*

1.5 System Safety

1.5.1 Safety Management

A safety management approach should be used throughout the system life cycle. This approach should be documented and include:

a. The management decision-making authority, management functions, and safety responsibilities;

b. The severity and likelihood criteria used for assessing risk;

c. The methodology used to make risk-informed safety decisions;

d. The techniques for identifying hazards throughout the life cycle of the system;

e. A method for reviewing and assessing hazards, hazard controls, risk mitigations, verification strategies, and the resultant risk;

f. A process for tracking hazards, risks, mitigation and control measures, and verification activities;

g. A process that ensures the accuracy and validity of any hazard analyses; and

h. The review and disposition of occupant survivability analysis results.

Rationale: The system safety process employs structured applications of system engineering and management principles, criteria, and techniques to address safety within the constraints of operational effectiveness, time, and resources throughout a system's life cycle. Management processes ensure that a coordinated approach is used to identify and assess hazards, and to either eliminate them, mitigate risk, or accept residual risk.

Without a comprehensive and systematic approach to system safety, there exists the potential that the hazards in a system will not be known, understood, and controlled, resulting in an increase in residual risk. Space flight systems intended to fly people are generally very complex. As the number of subsystems increase, designers and operators are challenged with the identification and mitigation of the risks these space flight systems introduce. In a very real sense, complexity hides safety concerns in reams of interlocking documentation, all of which appear to demonstrate that the relevant system is safe.

A system safety program planning process is a means of synchronizing definitions and methods so that engineers, designers, testers, and users all speak the same language regarding risk and its management. Planning allows an organization to better mitigate the effects of complexity, and reduces the perceived complexity of hazard analyses by standardizing the definitions and approaches to be used. The safety management approach ensures that the hazard analyses are valid and current throughout the life cycle of the system and are updated when changes are made to the baseline design, flight rules, flight profile, and operations. Furthermore, the safety management approach ensures that the result of corrective actions from anomalies and mishap investigations are reviewed such that any new hazard controls are implemented to prevent reoccurrence of the anomaly or mishap.

1.5.2 System Safety Engineering

A system safety engineering process should be implemented at the beginning of the development cycle of the system to identify and characterize each hazard, assess the risk to occupant safety, reduce risks through the use of risk elimination and mitigation measures, and verify that risks have been reduced to an acceptable level. Hazard analyses should be continuously updated throughout the life cycle of the system. The process should:

a. Identify and describe hazards and the associated causes, including those that result from:

    1. Component, subsystem, or system failures or faults;
    2. Software errors and operations;
    3. Environmental conditions;
    4. Human errors;
    5. Design inadequacies;
    6. Procedural deficiencies;
    7. Incompatible materials;
    8. Functional and physical interfaces;
    9. Biological sources; and
    10. Interactions of any of the above.

b. Identify and describe each safety-critical system and its function.

c. Identify and describe all safety-critical events.

d. Implement a hazard control strategy that will prevent the occurrence of the hazard, or mitigate the risk to an acceptable level. These hazard controls should include one or more of the following:

    1. Failure tolerance;
    2. Sufficient design margins;
    3. Operating and emergency response procedures;
    4. An environmental qualification and acceptance testing program;
    5. Training or certification;
    6. Operational constraints; and
    7. Monitoring of safety-critical systems.

e. Demonstrate that the hazard controls and risk mitigation measures have been successfully implemented through objective verification evidence. Verification should include one or more of the following:

    1. Test data;
    2. Inspection results;
    3. Analysis; and
    4. Demonstration.

Rationale: Complex systems introduce safety concerns, most of which arise from the interactions of subsystems. These complex interactions cannot be thoroughly planned, understood, anticipated, or guarded against and hence increase the potential for unanticipated harm to the occupant. Hazard analyses address the hazards that arise in the design, development, manufacturing, construction, facilities, transportation, and operations associated with hardware, software, maintenance, operations, and environments. Hazard analysis is a proven engineering discipline that, when applied during system development and throughout the system's life cycle, identifies and mitigates hazards, and in so doing eliminates or reduces the risk of potential mishaps and accidents. The system safety engineering process outlined in this document is consistent with common space industry practice.

1.5.3 Software Safety Engineering

a. Hazards from computing systems and software should be integrated into the safety engineering process as outlined in section 1.5.2.

b. Computing systems and software functions should be considered safety-critical if they:

    1. Are used to control or monitor safety-critical systems;
    2. Transmit safety-critical data, including time-critical data and data about hazards;
    3. Are used for fault detection in safety-critical computer hardware or software;
    4. Respond to the detection of a safety-critical fault;
    5. Compute safety-critical data;
    6. Access safety-critical data;
    7. Are used to model or simulate safety-critical parameters or functions; and
    8. Share hardware resources with safety-critical data, or share command pathways with safety-critical data.

c. A software development process and maintenance approach should be documented and maintained. The process should, at a minimum, include:

    1. Software development methods and standards;
    2. Software design (i.e., architecture, components, modules, interfaces, and data); and
    3. Approach to analyze and certify off-the-shelf software.

Rationale: Space flight systems have become highly dependent upon the use of software. Therefore, software safety analysis should be an integral part of the overall system safety management and engineering process. Software is used to perform complex maneuvers, issue safety-critical commands, monitor and respond to events that could lead to a catastrophic result, and provide data used to make safety-critical decisions. Therefore, software can be a source or a control to hazards. Software system safety is an element of the total safety approach, and is implemented in the software development program to achieve an acceptable level of safety for software and computing systems used in safety-critical applications. The software safety process outlined in this document is consistent with common industry practice.

1.5.4 Occupant Survivability Analysis

An analysis should be conducted to identify what additional equipment or capability, in a catastrophic event, might provide the occupants with an increased chance of survival. The results of the analysis should be documented and include:

a. A description of occupant survivability measures that could be implemented to mitigate risk;

b. A discussion of the relative change in risk to the occupant; and

c. An evaluation of the design impacts.

