Federal Aviation Administration

Recommended Practices for Human Space Flight Occupant Safety

Version 2.0

September 2023

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

Record of Revisions

Version	Description	Date
1.0	Baseline version of document	August 27, 2014
2.0	Updated version of the document to incorporate lessons learned from the Commercial Crew program and initial commercial human space flight operations; added extravehicular activity, verification statements, and references.	September 29, 2023

TABLE OF CONTENTS

A. INTRODUCTION 5

1.0 Purpose 5

2.0 Scope 5

3.0 Development Process 6

4.0 Level of Risk and Level of Protection 6

4.1 Level of Risk 6

4.2 Level of Protection 7

5.0 Structure and Nature of the Recommended Practices 8

5.1 Categories 8

5.2 Performance and Process Based Practices 11

5.3 Depth and Breadth of Practices 11

5.4 Verification Statements 11

5.5 References 11

5.6 "System" vs. "Vehicle" 11

6.0 Notable Omissions 12

6.1 Medical Limits for Space Flight Participants 12

6.2 Ionizing Radiation 12

6.3 Integration of Occupant and Public Safety 13

7.0 Future Versions 13

B. Recommended Practices for Human Space Flight Occupant Safety 14

1.0 GENERAL RECOMMENDATIONS 14

1.1 Integration of Cybersecurity Best-Practices in Design, Manufacturing, and Operations 14

1.2 Development and Use of Consensus Standards for Occupant Safety 15

1.3 Configuration Management 15

2.0 DESIGN 16
2.1 Human Needs and Accommodations 17
2.2 Human Protection 22
2.3 Flightworthiness 32
2.4 Human/Vehicle Integration 42
2.5 Extra Vehicular Activity 55
2.6 System Safety 59
2.7 Design Documentation 63
3.0 MANUFACTURING AND MAINTENANCE 64
3.1 Quality Manufacturing 65
3.2 Lifecycle Risk Sustainment 66
3.3 System Maintainability 67
3.4 Manufacturing Facilities 68
4.0 OPERATIONS 69
4.1 Management 69
4.2 System Safety 73
4.3 Planning, Procedures, and Rules 74
4.4 Medical Considerations 85
4.5 Training 91
5.0 DEFINITIONS 96

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) recommends for commercial human space flight occupant safety. The document is intended to create 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 several 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.

AST is issuing Version 2 of this document because significant progress has been made in the commercial human space flight industry since 2014, the year Version 1 was issued. SpaceX, via its Dragon capsule, is regularly conducting orbital flights to the International Space Station under contract with the National Aeronautics and Space Administration's (NASA's) Commercial Crew Program, as well as private orbital flights. Virgin Galactic has successfully taken people on a suborbital flight from Spaceport America. And Blue Origin is regularly launching passengers on suborbital flights from its site in West Texas.

This version of the document incorporates lessons learned from the Commercial Crew program and recent space flight participant orbital and suborbital flights. AST added verification statements and references for each recommended practice, to give operators an idea of what could be produced as measurable evidence to meet each recommendation.

This document is not regulatory and does not have the force and effect of law. These recommended practices are not meant to bind the public in any way and the document is intended only to provide information to the public.

2.0 Scope

The scope of this document includes suborbital and orbital launch and reentry vehicles. Extravehicular activity is also included in the current version of this document. Future versions of this document may cover additional human space flight operations and missions.

The recommended practices in this document cover the safety of occupants only, that is, flight crew, government astronauts, and space flight participants. This document refers only to flight crew and space flight participants. A government astronaut's role will likely resemble either

flight crew or space flight participant. 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

Sixty years of human space flight have provided AST with a wealth of information to use in developing this document. In the development of Version 1 of the Recommended Practices, AST reviewed existing government and private sector requirements and standards, including those from 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. 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 to capture safety practices and judge whether they are, at a general level, appropriate for the commercial human space flight industry.

The updated recommended safety practices have been vetted with a wide audience, including NASA and the FAA's Civil Aerospace Medical Institute (CAMI). NASA was extensively involved in this update by incorporating lessons learned from the Commercial Crew Program and Suborbital Crew (Sub-C) Program. AST worked closely with CAMI and a NASA flight surgeon team on space flight medical issues related to human space flight safety.

4.0 Level of Risk and Level of Protection

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 address occupant safety considerations throughout the life cycle of a space flight system, and assure that occupants are not exposed to avoidable risks.

[1] Specifically, Crew Transportation Technical Management Processes, CCT-PLN-1120; ISS Crew Transportation and Services Requirements Document, CCT-REQ-1130; and Crew Transportation Operations Standards, CCT-STD-1150.

4.2 Level of Protection

Three levels of protection 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 level is below the level of comfort that most space flight participants would want to experience.[2]

Second, the level of protection 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 to move their arms to perform a safety-critical operation, then an increased level of protection 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 protection applies to emergencies. In emergencies, occupants should have a reasonable chance of survival. Several recommended practices in this document address emergencies and are listed in Table 1.

[2] 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 protection through the end of flight.

Table 1: Practices Addressing Emergencies

Recommended Practice	Section
Terrestrial Emergency Survival Equipment and Supplies	B.2.1.6
Emergency Response to Contaminated Atmosphere	B.2.2.9
Emergency Response to Loss of Cabin Pressure Integrity	B.2.2.10
Emergency Response – Abort and Escape	B.2.2.11
Emergency Occupant Location Post-Landing	B.2.3.13
Emergency Communication with Rescue Personnel	B.2.3.14
Emergency Control Markings	B.2.4.14
Emergency Equipment Access	B.2.4.15
Emergency Lighting	B.2.4.16
Emergency Vehicle Egress	B.2.4.17
Occupant Survivability Analysis	B.2.3.15
Emergency Training	B.4.5.9
Emergency Operations Management	B.4.5.10

5.0 Structure and Nature of the Recommended Practices

5.1 Categories

The recommended practices are divided into four categories: general, 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 addresses safety concerns in an integrated fashion over the entire life cycle of a system.

These categories are further broken down into subcategories, as shown in Figure 1.

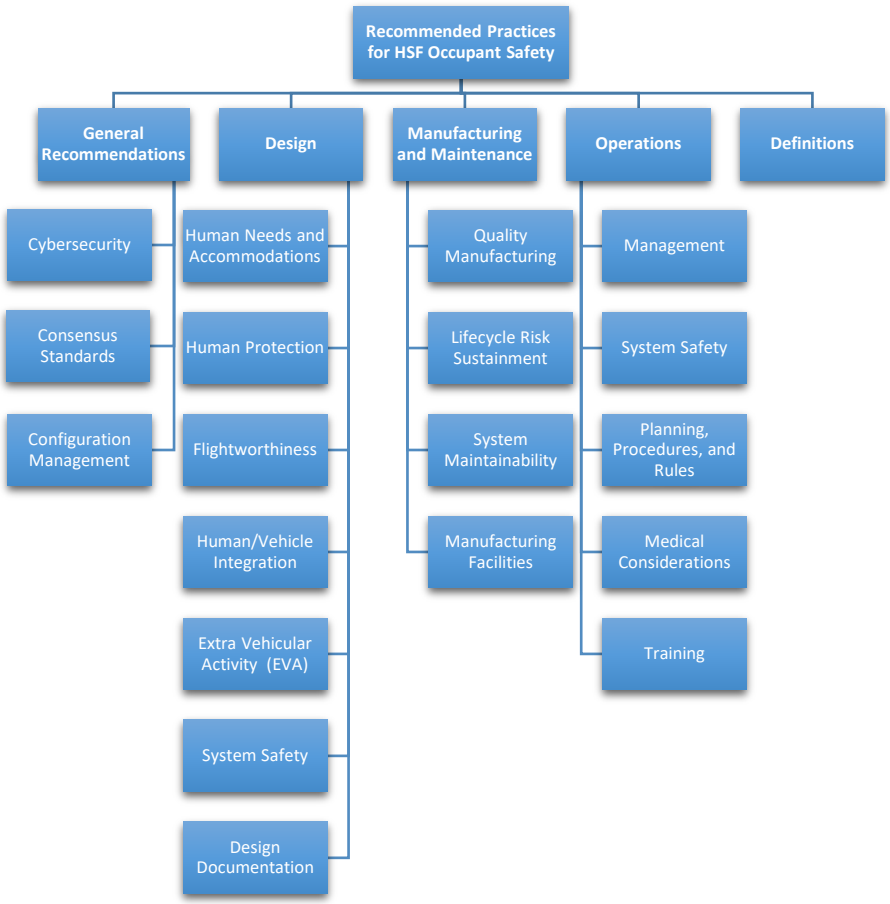

Figure 1: Framework of Recommended Practices

The subcategories are defined as follows:

General Recommendations

Includes overarching recommendations that are applicable to all phases of a human space flight system—design, manufacturing, and operations. These recommendations include cybersecurity, consensus standards, and configuration management.

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 occupants and sufficient for occupants to execute their duties.

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.

Extra Vehicular Activity – This subcategory includes considerations for designing a system that includes extra vehicular activities.

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.

Manufacturing & Maintenance

Quality Manufacturing – This subcategory includes the specifications and systematic efforts for manufacturing, including quality assurance, acceptance testing, and configuration management to address performance, design, reliability, and maintainability requirements and expectations.

Lifecycle Risk Sustainment – This subcategory includes the process of managing the lifecycle of a product, from creation through end of life.

System Maintainability – This subcategory includes the processes to address maintainability (the probability of performing a successful repair action within a given time) measures the ease and speed with which a system can be restored to operational status after a failure occurs.

Manufacturing Facilities – This subcategory includes instructions on how to maintain buildings and structures, including machinery and equipment, where manufacturing of tangible goods or materials or the processing of such goods or materials by physical or chemical change takes place.

Operations

Management – This subcategory includes program controls necessary for 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 safely 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 Atmospheric Conditions, 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.

Several 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 practice. Such details may be better addressed in industry standards.

5.4 Verification Statements

This document now addresses how a designer or operator would verify that it meets each safety measure. The verification statements provide a method for the operator to verify the recommended practice is implemented.

5.5 References

Where applicable, references or supporting material are provided as an additional resource. All references in this document are publicly available and provide a resource to supplement the recommended safety practices.

5.6 "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 accomplish a function and will safely carry occupants on a planned space flight.[3]

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

An example of the use of "system" is found in section B.2.3.1, 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, B.2.3.3, 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 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 specific 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 help prevent them from endangering other occupants.

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.

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 exposure is an inherent risk of space flight. An operator can minimize occupant exposure to radiation

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

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 Future Versions

AST will continue to improve these recommended practices and verifications by incorporating lessons learned gained either from feedback we receive or from industry experience.

B. Recommended Practices for Human Space Flight Occupant Safety

1.0 GENERAL RECOMMENDATIONS

This section consolidates recommendations that apply across all three areas of design, manufacturing, and operations of a human space flight system. These recommendations are over-arching tenants of robust and safe human space flight.

1.1 Integration of Cybersecurity Best-Practices in Design, Manufacturing, and Operations

System owners and operators should develop and implement cybersecurity measures for their systems that incorporate capabilities to ensure protection against unauthorized access to critical vehicle functions.

a. The design, manufacture, and operation of the system should protect against unauthorized access to system functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats throughout the flight.

b. The operator or other part of the system should have the capability to retain or recover positive control of the vehicle.

Rationale: Space systems are reliant on information systems and networks from design conceptualization throughout flight. Further, the transmission of command and control and mission information between space vehicles and ground networks relies on the use of radiofrequency-dependent wireless communication channels. These systems, networks, and channels can be vulnerable to malicious activities that can deny, degrade, or disrupt human space flight operations.

Verification Statement: Cybersecurity measures should be verified by documentation of mitigations in design, manufacturing, and operation of integrated systems. The verification is successful when cybersecurity measures demonstrate the ability to mitigate attacks.

References:

- Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems
- 32 CFR Part 236 – Department of Defense – Defense Industrial Base Cyber Security Activities
- NIST Interagency Report 8270 – Introduction to Cybersecurity for Commercial Satellite Operations

1.2 Development and Use of Consensus Standards for Occupant Safety

Operators should support the development and use of voluntary consensus standards in support of human space flight occupant safety. The use of consensus standards which have been developed and are found to conform to best practices can recognize time and financial savings.

Rationale: The National Technology Transfer and Advancement Act (NTTA) directs Federal agencies to adopt voluntary consensus standards whenever possible. Additionally, the Office of Management and Budget's (OMB) Circular A-119 promotes agency participation in the development of standards.

OMB A-119 guides Federal agencies to use voluntary consensus standards from the private sector where they meet agency needs, rather than creating government-unique standards for acquisition and regulatory purposes. The use of industry consensus standards is further supported in Title 51-NATIONAL AND COMMERCIAL SPACE PROGRAMS, CHAPTER 509-COMMERCIAL SPACE LAUNCH ACTIVITIES.