Rationale: Despite best efforts, hazards may occur during space flight. An occupant survivability analysis is intended to determine if there are design changes that may increase the chances of crew survival in an emergency situation, without creating added risks to the occupants or significantly limit system capability, affordability, or sustainability. Implementation, however, is a function of overall risk the commercial operator is willing to assume verses the cost of implementing a design change or providing additional equipment. The occupant survival strategy is determined by the designer or operator and could include some combination of abort, escape, emergency egress, safe haven, emergency medical, and rescue capabilities throughout a flight.

1.6 Design Documentation

1.6.1 Operational Documentation

Documentation should be developed and kept current that describes how to operate and maintain the vehicle within the limitations and capabilities of the vehicle. At a minimum, this documentation should include the following items:

a. Vehicle and operations overview;

b. Vehicle systems descriptions (hardware and software), functions, and associated hazards;

c. Performance;

d. Mass properties;

e. System limitations;

f. Consumable limitations;

g. Physical and anthropometric limitations on the flight crew or space flight participants;

h. Weather limitations;

i. Landing site limitations;

j. Normal procedures;

k. Emergency procedures;

l. Crash, fire, and rescue procedures;

m. Software and computing system user procedures, operating limitations, and known problems; and

n. Maintenance requirements for hardware and software to ensure continued flightworthiness.

Rationale: To safely operate a space flight system, an operator needs to be provided with a clear understanding of the vehicle and the vehicle's performance capability, operational procedures, limitations, hazards, and maintenance needs so that the vehicle is operated as designed and within its capabilities.

1.6.2 Configuration Management

A process should be implemented that provides configuration control over safety-critical systems design, manufacturing, and operations throughout the system's life.

Rationale: A configuration management process provides evidence that the system was manufactured to, and operated within, the design specification. The process is necessary to maintain the established system design throughout the life cycle of the vehicle. Failure to ensure the system conforms to the established system design can lead to safety-critical failures that could cause a loss of vehicle and occupants.

2.0 MANUFACTURING

2.1 Manufacturing

2.1.1 Quality Assurance

The system should be manufactured, maintained, and operated in accordance with a quality assurance process that ensures the system meets design specifications and safety requirements.

Rationale: Quality assurance processes are essential to ensure that the system manufactured matches the design. Manufacturing to and operating within the design specifications is important because the system safety products reflect the design and operational concepts that were assessed during the life cycle, and any changes to these concepts have the potential to impact occupant safety. When hardware, software, or operational approaches deviate from the system analyzed during the system safety process, it introduces a possibility that hazard controls and mitigation measures may be ineffective, or increases the likelihood that new hazards may be introduced.

2.1.2 Acceptance of Flight Hardware

a. Each safety-critical system should be functionally demonstrated while exposed to no less than its maximum expected operating environment to demonstrate that it is free of defects, free of integration and workmanship errors, and ready for operational use.

b. As an alternative, in-process controls and a quality assurance process can be combined to ensure functional capability of each safety-critical system during its service life.

Rationale: Acceptance testing is a risk mitigation strategy that verifies that the manufacturing and assembly process has been accomplished in an acceptable manner and that the product performs within specified parameters. This practice applies to all vehicle and ground safety-critical systems.

An effective acceptance testing program ensures that the system manufactured is free of defects and free of integration and workmanship errors, and that the system is capable of meeting its performance requirements during its service life. Acceptance testing simulates, as close as possible, the environments of space flight. Acceptance testing typically exposes the system to environmental levels (e.g., vibration, acoustics, thermal, and pressure) no less than the maximum levels that the system is expected to see during its operational lifetime. The minimum environmental test levels and cycles selected are intended to stress the system sufficiently to identify integration and workmanship errors and part defects.

Acceptance testing is intended to be the last step in assuring the quality of each production item. When a manufacturer has demonstrated that the purpose of an acceptance test program has been achieved by in-process controls or other quality management steps, it may be possible to reduce the scope or delete acceptance testing altogether.

2.1.3 Configuration Management

Refer to section 1.6.2

3.0 OPERATIONS

3.1 Management

3.1.1 Flight Operations Authority

An operator should identify lines of communication and approval authority for all safety-critical decisions during pre-flight, flight, and post-landing.

Rationale: Clear lines of communication and approval authority within a program are necessary to avoid confusion and lessen the chance that safety issues will be missed. Clear approval authority for safety-critical flight operations helps ensure that real-time or near real-time safety-critical decisions are made in a timely manner.

3.1.2 Flight Crew Decision Authority

An operator should designate a member of the flight crew who has ultimate decision authority on the vehicle. This flight crew member is responsible for the safe operation of the vehicle and for the safety of occupants.

Rationale: The dynamic nature of space flight often requires safety-critical decisions to be made in a timely manner. Having a member of the flight crew with decision authority for the safety of the vehicle and occupants aids in achieving timely decisions. Designating a flight crew member, independent of ground personnel, is important due to the flight crew's unique situational awareness.

3.1.3 Configuration Management

Refer to section 1.6.2

3.1.4 Quality Assurance

Refer to section 2.1.1

3.1.5 Flight Readiness

Prior to any flight, an operator should assess and document that the system is ready to execute the flight within the design and operational limitations of the system.

Rationale: The likelihood of having a safe flight is enhanced when an operator evaluates the system's readiness. A detailed evaluation of the system prior to flight allows for a final review of items that include the system hardware and software, procedures, and the readiness of personnel. It allows an operator to verify the system meets design and operational requirements, and resolve any open issues before the intended flight. Documenting flight readiness also provides a historical reference for lessons learned and, as an additional benefit, can be useful for post-flight analysis.