Verification Statement: Industry use of voluntary consensus standards should be verified by review or audit of human space flight operations incorporating industry developed, voluntary consensus standards.

The verification should be considered successful when the audits can define industry use of consensus standards supporting safety and regulatory paradigms, and enhancing commercial space safety frameworks.

Reference:

- Title 51-National and Commercial Space Programs, Chapter 509-Commercial Space Launch Activities
- OMB A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities
- National Technology Transfer and Advancement Act (NTTA)

1.3 Configuration Management

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

The designer, manufacturer, maintainer, and operator should establish, implement, and maintain a configuration management process that includes the following:

a. Configuration management planning,

b. Configuration identification,

c. Change control,

d. Configuration status accounting, and

e. Configuration audit.

An operator should also ensure that the configuration identification, configuration change control, configuration status accounting, and configuration audits of the functional and physical configuration (i.e., validation and distribution) are unique to the vehicle being manufactured.

Rationale: A configuration management process provides evidence that the system was manufactured to, and operated within, the design specification. The process would 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.

Configuration management ensures that product functional, performance, and physical characteristics are properly identified, documented, validated, and verified to establish product integrity; that changes to these product characteristics are properly identified, reviewed, approved, documented, and implemented; and that the products produced against a given set of documentation are known.

Verification Statement: Configuration management should be verified by inspection. The verification should be considered successful when inspection shows alignment of safety-critical systems design, manufacturing, maintenance, and operations throughout the system's life.

Reference:

- Systems and software engineering - System life cycle processes (ISO/IEC/IEEE International Standards 15288:2023)
- ISO 10007:2017 - Quality management – Guidlines for configuration management
- MIL-HDBK-61B – Configuration Management Guidance

2.0 DESIGN

This section includes design recommendations, including, testing and demonstration, so that the design of the system supports safe human space flight.

2.1 Human Needs and Accommodations

2.1.1 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 in nominal and off-nominal situations.

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 or prevent other occupant duties in case of an emergency, 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 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.

Verification Statement: The ability of the Environmental Control and Life Support System (ECLSS) to provide adequate atmospheric conditions should be verified by analysis and demonstration. The verification should be considered successful when testing in its simulated or operational environment shows the ECLSS provides acceptable atmospheric conditions.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1), Chapter 6.2, Internal Atmosphere
- ISS Crew Transportation and Services Requirements Document, CCT-REQ-1130
- ISS Safety Requirements Document (SSP 51721), Chapter 4.7.1.1, Flammable Materials
- Designing for Human Presence in Space: An Introduction to Environmental Control and Life Support Systems (ECLSS), NASA Reference Publication 1324, with update – Historical ECLSS for U.S. and U.S.S.R./Russian Space Habitats
- Spacecraft Maximum Allowable Concentrations for Airborne Contaminants (JSC 20584)
- Guiding Requirements for Designing Life Support System Architectures for Crewed Exploration Missions beyond Low Earth Orbit, Jay L. Perry, Miriam J. Sargusingh, and Nikzad Toomarian, AIAA

2.1.2 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.

Verification Statement: The adequacy of handling, storage, and dispensing of food and water should be verified by inspection, analysis, and demonstration. The verification should be considered successful when the analysis and demonstration show that food and water handling, storage, and dispensing meet accepted standards for consumption.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1), Chapter 7.2.3.1.2, Contamination

- Advanced Life Support Requirements Document (JSC-38571), Section 3.9, Food Quality Standards

- Space Food Systems Laboratory Shelf-Life Analysis Operations Guideline (SFSL-004)

2.1.3 Occupant Rest

a. For orbital flight, the vehicle should provide accommodations and an environment for occupant sleep. The environment should allow for proper isolation of resting occupants for the duration of assigned sleep cycles.

b. Space flight participant rest should not interfere with flight crew rest.

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

Verification Statement: Adequacy of occupant rest accommodations should be verified by analysis of the vehicle design. The verification could be considered successful when the analysis shows that occupant rest accommodations provide a reasonable environment that allows proper isolation for the duration of assigned sleep cycles.

Reference:

- NASA Space Flight Human-System Standard, Volume 1: Crew Health (NASA-STD-3001, Volume 1, Revision B)

- NASA Space Flight Human-System Standard, Volume 2: Human Factors, Habitibility, and Environmental Health (NASA-STD-3001, Volume 2, Revision C)

2.1.4 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.

Verification Statement: The adequacy of the waste management system to operate in orbit without causing a serious injury or to allow safety-critical operations to be performed should be verified by testing and demonstration in its simulated or operational environment. The verification should be considered successful when the performance analysis and demonstration of the system to manage body waste and vomitus show that the design meets accepted standards, or other approved means of compliance.

Reference:

- NASA STD 3001 Vol 2 NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health, Section 7.3 Body Waste Management
- Manual of Naval Preventative Medicine, Chapter 2 – Sanitation of Living Spaces and Related Service Faculties

2.1.5 Biological Waste, Wet and Dry Trash Management

For orbital flight, the system should manage biological waste and wet and dry 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 or dry 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 or dry trash contents could damage equipment, injure occupants, or transmit disease.

Verification Statement: The adequacy of the waste management system should be verified by analysis and simulation or demonstration. The verification should be considered successful when the analysis and simulation or demonstration show that the design protects all occupants from serious injury and health hazards, safely and sanitarily stows the waste, and does not hinder nominal and safety critical operations.

Reference:

- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / SSP 50005), Paragraph 10.3.3.1, Defecation and Urination Facilities Design Requirements

- Army Training Circular (TC) No. 4-02.3 – Field Hygiene and Sanitation

2.1.6 Terrestrial 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 or exposure protection;

e. Flotation device;

f. Food;

g. Signaling equipment;

h. Navigation; and

i. Survival tools for all probable environments.

Rationale: In a post-landing 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 and areas of extreme heat.

Verification Statement: The adequacy of the emergency survival equipment should be verified by inspection and analysis of the spacecraft design and occupant survival training plans. The verification should be considered successful when the analysis shows that the emergency survival equipment, supplies, and instructions are readily accessible to support occupant needs while awaiting rescue.