3.1.6 Anomaly Investigation, Tracking, and Resolution

a. During flight, an operator should assess any safety-critical anomaly and its effect on continued flight operations.

b. For each anomaly that affects a safety-critical function, an operator should:

    1. Document the anomaly;

    2. Identify the root cause of the anomaly; and

    3. Implement any actions necessary for subsequent safe flight.

Rationale: Assessing the effects of safety-critical anomalies during flight is important to maintain the system in a safe state, if possible, through short term operational constraints or other corrective actions. Examination and understanding of system and subsystem anomalies throughout the life cycle can warn an operator of an impending mishap and can provide important information about what corrective actions need to be implemented to mitigate risk. Anomalies can include failures of hardware, software, procedures, and operations, and human error.

3.1.7 Accident and Incident Investigation

An operator should investigate and document the cause of any accident or incident, and identify and adopt preventive measures for avoiding recurrence of the event prior to the next flight.

Rationale: Continuing to operate a system that has experienced a launch or reentry accident or incident prior to the completion of an investigation, and the adoption of preventive measures, could jeopardize the safety of occupants.

3.2 System Safety

3.2.1 Safety Management

An operator should have a safety management approach as outlined in section 1.5.1, including a process for updating hazards and identifying new hazards based upon design modifications or operational changes.

Rationale: The primary goal of system safety management in the operational phase of the program is to manage risk to acceptable levels. Ideally, the system safety program used in the design phase implemented a hazard control strategy that an operator should utilize prior to, or during, each flight to prevent a known hazard from occurring. When changes are made to the design or operations, the potential exists that new hazards might have been generated. Thus, a process should be in place that continually evaluates the system to ensure a continued acceptable level of risk.

3.2.2 System Safety Engineering

For each design modification or operational change, an operator should:

a. Review all existing hazards and update as necessary to reflect any new causes, mitigations, and changes to overall risk;

b. Implement the system safety engineering processes as outlined in section 1.5.2 and section 1.5.3; and

c. Review and, if necessary, revise the occupant survivability analysis as outlined in section 1.5.4.

Rationale: The accepted risk is predicated on a configuration that was manufactured, qualified, and tested to ensure the system meets expected performance in its operational life. When enhancements or alternate designs are proposed, an operator should have a systematic approach to review the impact of the changes on the overall safety. This engineering process evaluates the specific changes and the impact of the changes on the integrated system to ensure that no new hazards or causes to existing hazards were introduced, and that the existing hazard control strategies are still valid to ensure that the risk is maintained to an acceptable level.

3.2.3 Payload Safety

Prior to each flight, an operator should identify and mitigate payload hazards using the system safety management and engineering approaches outlined in sections 1.5.1, 1.5.2, and 1.5.3.

Rationale: Payloads that are flown either within the pressurized habitable volume or external to a space flight vehicle could fail or adversely interact with the vehicle and expose the occupants to toxic gasses, explosions, or fire. While the system design and operations are analyzed throughout the life cycle to mitigate identified hazards, the wide range of potential payloads that may fly introduces the possibility that a payload might be the source of a catastrophic event.

3.3 Planning, Procedures, and Rules

3.3.1 Operating Within Constraints

An operator should operate the system within the most current documented operating limitations and procedures.

Rationale: Occupants can be put at risk if operations are conducted outside of documented operating limitations or procedures (e.g., on STS-51L, the Space Shuttle Challenger was operated outside its temperature limits, contributing to the loss of vehicle and crew).

3.3.2 Operations Products

All products that are necessary to operate the system, such as plans, procedures, processes, schedules, and supporting information, should be current and consistent with the operating limits of the system.

Rationale: Ensuring that the processes, plans, and procedures are consistent with operating limits of the system reduces the likelihood of a system failure that could potentially lead to a hazardous situation. The use of outdated procedures may result in incorrect operations. Using the current processes, procedures, and supporting data reduces the likelihood that the system operations will introduce new hazards.

3.3.3 Procedures

An operator should have procedures for safety-critical operations that ensure the vehicle is operated within established limits.

Rationale: Safety-critical operations typically require time-critical or sequence-critical actions. Proper documentation, in the form of a procedure, helps ensure that any safety-critical operations are performed in a safe manner. Typically, procedures formalize the steps to execute operations. Procedures can help ensure operations are performed within established limits of the vehicle, and that operations remain consistent with any launch commit criteria and flight rules.

3.3.4 Integrated Operations Coordination

An operator should coordinate all plans and procedures for safety-critical integrated operations among all affected entities.

Rationale: Space flight operations often involve multiple entities, such as a launch vehicle operator, spacecraft operator, launch complex, and landing facility. Conducting integrated operations is challenging. Coordinating all plans and procedures with affected parties helps to minimize confusion and uncertainties, ensures flight safety-critical procedures are completed successfully, and allows individuals with safety-critical decision authority to make sound decisions.

3.3.5 Fatigue Management

An operator should manage flight crew, ground controller, and safety-critical ground operations personnel fatigue through training and duty limitations as follows:

a. Flight crew, ground controllers, and safety-critical ground operations personnel should receive training that makes each of them aware of the signs of fatigue, the effects of fatigue on performance, and fatigue countermeasures.

b. Duty limitations should be applied to flight crew, ground controllers, and safety-critical ground operations personnel to ensure they are physiologically and mentally capable of performing safety-critical operations.

Rationale: Developing rules to manage fatigue is important to ensuring the safety of the occupants aboard a vehicle. This is due in large part to the safety-critical role the flight crew, ground controllers, and safety-critical ground operations personnel have, and the fact that fatigue can cause mistakes that jeopardize the occupants.

a. Training is important to provide the flight crew, ground controllers, and safety-critical ground operations personnel awareness of the many aspects of fatigue, and the ability to identify the appropriate rest periods necessary to allow a return to duty fully capable.

b. *Necessary duty limitations vary based on a number of operational factors that contribute to fatigue. These include the amount of recent sleep, length of duty, starting time, workload, and number of consecutive duty periods.*

3.3.6 Maintenance and Preventative Maintenance

An operator should perform and document maintenance and preventive maintenance for both hardware and software in accordance with the Operational Documentation, outlined in section 1.6.1, to ensure readiness for safe flight.