Reference:

- FAA Civil Aerospace Medical Institute Basic Survival Skills for Aviation, https://www.faa.gov/pilots/training/airman_education
- NASA-STD-3001 Human Factors, Habitability, and Environmental Health, Vol. 2, Rev. C
- Space rescue - NASA technical reports server (NTRS). NASA. https://ntrs.nasa.gov/citations/20070025530

2.2 Human Protection

2.2.1 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 abort, 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.

Verification Statement: The vehicle's ability to stay below the acceleration limits of different phases of flight for nominal missions and planned contingencies should be verified through analysis and demonstration. The verification should be considered successful when analysis and demonstration show that the countermeasures protect occupants from exposure to transient and sustained linear and angular acceleration.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1), Chapter 6.5, Acceleration
- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / SSP 50005), Section 5.3, Acceleration

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Appendix H, Acceleration Limits

2.2.2 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 or sustained vibration can increase the risk of occupant incapacitation, or a serious injury or fatality. Excessive or sustained 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.

Verification Statement: The vehicle's ability to limit occupant exposure to vibration should be verified by analysis, demonstration, and testing such as from vibration tests or full integration tests. The analysis should use a validated simulation to identify and assess bounding acceleration cases including guidance, navigation and control, and vehicle and environmental dispersions. The verification should be considered successful when the analysis and demonstration show that vibration levels do not incapacitate occupants, decrease occupant duty performance, or cause serious injury to occupants.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1)
- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraph 3.10.5.1.1, 24-Hour Noise Exposure Limit
- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / SSP 50005), Section 5.5, Vibration

2.2.3 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. Ultraviolet-A and Ultraviolet-B radiation have damaging effects on exposed soft tissues, such as skin and eyes.*

Note: Not all parts of the vehicle must be able to protect occupants from high radiation events; the vehicle design should identify an accessible section of the vehicle that provides sufficient protection for radiation environments.

Verification Statement: The vehicle's ability to reduce the interior radiation levels (from expected environments) to acceptable amounts based on the operator's documented analysis should be verified by inspection, demonstration, and testing. The verification is considered successful when the operator can demonstrate differential shielding amounts within the vehicle such that occupants can shelter in more heavily shielded sections to endure temporary high radiation events.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1), Chapter 6.9, Non-Ionizing Radiation
- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / SSP 50005), Section 7, Health Management and Paragraph 5.7.3, Nonionizing Radiation
- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Appendix I, Radiation

2.2.4 Noise Exposure Protection

The vehicle should be designed to limit occupant exposure to noise such that occupants are protected from significant hearing impairment and safety-critical operations can be performed successfully. The vehicle should be designed such that noise limits within the vehicle are within the National Institute for Occupational Safety and Health (NIOSH) Recommended Exposure Limits.

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.

Verification Statement: The vehicle's ability to limit occupant exposure to noise should be verified by analysis, testing, and demonstration. The verification is considered successful when the analysis, testing, and demonstration show the vehicle's design protects occupants from significant hearing impairment.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1, 2014), Chapter 6.6, Acoustics
- ISS Safety Requirements Document (SSP 51721), Chapter 4.9.1, Acoustics
- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / Section 5.4, Acoustics
- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraph 4.3.10.5.1.1, 24-Hour Noise Exposure Limit

2.2.5 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: Consideration of the items below will enhance safety and 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. ***Moving parts*** *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. ***Stored potential energy*** *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. ***Burrs*** *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. ***Sharp edges*** *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. ***Sharp items*** *Functionally sharp items (e.g., syringes, scissors, and knives) are intentionally sharp and should be prevented from causing serious injury when not being used for their intended purpose.*

h. ***Temperature*** *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.*

Verification Statement: The vehicle's ability to protect occupants from mechanical hazards should be verified by analysis, testing, and demonstration. The verification is considered successful when analysis, testing, and demonstration show that mechanical hazards are identified and mitigated.

References:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1), Chapter 9.12, Safety Hazards
- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / SSP 50005), Paragraphs 6.3, Mechanical Hazards, and 6.5.3, Touch Temperature Design Requirements

2.2.6 Orthostatic Protection

Orthostatic intolerance countermeasures should be provided to the extent necessary for occupants to perform safety-critical operations. Countermeasures should include anti-orthostatic garments or G-suits, medications, oral fluids, or salt loading prior to landing.

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. These symptoms 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, an occupant 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.

Verification Statement: The incorporation of orthostatic intolerance countermeasures within the vehicle's design should be verified by analysis, testing and demonstration. The verification is considered successful when analysis, testing, and demonstration show that the provided orthostatic intolerance countermeasures protect against serious injury.

References:

- NASA Space Flight Human-System Standard, Volume 2: Human Factors, Habitability, and Environmental Health (NASA-STD-3001, Revision C)
- NASA-STD-3001 Technical Brief - OCHMO-TB-019 Orthostatic Intolerance, Rev A

2.2.7 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, flight duration, and the number of occupants.

Rationale: Injuries to occupants have occurred during space flights, 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 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.

Verification Statement: The availability of first aid supplies and medical equipment during spaceflights should be verified by inspection. The verification is considered successful when proper supplies and medical equipment are available in the vehicle so that occupants can treat injuries or use during medical emergencies. The verification is also considered complete when periodic testing and inspection of medical equipment is conducted by the operator.

Reference:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Appendix J, Reference NASA-Provided Supplies
- NASA-STD-3001 – Crew Health, Vol. 1, Rev C
- G. Starr Schroeder, Jessica C. Clark, Dr. Michael Gallagher, Dr. Shawna Pandya. Medical guidelines for suborbital commercial human spaceflight: A review

2.2.8 Fire Event Detection and Fire Suppression

a. The system should have the ability to detect a fire event 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.

Verification Statement: The spacecraft's fire event detection and fire suppression for the enclosed or isolated areas in the pressurized volume should be verified by analysis, testing, and

demonstration. The verification should be considered successful when the analysis, testing, and demonstration show that a fire in the enclosed or isolated areas in the pressurized volume can be detected and suppressed before it can propagate. In addition, where applicable, human senses such as sight and smell can be used to detect smoke or a fire.

Reference:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraphs
    - 3.2.5.9, Fire Detection in Habitable Cabin
    - 3.2.5.5, Portable Fire Suppression
    - 3.2.5.7, Fire Detection and Suppression in Isolated Areas
    - 4.3.2.5.7, Fire Detection and Suppression in Isolated Areas
- Gary A. Ruff, David L. Urban, Daniel L. Dietrich. Spacecraft Fire Safety Technology Development Plan for Exploration Missions

2.2.9 Emergency Response to Contaminated Atmosphere

In order to respond to a contaminated atmosphere including from fire, 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.