Rationale: Maintenance and preventative maintenance are important to ensure the system capabilities are retained throughout the system life cycle. The effectiveness of safety systems can often degrade over time and cycles through continued use, exposure to the flight environment, and testing. Failure to maintain those systems that are life limited can lead to system degradation or failure, resulting in a serious injury or fatality. Failing to perform maintenance and preventive maintenance in accordance with the Operational Documentation may cause the vehicle to be operated outside the limitations and capabilities of the vehicle. Maintenance may also be used as controls to a hazard.

3.3.7 Cabin Hygiene

An operator should implement cabin hygiene procedures and processes to prevent occupant exposure to microbial contamination and foreign object debris, which could lead to an incapacitating illness or serious injury.

Rationale: Microbial contamination and foreign object debris could cause incapacitating illness or serious injury, which could prevent the performance of safety-critical operations by the flight crew. The history of human space flight has shown that careful attention to cabin hygiene prior to flight is important, as it is very difficult to clean a cabin of foreign object debris in microgravity. Cabin cleanliness procedures may include inspection criteria, cleaning, disinfecting, and vacuuming the cabin prior to flight, as well as filtering cabin air or cleaning surfaces while in flight.

3.3.8 Launch Commit Criteria and Flight Rules

An operator should document operational rules and criteria that identify the system's condition and the capability that should exist in order to safely ingress the vehicle, begin the flight, remain in flight, reenter (if applicable), and egress the vehicle.

Rationale: Certain events during pre-flight, flight, and post-landing do not afford an operator time to develop a real-time plan to avoid the potential of a serious or fatal injury to an occupant. Predetermined operational rules and criteria, such as launch commit criteria and fight rules, provide an operator with tested and verified steps to maintain a vehicle within its limits. Rules and criteria can be used to provide direction for safety decisions and management of operational risks during a flight.

3.3.9 Communications Protocol

All flight crew, ground controllers, and safety-critical ground operations personnel should adhere to a defined communications protocol when executing safety-critical operations.

Rationale: Executing safety-critical operations using a defined communications protocol helps an operator clearly convey information. The use of proper protocol decreases miscommunication and increases message comprehension.

3.3.10 Consumables

a. For orbital flight, an operator should carry onboard consumable quantities sufficient for the planned flight duration plus 24 hours margin including deorbit, reentry, and post-landing, and maintain the margin throughout the flight. An operator should monitor and maintain the required propellant for a nominal deorbit and reentry.

b. For suborbital flight, an operator should carry onboard consumable quantities sufficient to cover planned flight duration plus margin to account for variables in usage.

Rationale: Having adequate consumable quantities with sufficient margins to address weather conditions, unplanned events, and other events outside the control of an operator is recommended. For orbital flight, having 24 hours of margin is a current practice, allowing time for troubleshooting and crew preparations for landing. By maintaining the consumable margins throughout the flight, an operator would deorbit when any consumable margin is less than 24 hours. Propellant may or may not be used as part of the on-orbit control, however, monitoring and maintaining sufficient propellant to conduct a successful deorbit and reentry is essential to safety.

3.3.11 Landing Sites

An operator should identify a primary and a minimum of one alternate landing site prior to flight and should identify the criteria for determining when a site will be used.

Rationale: The identification of landing sites is necessary for the safe conduct of a flight. Having an alternate landing site protects for scenarios due to issues that may prevent landing at the primary landing site (e.g., unanticipated wind gusts) or vehicle configuration issues. In addition, clear criteria for a landing site's use are necessary because space flight operations are often time-critical.

3.3.12 Collision Avoidance

a. For flights above 150 kilometers, an operator should not launch if the probability of collision with any known orbital object would exceed 1E-6.

b. On-orbit, an operator should perform a collision avoidance maneuver if the probability of collision with any known orbital object exceeds 1E-4.

c. Before maneuvering to a new orbit, an operator should have the orbit screened to ensure the probability of collision with any known orbital object does not exceed 1E-4.

Rationale: Avoiding known orbital objects by delaying a launch or on-orbit maneuver, or maneuvering from a steady-state orbit protects occupants from the potentially catastrophic consequences of a collision.

In the pre-launch time frame, a launch can be delayed to avoid an object that has a high risk of collision with the vehicle. While on-orbit, a higher risk threshold is appropriate because of the relative difficulty and operational impact in making an unplanned on-orbit adjustment. When the risk exceeds the on-orbit threshold, an operator should perform a translational maneuver to eliminate the collision risk. In practice, collision avoidance maneuvers are planned and performed with enough time to screen the new orbit, execute the maneuver, and allow the orbit to change such that the collision probability is no longer violated. Before performing such a maneuver, screening the new orbit for potential collisions would avoid putting the occupants on a collision course with another object.

The collision probabilities match risk levels NASA has accepted for its human missions. The goal is to provide reasonable protection while minimizing operational impacts. For launch, FAA and NASA studies have shown launch availability averages 80% when screening for a collision probability of 1E-6. By adjusting the preferred launch time by a few seconds (15-30 seconds), potential collision can be avoided. On-orbit, predicted collisions vary based on the debris density at the altitude of the vehicle. At International Space Station altitudes, the ISS averages 1 maneuver annually to avoid exceeding the on-orbit collision probability. A smaller vehicle on a 2-week flight would need significantly less.

Calculation of collision probabilities may not be possible, such as for new launch vehicles whose trajectory dispersions are not well characterized. In those cases, a similar level of safety may be achieved by maintaining a predicted miss distance between trajectories. Historical miss distances for launch have been greater than ±8 km x ±30 km x ±30 km (defined in uvw coordinates relative to the vehicle as radial x downtrack x crosstrack), and for on-orbit maneuvers have been greater than ±0.5 km x ±4 km x ±4 km.