For an emergency response to any contaminated atmosphere, the equipment and provisions should:

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

b. Provide voice communication between the occupants and the ground controllers; and

c. Provide voice communication between the occupants.

Rationale: In an emergency, 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 occupants 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 occupants to manage the emergency.

The ability to verbally communicate with the ground while wearing emergency gear provides the occupants 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.

Verification Statement: The spacecraft's ability to supply a contingency breathing apparatus whenever the cabin atmosphere may be contaminated should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis show that the contingency breathing apparatus provides each occupant a safe individual breathing mask to provide protection and breathable atmosphere until acceptable carbon monoxide, hydrogen cyanide, and hydrogen chloride levels have been re-established. The capability for occupants to communicate with each other and with ground controllers while wearing contingency breathing apparatus should be verified by demonstration. The verification should be considered successful when the demonstration shows that voice communications exist between occupants and with ground controllers while wearing the contingency breathing apparatus under expected ambient noise levels.

Reference:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraphs 4.3.2.5.2, Breathing Mask, and 4.3.2.5.3, Voice Communication in Breathing Apparatus.
- NASA-STD-3001 – NASA Space Flight Human System Standard Volume 2: Human Factors, Habitability, and Environmental Health. Rev C.

2.2.10 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 the occupants and serious injury of occupants by providing:

a. Enough pressurant gases to maintain cabin pressure;

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

c. For missions with time permitting, a contingency breathing apparatus whenever an unplanned reduction in cabin pressure occurs until occupants are in a fully functioning pressure suit or at an altitude where the breathing apparatus is no longer needed.

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 humans 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.

Verification Statement: The vehicle's design to prevent incapacitation of occupants and to prohibit serious injury from loss of cabin pressure should be verified by inspection and analysis. The verification is considered successful when analysis shows the contingency breathing apparatus provides each occupant environmental protection and breathable atmosphere until the end-of-flight or until occupants are in a fully functioning pressure suit in case of an unplanned reduction in cabin pressure. Further demonstration of the vehicle's ability to protect each occupant from a depressurized cabin during ascent and entry is also considered satisfactory verification. The verification is successful when the environmental control and life support system tests confirm that the system(s) operates at the required limits.

Reference:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraphs 4.3.2.5.2, Breathing Mask, and 4.3.2.5.10, Protection from Cabin Depressurization.
- NASA-STD-3001 – NASA Space Flight Human System Standard Volume 2: Human Factors, Habitability, and Environmental Health. Rev C

2.2.11 Emergency Response – Abort and Escape

The system should provide the capability to abort, escape, or both, during pre-flight and ascent, and where practical, during reentry, descent, and landing.

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, descent, and landing, or by the removal of the occupants from the portion of the space flight system normally used for reentry, descent, 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.

Verification Statement: The vehicle's abort capability should be verified by testing and analysis to demonstrate controllability, no near-field re-contact with the launch vehicle or ground infrastructure, operation within hardware thermal constraints, human capability constraints,

structural loads limits, and ability to achieve acceptable landing. The verification is considered successful when the emergency response capability shows the acceptable performance of the abort detection, logic, and abort flight systems (as applicable). The verification is also considered successful when analysis demonstrates accurate 6DOF simulations, including appropriate modeling of all systems affecting abort dynamics, along with their uncertainties, and the Monte Carlo simulations show the spacecraft's entire abort trajectory from abort initiation through landing location or achievement of a stable orbit (for abort to orbit cases).

References:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Section 4.3.3.1, Pad and Ascent Aborts, and 4.3.5.2.1 Emergency Entry Capability
- Crew Transportation Technical Management Processes (CCT-PLN-1120), Section 4.2, System Safety and Reliability

2.3 Flightworthiness

2.3.1 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.

Failure tolerance should apply 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.

Verification Statement: The system's ability to control hazards that can lead to catastrophic events should be verified by documentation, analysis, and demonstration. The verification should be considered successful when analysis and demonstration show at least single failure tolerance or an equivalent level of safety.

Reference:

- ASTM F3479-20, Standard Specification for Failure Tolerance for Occupant Safety of Suborbital Vehicles
- NPR 8705.2C - Chapter 3. Technical Requirements for Human-Rating. NASA

2.3.2 Limitations on Failure Tolerance

The system should provide failure tolerance capability without relying on time-consuming or potentially dangerous crew intervention, including:

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 or 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.

Verification Statement: The system's ability to provide failure tolerance capability should be verified by analysis, simulation, or demonstration. The verification should be considered successful when analysis, simulation, and demonstration show that the failure tolerance does not

rely on extravehicular activity, in-flight maintenance of safety-critical equipment under time-critical situations, using emergency equipment, or using a launch escape system.

Reference:

- Procedural Handbook for NASA Program and Project Management of Problems, Noncomformances, and Anomalies (NASA-HDBK-8739.18)
- NPR 8705.2C - Chapter 3. Technical Requirements for Human-Rating. NASA

2.3.3 Separation of Redundant Systems

The design of the vehicle should separate or protect redundant safety-critical systems and subsystems such that an unexpected event that damages one system does not inhibit the other systems' 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.

Verification Statement: The separation of redundant safety-critical systems should be verified by analysis or simulation. The verification should be considered successful when analysis or simulation show that probable failure modes will not cause redundant systems to fail with the related primary system.

Reference:

- Survivability of Systems (AC 25.795-7), Federal Aviation Administration
- NPR 8705.2C - Chapter 3. Technical Requirements for Human-Rating. NASA

2.3.4 Isolation and Recovery 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.

Verification Statement: The system's ability to detect and isolate faults in safety-critical systems should be verified by analysis and demonstration. The verification should be considered successful when analysis and demonstration show fault detection, isolation, and recovery for each safety critical system while in flight configuration.

Reference:

- Innovative Fault Detection, Isolation and Recovery Strategies On-Board Spacecraft: State of the Art and Research Challenges, A. Wander & R. Förstner, Bundeswehr University Munich, Institute of Space Technology and Space Applications, Document ID: 281268, 2012
- NPR 8705.2C - Chapter 3. Technical Requirements for Human-Rating. NASA

2.3.5 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.

Verification Statement: The vehicle's structural design should be verified by analysis and testing. The verification should be considered successful when analysis and testing show that the vehicle can withstand the maximum predicted operating environments with sufficient margins.