Based on an analysis of a catalog of orbiting objects performed by the U.S. Strategic Command for the FAA's Experimental Permit rulemaking, collision avoidance is not needed for flights with a planned maximum altitude less than 150 kilometers, because there are few objects below that altitude.

3.3.13 Early End of Flight

Once a safety-critical function becomes zero failure tolerant, an operator should end the flight as soon as practicable, normally at the next available primary or alternate landing site.

Rationale: Continuing a flight with zero failure tolerance in a safety-critical function may lead to a serious injury or fatality. If in-flight maintenance fails to recover failure tolerance prior to the next landing opportunity, then an operator should end the flight. This practice does not apply to systems whose level of safety has been achieved through design for minimum risk as outlined in section 1.3.1.

3.3.14 Atmospheric Conditions

Refer to section 1.1.1

3.3.15 Food and Water

Refer to section 1.1.2

3.3.16 Body Waste and Vomitus Management

Refer to section 1.1.4

3.3.17 Biological Waste and Wet Trash Management

Refer to section 1.1.5

3.3.18 Probability of No Penetration by Micrometeoroids or Orbital Debris

Refer to section 1.3.10

3.3.19 Control of Glare and Reflection

Refer to section 1.4.11

3.3.20 Emergency Operations Management

An operator should develop and execute a plan to manage system emergencies, including:

a. Launch escape, if applicable;

b. Occupant rescue and recovery;

c. Contacting, and providing necessary vehicle information to, emergency responders to aid in preserving life and treating the injured; and

d. Preservation of data and physical evidence for use in any anomaly or accident investigation.

Rationale: In an emergency situation, an operator will not have time to develop a plan to avoid the potential of a serious injury or fatality. In general, having a plan to manage system emergencies is necessary to successfully address the situation in the time available. For example, a launch escape plan may be necessary depending on the vehicle complexity, flight configuration, and integrated operations taking place during a launch. Contacting and providing key information to emergency responders should allow them to help preserve life and treat injured occupants. Preservation of data and physical evidence is important to help determine the root cause of any anomaly or accident so that it can be prevented in the future.

3.4 Medical Considerations

3.4.1 Flight Crew Medical Fitness for Flight

a. Within 6 months of an orbital space flight, each flight crew member should have a medical examination by a licensed physician board certified in aerospace medicine to

identify any medical condition or physiological change (acute or chronic) that could lead to incapacitation or inability to perform safety-critical operations.

b. Within 12 months of a suborbital space flight, each flight crew member should have a medical examination by a licensed physician board certified in aerospace medicine to identify any medical condition or physiological change (acute or chronic) that could lead to incapacitation or inability to perform safety-critical operations.

c. A flight crew member should not fly if they have a medical condition or physiological change (acute or chronic) that would make them unable to perform safety-critical operations.

d. A flight crew member should not fly if they are taking medication or receiving other medical treatment or intervention that could result in being unable to perform safety-critical operations.

e. Each flight crew member should demonstrate an ability to withstand the stresses of space flight, which may include high acceleration or deceleration, microgravity, decreased barometric pressure, temperature and humidity changes, vibration, and confined physical environment, in sufficient condition to perform safety-critical operations.

Rationale: NASA astronauts are subjected to extensive medical and psychological testing in order to be admitted to the astronaut corps. In addition to regular health checkups throughout their time of service, astronauts receive extensive medical examinations prior to each flight. Besides crew safety, these examinations serve to ensure a medically fit crew will not be cause for an early end of a multi-million dollar space flight mission.

Commercial space flight missions impose similar physical demands on human tolerance. However, the frequency of medical examinations recommended here is based on the necessity for crew and occupant safety rather than mission success. Using this different perspective, an operator should work with licensed physicians trained or experienced in aerospace medicine to develop a medical evaluation program to ensure that those individuals selected for flight crew duty have the physical capability to perform their safety-critical operations. Further, it should be recognized that while a 6- and 12-month period are identified for orbital and suborbital flights, respectively, this frequency may be too low in some cases and too high in others. However, experience in aviation has shown that the medical condition of most aviators will not change so drastically during the validity period of an FAA Class I or II Medical Certificate (6 and 12 months, respectively) that a pilot would be unable to perform their duties for the given type of flight operation.

In the case of commercial space flight, AST considers an additional 6 months before the next medical examination for suborbital flight crew to be acceptable because of the short period of time that the flight will be aloft. An orbital crew could be on-orbit for an extended period of time, resulting in a greater risk

window and the inability to seek a face-to-face medical consultation, should a flight crew member suspect that their medical condition or fitness for flight may have changed.

The primary goal of a medical examination prior to flight should be the detection of significant disorders or diseases that could prevent the flight crew from performing their safety-critical operations. Emphasis is also placed on an individual's response to various forms of stress and to those procedures that might provide information of a predictive nature regarding future health (within either a 6- or 12-month period, as appropriate).

The foundation of any medical evaluation consists of a comprehensive history and a detailed physical examination by a licensed physician trained or experienced in aerospace medicine. Many health disorders, some not suspected by the individual himself, are detected by these means. As some significant abnormalities may not be uncovered by these techniques, additional laboratory, and other diagnostic tools may be used. Despite a normal physical examination, some disease states can remain hidden when the subject is examined in a resting state. Only when the individual is evaluated under conditions that tax the functions of the various organs do the defects appear. Thus, it may sometimes be beneficial to perform dynamic testing as part of the examination.

One of the most prevalent disorders for flight crew is coronary heart disease. This condition is not limited to the aged, but is encountered frequently in the fifth, fourth, or even in the third decade of life. It is of particular significance in aerospace medicine in that it may cause sudden incapacitation or death. Not uncommonly, warning symptoms that may be present for variable periods of time are misinterpreted by the individual and passed off merely as pains, indigestion, muscle soreness, etc. In some instances, there may be no symptoms whatsoever preceding a catastrophic event. History alone cannot be used to detect susceptibility in individuals. Thus, a physician may choose to use the electrocardiogram as a diagnostic aid to determine if permanent damage has been done to the heart muscle.

Additionally, each flight crew member has a duty to assess their own personal fitness for flight to determine if anything has changed that might prevent them from performing their safety-critical operations. Many over-the-counter and prescribed medications can cause impairment to the flight crew. To determine whether a medication can cause impairment, a flight crew member may wish to consult the FAA's Guide for Aviation Medical Examiners website or a licensed physician trained or experienced in aerospace medicine.

Further, AST recommends that each flight crew member demonstrate an ability to withstand the stresses of space flight so as to ensure the flight crew member can perform his or her duties in the environment in which they plan to operate. Past methods for demonstrating this have been through the use of a centrifuge or high-performance aerobatic aircraft. Flights in an aircraft performing parabolic maneuvers that provide periods of microgravity can also be used to demonstrate that a flight crew member can successfully perform their safety-critical operations.

3.4.2 Space Flight Participant Medical Consultation

Within 12 months of their flight, each space flight participant should consult with a physician, trained or experienced in aerospace medicine, to ascertain their medical risks of space flight.

Rationale: Space flight participants that are medically fit to withstand the stresses of suborbital or orbital flight are less likely to suffer a serious or fatal injury, or pose a hazard to other occupants. Consulting with a physician trained or experienced in aerospace medicine will raise a space flight participant's awareness of any medical concerns so that he or she can make an informed decision about his or her own health and the consequences of space flight. Historically, NASA astronauts have received a pre-selection physical followed by periodic medical exams leading up to their flight. AST believes that 12 months is a reasonable period of time between when the consultation occurs and how quickly a medically and physically fit person's medical condition could change.

3.4.3 Health Stabilization and Medical Planning

Prior to flight, operators conducting multi-day orbital flights should:

a. Implement procedures and processes to prevent acute infectious diseases from being manifested during flight, such as through quarantine and social isolation of flight crew and space flight participants;

b. Identify specific types of medical conditions that could result in ending an orbital flight early; and

c. Identify the medical criteria for ending an orbital flight early due to illnesses or medical emergencies.

Rationale: A medical condition or illness could prevent a flight crew member from performing safety-critical operations. An infectious disease could also be spread from a space flight participant to a flight crew member, preventing the crew member from being able to perform his or her duties. Alternatively, the illness of a space flight participant due to an infectious disease could affect the flight crew due to the need to provide medical care.

By planning, an organization can be better prepared to react appropriately in a timely manner to address medical situations. During flight, there is often not enough time to organize subject matter experts to make a decision. Planning, therefore, is vital to ensuring the safety of occupants.

3.5 Training

3.5.1 Safety-Critical Training Requirements and Standards

An operator should establish and maintain training requirements, completion standards, and any currency requirements for flight crew, ground controllers, and safety-critical ground operations personnel.

Rationale: Safety-critical personnel can be sources of or controls to hazards. Improperly completed safety-critical operations could lead to serious injury to occupants. A training program lacking in training requirements, completion standards, and currency requirements could lead to unsafe conditions. A process that maintains requirements, completion standards, and currency requirements will help ensure safety-critical in-flight operations are properly completed.

3.5.2 Safety-Critical Training

a. An operator should ensure that all flight crew, ground controllers, and safety-critical ground operations personnel are trained and qualified to perform their safety-critical functions.

b. An operator should retain completed safety-critical training and qualification records.

Rationale: The use of untrained or improperly trained personnel in safety-critical positions could lead to unsafe operations. A process that qualifies personnel for the operations they may perform will help ensure safety-critical operations will be properly completed. Retaining records helps to ensure completeness of training, verify proficiency, and monitor performance.

3.5.3 Instructor Qualification

An operator should ensure that personnel conducting safety-critical training are qualified in the subject matter and qualified to teach.

Rationale: Safe operations of the system are highly dependent upon the knowledge and experience of the personnel executing safety-critical operations. Instructors need to demonstrate knowledge of the system and the skill set to convey the information such that the personnel execute the necessary steps as required.

3.5.4 Crew Resource Management and Communication

Training for flight crew and ground controllers should include clear definitions of roles and responsibilities, use of a defined communications protocol, and crew resource management techniques.

Rationale: Lack of clarity concerning roles and responsibilities of flight crew and ground controllers, as well as poor communication among the flight crew and ground controllers, can lead to unsafe operations. This is especially true during dynamic, complex, or high stress situations. Crew resource management training helps the flight crew and ground controllers make good informed decisions using all available resources.

3.5.5 Aerospace Physiology Training

Flight crews should receive aerospace physiology training, including:

a. Aerospace environment;

b. Physiology stress factors (environmental, operational, and self-imposed);

c. Aerospace operations;

d. Aerospace medicine; and

e. Aerospace human factors issues.

Rationale: Space flight may have negative effects on human physiology such that crew members can become incapacitated or hindered in their ability to complete safety-critical operations.

Aerospace physiology training provides knowledge required to recognize human limitations in the aerospace environment, the physiological stress factors associated with flying in a zero-gravity environment, and human factor limitations on flight crew and space flight participants. Knowledge of the effects of space flight on the human body has proven to be an effective means of identifying initial conditions that lead to incapacitation or reduced cognitive abilities. Training also provides each individual with basic knowledge of aerospace medicine and operations in order to respond appropriately during these conditions.

3.5.6 Medical Training

Training for flight crews should include the use and location of onboard medical equipment and supplies, and the recognition of when an occupant requires medical attention that exceeds the capability of the flight crew and onboard equipment.