References:

- Structural Design and Test Factors of Safety for Space Flight Hardware (NASA-STD-5001B)
- Structural Design Requirements and Factors of Safety for Space Flight Hardware (JSC 65828B)
- Loads and Structural Dynamics Requirements for Space Flight Hardware (JSC 65829)
- AFSPCMAN 91-710 Volume 3, Chapter 12 and Attachment 2

- Strength and Life Assessment Requirements for Liquid Fueled Space Propulsion System Engines (NASA-STD-5012)

2.3.6 Electrical Systems

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

a. Prevent electrical shock hazard to occupants,

b. Fail safe to protect safety critical electrical equipment,

c. Prevent the generation of molten material,

d. Provide circuitry protection,

e. Prevent electrical wires from overheating, and

f. 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 put at risk.

Verification Statement: The vehicle's electrical circuitry and power distribution should be verified by analysis and testing. The verification should be considered successful when analysis and testing show that the electrical system prevents shocks to occupants, fails safe, does not generate molten material, provides circuitry protection, prevents overheating of wires, and protects circuitry from floating debris.

References:

- AFSPCMAN 91-710 Volume 3, Chapter 14, Electrical and Electronic Equipment, and Attachment 2, Missile System Prelaunch Safety Package
- ISS Safety Requirements Document (SSP 51721), Chapter 4.3, Electrical
- Crewed Space Vehicle Battery Safety Requirements (JSC 20793)

2.3.7 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.

Verification Statement: The vehicle's stability should be verified by analysis and simulation. The verification should be considered successful when analysis and simulation show that the vehicle is sufficiently stable in all flight configurations in both static, dynamic, and other applicable stability modes.

Reference:

- Best Practices for the Design, Development, and Operations of a Robust and Reliable Space Vehicle Guidance, Navigation and Control Systems (NASA/TP-20230005922, NESC-RP-22-01762), National Aeronautics and Space Administration
- CCT-STD-1140, Rev. B-1. Crew Transportation Technical Standards and Design Evaluation Criteria. NASA

2.3.8 Materials and Commodities

a. The vehicle should be designed to ensure that materials and commodities are compatible and do not result in a hazard under the expected operating environment.
b. For inhabitable spaces, the materials and commodities 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 or commodity choices may lead to a hazard that puts occupants at risk. Proper selection or testing of materials and commodities during design prevents unsafe conditions related to flammability, off-gassing, and fluid compatibility. More stringent material and commodity selection is necessary in the inhabitable space 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 commodity or material-to-material interactions (e.g., different thermal properties from different materials may

induce thermal stress), as well as whether a material or commodity is compatible with the environment (e.g., reduced cabin pressure may result in off-gassing that leads to a hazard).

Verification Statement: The vehicle's materials and commodities compatibility, ignitability, explosiveness, out-gassing, particulate generation, and toxicity should be verified by analysis and testing. The verification should be considered successful when analysis and testing show that the materials and commodities do not result in a hazard to the occupants.

References:

- ASTM E595, Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment
- NASA-STD-6001

2.3.9 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.

Verification Statement: The vehicle's ability to operate in all expected natural and induced environments should be verified by analysis, modeling, testing, and monitoring. The verification should be considered successful when analysis, modeling, testing, and monitoring show that the vehicle's safety-critical systems operate in maximum predicted non-operating and operating environments.

Reference:

- Test Requirements for Launch, Upper-Stage and Space Vehicles (SMC-S-016)
- NASA Space Flight Human System Standard Volume 2: Human Factors, Habitability, and Environmental Health. Rev. C

2.3.10 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 penetration by a micrometeoroid or orbital debris.

Rationale: Micrometeoroids and orbital debris (MMOD) 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 MMOD 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, designing the mission to use an orbit with less MMOD risk is often used to reduce exposure of critical surface area to the MMOD environment. Because it is not technically feasible to detect or shield against all debris, it is not possible to completely avoid the possibility of penetration to safety-critical systems. Shielding and operations are used to reduce the risk to an acceptable level.

Verification Statement: The vehicle's MMOD mitigation should be verified by analysis and simulation. The verification should be considered successful when analysis and simulation show that the probability of a penetration by a micrometeoroid or orbital debris is minimized.

Reference:

- ISS Safety Requirements Document (SSP 51721), Chapter 4.11.1, Micrometeoroid and Orbital Debris
- CCT-STD-1140, Rev. B-1. Crew Transportation Technical Standards and Design Evaluation Criteria. NASA

2.3.11 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.

Verification Statement: The vehicle's ability to operate at conditions beyond the maximum expected operating environment should be verified by analysis and testing. The verification should be considered successful when analysis and testing show that the operation of safety-critical systems is not degraded due to design tolerances, manufacturing variances, and uncertainties in the environment.

References:

- Qualification and Acceptance Environmental Test Requirements, International Space Station Program (SSP 41172)
- Test Requirements for Launch, Upper-Stage and Space Vehicles (SMC-S-016)

2.3.12 Flight Demonstration

a. Prior to any flight with space flight participants, a demonstration flight should be conducted that is consistent with the nominal design reference mission that demonstrates integrated performance of a vehicle's hardware, software, and operational procedures.
b. Further flight demonstration should be conducted for any subsequent safety-critical modification that needs flight testing to verify integrated system performance.
c. Operational testing of the abort system should be conducted, as applicable.

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 occupants. The demonstration should represent the expected flight operations and mission profile as much as possible 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 occupants.

Verification Statement: The integrated performance of a vehicle's hardware, software, and operational procedures should be verified by flight test demonstration. The verification should be considered successful when flight test demonstration shows that the nominal design reference mission, subsequent safety-critical modifications, and any abort systems operate as designed.

Reference:

- Test Requirements for Launch, Upper-Stage, and Space Vehicles. Space and Missile Center Standard (SMC-S-016)
- NASA's Exploration Systems Architecture Study – Final Report. 10. Test and Evaluation

2.3.13 Emergency Occupant Location Post-Landing

The vehicle should:

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

b. Have high contrast markings on the vehicle itself, and

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

Rationale: In an unforeseen or emergency situation, the vehicle may not land at its pre-planned location. 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.

Verification Statement: The vehicle's ability to be located post-landing should be verified by analysis, demonstration, and testing. The verification should be considered successful when analysis, demonstration, and testing show that the vehicle's transmitter, markings, and visual aids are sufficient to locate the vehicle post-landing.

Reference:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraph 4.3.5.1.3, Visual Aids for Search and Rescue/Recovery

2.3.14 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 emergency, 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 pre-planned landing location, and of those searching to find them.