Rationale: Injuries and illnesses to astronauts have been common occurrences, and have included musculoskeletal injuries, abrasions, contusions, lacerations, burns, commonplace illnesses, and a foreign object in the eye. As such, it should be expected that medical injuries and illnesses may be sustained during space flight. Inability to locate or improper use of medical equipment can lead to further incapacitation or the inability to perform safety-critical operations.

Injuries and illnesses may occur that require medical attention that exceeds the capability of the flight crew or onboard equipment. It is important for the flight crew to recognize such injuries or medical conditions in order to take alternative measures to protect occupants, such as an early return to Earth.

3.5.7 Space Flight Participant Training

Prior to flight, an operator should instruct each space flight participant on:

a. The identified hazards of human interactions with the vehicle and other occupants in all phases of flight;

b. Aerospace physiology, commensurate with the expected flight and operational environment; and

c. How to respond to an emergency situation; including -

    1. The use and location of survival equipment,

2. The use and location of fire event detection and fire suppression equipment, and

3. Egress.

Rationale: The limited internal habitable volume of a space flight vehicle may restrict the mobility of occupants, thereby creating situations where a space flight participant can become a source of a hazard. A space flight participant can also be a resource to respond to non-nominal events. Providing instruction to space flight participants on identifying hazards that result from human interactions, how their bodies will react to the space environment, and their expected roles in an emergency situation, will provide them with the operational knowledge required to recognize, avoid, and respond to potential onboard hazards.

3.5.8 Emergency Survival Equipment Training

Training for flight crews should include the use and location of all onboard emergency survival equipment.

Rationale: Inability to locate or improper use of emergency survival equipment can further degrade a non-nominal situation. Training flight crews on the use and location of onboard emergency survival equipment will allow immediate access to the equipment that may be required during extreme conditions and when speed is essential.

C. DEFINITIONS

Abort means to change the ascent trajectory due to a condition in which continued flight would cause an increase in risk to the occupants.

Acceptance Test means any test or inspection conducted on flight components, units, assemblies, subsystems, and systems to demonstrate that flight items are free of defects, latent material deficiencies, and workmanship and integration errors, and are ready for operational use.

Accident means a serious or fatal injury to a space flight participant or flight crew member that occurs during pre-flight, flight, or post-landing.

Alternate Landing Site means a supported landing site to which the vehicle landing can be diverted in the event there is an issue with the vehicle or the primary landing site.

Analysis means a detailed systematic examination of a complex system by breaking it into its component parts to evaluate the interrelationships, or understand the cause-effect relationships. It is generally used when a physical prototype or product is not available or not cost effective. Analysis can include the use of both modeling and simulation.

Anomaly means a problem that occurs during operation of a system, subsystem, process, facility, or support equipment.

Annunciate means to provide a visual, tactile, or audible indication.

Ascent means the period of time from first motion of a launch vehicle until apogee for a suborbital mission, or orbit insertion for an orbital mission.

Automatic means an event that can occur without the need for human intervention.

Catastrophic means the loss of the vehicle, or a serious injury or fatality.

Collision Avoidance Maneuver means a maneuver conducted by an orbiting object to avoid colliding with another object.

Component means an assembly of parts that constitute a functional article viewed as an entity for purposes of analysis, manufacturing, maintenance, or record keeping.

Configuration Control means a process for establishing and maintaining consistency of a system's functional and physical attributes, safety-critical procedures, and operations throughout its life.

Consumable means an item intended to be consumed during space flight operations. Consumable items include, but are not limited to, food, water, propellant for maneuvering or deorbit propulsion, oxygen and other make-up gasses, and stored energy such as electricity. Consumables do not include the necessary fuel, oxidizer, or monopropellant necessary to propel a vehicle into suborbital or orbital flight.

Contaminated Atmosphere means a collection of unwanted airborne solid or liquid particulates and gasses that is mixed into the habitable volume air mass. Contamination is commonly caused as a by-product of a fire or a leak of an enclosed fluid system.

Crew Resource Management means the effective use of all available resources for flight crew interaction and decision-making.

Design means activities leading to the development of final drawings and specification for a system. Design includes tests to verify or validate requirements, models, reliability, and performance.

Design For Minimum Risk means a process that allows safety-critical systems to meet the intent of failure tolerance through robust design, such as factors of safety, high reliability, and other design margin techniques, rather than through redundancy.

Design Reference Mission means a time history or profile of events, functions, and environmental conditions that a system is expected to encounter.

Design Tolerance means a permissible limit of variation in physical dimensions for manufacturing purposes so that performance will not be degraded.

Emergency means an unexpected situation requiring immediate action to protect occupants from serious or fatal injuries.

Escape means removal of occupants from an imminent catastrophic hazard.

Extravehicular Activity means an activity outside of a vehicle's habitable volume performed by an individual using a pressure suit.

Fail Safe means that systems and associated components, considered separately and in relation to other systems, are designed so that the occurrence of any failure condition which would prevent continued safe flight and landing is extremely improbable, and the occurrence of any other failure condition which would reduce the capability of the system or the ability of the flight crew to cope with adverse operating conditions is improbable.

Failure means the inability of a system, subsystem, component, or part to perform its required function within specified limits.

Failure Tolerance means the ability to sustain a certain number of failures and still retain capability. A component, subsystem, or system that cannot sustain at least one failure is not considered to be failure tolerant.

Fatigue (Human) means a physiological state of reduced mental or physical performance capability resulting from lack of sleep or increased physical activity that can reduce a flight crew member's alertness and ability to safely operate a launch or reentry vehicle or perform safety-related duties.

Fault means an undesired system state or the immediate cause of failure. The definition of the term "fault" is broader than the word "failure," because faults include other undesired events, such as software anomalies and operational anomalies. Faults at a lower level could lead to failures at the higher subsystem or system level.

Flight means the period of time beginning at first motion of the launch vehicle and ending when the vehicle arrives on the Earth's surface.