Verification Statement: The vehicle's ability to communicate with rescue personnel should be verified by testing and demonstration. The verification should be considered successful when testing and demonstration show that the communication systems have sufficient power and the ability to use the correct IAD frequency.

Reference:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Paragraph 4.3.5.1.8, Spacecraft Voice Communication with Recovery/Rescue Forces

2.3.15 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.

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, 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 versus 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.

Verification Statement: The occupant survivability analysis should be verified by inspection. The verification should be considered successful when inspection shows what occupant survivability measures were implemented to mitigate risk, a discussion of the relative change in risk to the occupant, and an evaluation of the design impacts.

Reference:

- Human-Rating Requirements (JSC-28354)

2.4 Human/Vehicle Integration

2.4.1 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 considered:

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 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 can 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 can 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.*

Verification Statement: The vehicle's ergonomics and human-to-machine interface which allow occupants to perform safety critical functions should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis show that the vehicle design accommodates variable occupant physical characteristics.

References:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130)
    - Appendix D, Crew Physical Dimension and Mass Design Data
    - Appendix E, Crewmember Strength Data
    - Appendix K, Crew Range of Motion
- SSP 50808, *Section 3.3.2.1, Anthropometric Requirements*
- International Space Station Flight Crew Integration Standard (NASA-STD-3000 / SSP 50005), Paragraphs
    - 3.3.2, Joint Motion
    - 4.9.3, Strength Design Requirements
    - 5.4, Acoustics
    - 5.5, Vibration

2.4.2 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.

Verification Statement: A ground controller or flight crew user interface that incorporates safety critical system health, status, and engineering data, accounting for current human factors techniques should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis show that ground controllers or flight crew can successfully monitor data needed to perform their safety critical functions.

Reference:

- Space Systems – Launch Vehicle to Spacecraft Flight Environments Telemetry Data Processing. ISO 15862:2009

2.4.3 Manual Override of Automatic Functions

a. 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, and return to the automatic function if required.

b. The operator should document procedures and training as to when the manual controls should be activated. If the operator determines a manual override is not necessary, the operator should have a documented justification including safety mitigations.

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. If 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. Returning to automatic functions allows a software to continue after the problem(s) is resolved and reduces crew fatigue.

Verification Statement: The vehicle's ability to allow for manual override of the vehicle safety critical functions during test and simulation events should be verified by inspection and analysis. Verification should be considered successful when inspection and analysis show that manual

override of the function will not directly cause a catastrophic event and will return to the automatic function if required.

Reference:

- Human-Rating Requirements for Space Systems (NPR 8705.2C)

2.4.4 Detection and Annunciation of Faults

The system should detect and annunciate safety-critical vehicle system faults to the flight crew and ground controllers as applicable, within the time necessary for the flight crew or ground controllers 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.

Verification Statement: The vehicle's ability to detect and annunciate safety critical system faults in cases of single and multiple faults should be verified by inspection and analysis. Verification should be considered successful when the caution and warning system or communication system would wake crew in the event of an emergency.

Reference:

- 14 CFR 25.1322 Flight crew alerting
- 14 CFR 25.1302 Installed systems and equipment for use by the flight crew
- ISS Safety Requirements Document (SSP 51721)

2.4.5 Voice Communication with the Vehicle

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

Rationale: Communication between the ground controllers and occupants is beneficial, as it provides operational insight to the ground and enhances the ability of the occupants 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 timeframe 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 occupants.

Verification Statement: The vehicle's ability to provide two-way communication between ground controllers and occupants should be verified through inspection and analysis. The verification should be considered successful when the inspection and analysis show that there are clear communication capabilities between both parties throughout the duration of the operation.

Reference:

- *Voice and Audio Communications. Recommendation for Space Data System Standards. CCSCS 766.2-B-1*
- *NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health*
- *International Communication System Interoperability Standards (ICSIS). National Aeronautics and Space Administration, Revision A, September 2020.*

2.4.6 Occupant Communication

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

Rationale: Clear communication is instrumental for effective communications during safety-critical operations. For effective communications, the message should 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. A backup means of communication should be considered.

Verification Statement: The vehicle's ability to provide two-way communication between occupants and safety critical personnel should be verified through inspection and analysis. The verification should be considered successful when the inspection and analysis show that there are clear communication capabilities between all parties throughout the duration of the operation.

Reference:

- *NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health*

2.4.7 Field of View 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 addition, occupants should clearly see what they need to see (such as stars, the sun, spacecraft components, etc.) considering faint objects may be washed out by glare or other brighter light sources, such as sunshine and spacecraft lights. In the future, windowless vehicles may become prevalent, and this practice could evolve to allow for such technological advances.

Verification Statement: The vehicle's ability to provide a direct, non-electronic, through-the-hull view and the unobstructed field-of-view should be verified by inspection. The verification should be considered successful when inspection confirms that the spacecraft window clearly provides a sufficiently sized field of view for an occupant such that they are able to complete the safety critical operation with little to no assistance needed.

Reference:

- *NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health*

2.4.8 Inadvertent Actions

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

Rationale: In the unforgiving environment of space flight, an inadvertent occupant or ground controller action could lead to serious injuries to occupants. Inadvertent actions or errant switch activation could occur due to several factors such as limited occupant 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.

Verification Statement: The ability of the vehicle's design, controls, and procedures to deter single accidental or inadvertent actions should be verified by analysis, testing, and simulation. The verification should be considered successful when failure mode analysis, testing, and simulation show that single actions would not cause serious injuries or damage to the safety-critical components.

Reference:

- NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health

2.4.9 Hardware Loads

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

Rationale: This design practice should apply to intentional forces imparted on hardware by an occupant 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 an occupant 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.

Verification Statement: The vehicle's ability to withstand intentional occupant input loads should be verified by inspection, analysis, and testing. The verification should be considered successful when qualification and acceptance testing, inspection, and analysis show no loss of function for the expected intentional occupant input loads with added margin, as appropriate.

Reference:

- Hardware Quality Assurance Program Requirements for Programs and Projects (NPR 8735.2C)

2.4.10 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, reflections, parallax view, and viewing angle.

Verification Statement: The vehicle instrumentation's ability to display safety critical information should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis show that the occupants are able to readily view the safety critical information in all defined environments and mission configurations, in a format that is consistently legible.