Flight Crew means the personnel within a launch or reentry vehicle identified by an operator and qualified to conduct safety-critical operations during flight.

Flightworthiness means the minimum system capabilities necessary to maintain occupant safety.

Ground Controller means a safety-critical person identified and qualified by an operator to operate or command, directly or indirectly, the vehicle while flight crew or space flight participants are on board.

Habitable Volume means the space within the vehicle's environmentally controlled pressure vessel where human life is sustained.

Hazard means any real or potential condition that can cause a serious or fatal injury to an occupant.

Hazard Control means an attribute of the design, or operational constraint on the hardware or its function, that prevents a hazard or reduces the residual risk to an acceptable level. Design controls include those attributes that improve the robustness of the design. Operational controls include operational constraints as well as flight crew and safety-critical ground operations personnel training to prevent a hazard, lessen the likelihood or severity of a hazard, or to mitigate the effects of a hazard once it has occurred.

Human Factors means the scientific discipline concerned with the understanding of interactions between humans and other elements of a system. Human factors involve applying theory, principles, data, and other methods to a design to optimize human well-being and overall system performance.

Incident means an unplanned event during pre-flight, flight, or post-landing that poses a high risk of causing a serious or fatal injury to a space flight participant or flight crew member.

Induced Environment means the environment that is created as a result of the operation of the vehicle.

In-Process Controls means tests or inspections performed during a manufacturing process for the purpose of monitoring and, if necessary, adjusting the process to assure that the product conforms to its specifications.

Launch Escape System means a system used on launch vehicles to remove occupants from the launch vehicle in the case of an imminent catastrophic hazard.

Life Cycle means all phases of the system's life including design, research, development, test and evaluation, manufacturing, operations and support, and disposal.

Maximum Expected Operating Environment means the maximum environment (including pressure, temperature, vibration, shock, radiation, and loads) that a component, subsystem, or system is expected to experience during its service life.

Mitigation means any action taken to reduce or eliminate the risk from hazards.

Natural Environment means the environment that exists independent of the presence of the vehicle and that is present during the vehicle’s operation.

Nominal means normal operations, that is, all critical systems performing within expected parameters.

Normal Procedure means a procedure that is used during the standard or usual operation of the system. Normal procedures can be part of a checklist or do-list, aid the flight crew or a ground controller in recalling a process, or provide a sequential framework to meet internal and external operational requirements.

Occupant means flight crew or space flight participant.

Occupant Survivability Analysis means an assessment of existing hazards after the vehicle is designed to identify additional capabilities that could be incorporated into the system to preserve the occupant's life in the presence of imminent catastrophic conditions.

Operation means all core activities involved in executing a flight of a launch or reentry vehicle.

Operator means a person or entity that conducts or will conduct the flight of a launch or reentry vehicle carrying humans.

Orbit means a trajectory in which an object can remain in space for at least one revolution of the earth, and has an altitude at perigee above 100 kilometers (62 mi).

Post-landing means the period of time after completion of flight until occupants are no longer exposed to the hazardous conditions from the vehicle.

Pre-flight means the period of time beginning when occupants are exposed to hazardous conditions from the vehicle until flight begins.

Primary Landing Site means a supported landing site that is the intended site for landing.

Qualification means the functional testing of components, units, subsystems, and systems at levels beyond the maximum expected operating environment to prove there is design robustness, and to provide objective evidence that the system will survive the maximum expected operating environment to be experienced during its service life.

Quality Assurance means a system for ensuring a desired level of quality in the development, production, or delivery of products and services.

Residual Risk means the risk left over after risk mitigation measures have been implemented.

Risk means a measure that combines both the probability of occurrence of a hazardous event and the consequence of that event to an occupant.

Safety-Critical means essential to the prevention of serious or fatal injuries to vehicle occupants. A safety-critical system, subsystem, component, condition, event, operation, process, function, fault or item is one whose proper recognition, control, performance, or tolerance is essential to ensuring occupant safety.

Safety-Critical Ground Operations Personnel means any personnel that have a safety-critical role prior to or after a flight. Safety-critical ground operations personnel may include personnel that assist the flight crew in entering the vehicle, closing the hatch, performing leak checks, and working on the integrated space vehicle at the pad during launch operations or landing.

Safety-Critical Penetration means the occurrence of damage to a safety-critical system due to a micrometeoroid or orbital debris that results in loss of vehicle or serious or fatal injury to an occupant.

Serious Injury means any injury which: (1) requires hospitalization for more than 48 hours, commencing within 7 days from the date the injury was received; (2) results in a fracture of any bone (except simple fractures of fingers, toes, or nose); (3) causes severe hemorrhages, nerve, muscle, or tendon damage; (4) involves any internal organ; or (5) involves second- or third-degree burns, or any burns affecting more than 5 percent of the body surface.

Space Flight Participant means an individual, who is not crew, carried aboard a launch vehicle or reentry vehicle.

Supported Landing Site means a site that has an operator's recovery personnel on station at the time of landing.

Subsystem means a group of interconnected and interactive major parts that performs an important task as a component of a system and has the characteristics of a system, usually consisting of several components.

Support Equipment means any non-flight equipment, system, or device specifically designed and developed for a direct physical or functional interface with flight hardware to support the execution of ground production or processing.

System means an integrated composite of subsystems, personnel, products, and processes that when combined together will safely carry occupants on a planned space flight.

System Safety means the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, suitability, time, and cost, throughout all phases of the system life cycle.

Test means a method of verification wherein requirements are verified by measurement during or after the controlled application of functional and environmental stimuli.

Trained means that an individual has received instruction and can demonstrate that he or she can perform or is knowledgeable about the information, skills, or type of behavior that is expected.

Vehicle means that portion of a space flight system that is intended to fly to, operate in, or return from space. This includes any launch vehicle, carrier aircraft, equipment, and supplies, but excludes payloads.

Verification means the activity that establishes acceptable confidence of compliance with specifications.