Reference:

- Human Integration Design Handbook (HIDH) (NASA/SP-2010-3407/REV1), Chapters
    - 10.3, Display Devices
    - 10.5, Display Device and Control Layout
    - 10.6, Visual Displays

2.4.11 Control of Glare and Reflection

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

Rationale: Internal and external sources of light can create glare or reflections that can interfere with the occupant'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 occupants.

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.

Verification Statement: The vehicle's ability to deflect glare and reflection on windows and displays should be verified by inspection, analysis, and testing. The verification should be considered successful when testing and simulations show that glare and reflection can be mitigated for all safety-critical information on displays in all defined sun angles and lighting configurations.

Reference:

- Optical Property Requirements for Glasses, Ceramics, and Plastics in Spacecraft Window Systems (JSC 66320)
- NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitibility, and Environmental Health (NASA-STD-3001)

2.4.12 Handling Qualities

The vehicle should be controllable to the extent necessary to allow the flight crew to perform 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.

Verification Statement: The vehicle's controllability should be verified through inspection, testing, and simulation. The verification should be considered successful when the inspection, simulation, and testing show that vehicle controls allow the crew to perform safety critical operations safely.

References:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Appendix L, Crew Interfaces
- The Use of Pilot Rating in The Evaluation of Aircraft Handling Qualities (NASA-TN-D-5153)

2.4.13 Workload

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

Rationale: Inadequately designed user interfaces or vehicle design with significant controlling by flight crew or ground controllers 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.

Verification Statement: The physical and cognitive workload to perform safety-critical operations should be verified by simulation and testing. The verification should be considered successful when the simulation and testing show that flight crew and ground controllers can consistently perform safety-critical operations within the workload limits.

Reference:

- Commercial Human Systems Integration Processes (JSC 65995), Figure 3.1.3.1.1-1, Nominal Commercial Crew Transport Mission

2.4.14 Emergency Control Markings

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

Rationale: In an emergency, 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. Coding of controls and mechanisms also helps avoid the accidental accessing of an emergency control.

Verification Statement: The marking of emergency controls should be verified by inspection and testing. The verification should be considered successful when inspection and testing shows that the occupants can easily identify the emergency controls when needed.

Reference:

- Controls for Flight Deck Systems (AC 20-175). Federal Aviation Administration.

2.4.15 Emergency Equipment Access

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

Rationale: In an emergency, having timely access to emergency equipment gives the occupants 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 occupant impact accessibility and response time.

Verification Statement: The access of emergency equipment should be verified by inspection and testing. The verification should be considered successful when inspection and testing show that the equipment can be accessed in a timely manner by occupants in any foreseeable emergency.

Reference:

- NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health (NASA-STD-3001, Volume 2, Revision C)

2.4.16 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, always readily available for each occupant.

Rationale: In an emergency, 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 occupant in a lights-out condition to address an unforeseen event or emergency.

Verification Statement: Availability and operation of emergency lighting including personal lighting devices should be verified by inspection and testing. The verification should be considered successful when inspection and testing shows that emergency procedures can be performed using the emergency or personal lighting devices.

Reference:

- NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health (NASA-STD-3001, Volume 2, Revision C)
- Graphical Symbols – Safety Signs – Safety Way Guidance Systems (SWGS). ISO 16069:2017

2.4.17 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 can function in a 1-g environment.

In an emergency:

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 should 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 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 necessary if no one is available to assist occupants to avoid serious injuries.

Verification Statement: Emergency egress for all phases of the mission with occupants aboard the vehicle should be verified by demonstration and testing. The verification should be

considered successful when demonstration and testing show that all occupants can safety egress the vehicle during pre-launch, during/post-abort as applicable, during space flight, and after landing or splashdown.

Reference:

- Commercial Crew Transportation System Certification Requirements for NASA Low Earth Orbit Missions (ESMD-CCTSCR-12.10)
- NASA Space Flight Human-System Standard Volume 2: Human Factors, Habitability, and Environmental Health (NASA-STD-3001, Volume 2, Revision C)

2.5 Extra Vehicular Activity

Extra Vehicular Activity (EVA) is any activity performed by a pressure-suited participant in unpressurized or space environments. EVA begins with depressurization of the airlock or space module and ends with repressurization of the space module or airlock after participant ingress. This includes any internal activities where a pressure-suited participant may be operating in normal modes of operation (e.g., airlocks, passageways, unpressurized work areas, donning/doffing areas) and abnormal modes of operation (e.g., unpressurized modules).

2.5.1 Extra Vehicular Activity System Suit Protection Considerations

The vehicle, the EVA system, and the EVA suit should be designed to allow for safe EVA operations as applicable to each operator. The following EVA suit safety protections should be included in systems to ensure the safety of the participants and vehicle equipment.

a. Temperatures: Surface temperatures of space vehicle components requiring EVA interface should be compatible with the touch-temperature limits of the pressure suit design being used. The EVA system suit should maintain all occupant skin contact temperatures within the range of 10C to 44C (50F to 111F) for the duration of the EVA.

b. Radiation: The EVA system design and operational procedures should protect the EVA participant from radiation for the duration of the EVA exposure during the mission.

c. Micrometeoroids and Debris: EVA system design should protect the EVA participant from expected particles including sand and dust.

d. Chemical Contamination: The EVA system should protect the participant from hazardous chemical contamination.

e. Tethers: EVA participants should be tethered to the space vehicle at all times in microgravity, unless they are in a free-flying maneuvering unit or otherwise suitably restrained.

f. Ignition Sources: Electrical current limiting devices should be provided to eliminate all potential ignition sources within any oxygen-enriched atmosphere of the life support system and pressure suit.

g. Suit Pressure: The EVA System should maintain inspired oxygen partial pressure of greater than 149 mmHg. Protection should be provided to prevent rupture by over pressurization of the participant's pressure envelope due to failure of the pressure supply system. The spacesuit should indicate the suit internal pressure to the suited participant without the use of power. The EVA System should enable the participant to safely return to the vehicle and repress after a breach in the pressure garment of a size determined to reasonably bound MMOD and sharp edge risk.

h. CO2: The EVA system should provide CO2 management to keep levels below those which would cause impairment or significant negative impacts on the participant.

i. Trace Contaminants: The EVA spacesuit should control accumulation of gaseous pollutants in the suit produced by metabolic loads, system sources, and material off gassing so that the total toxic hazard index is maintained below defined levels.

j. Noise Limits: For continuous noise, the EVA System spacesuit should limit the suit induced Sound Pressure Levels, created by the sum of all simultaneously operating equipment, to tolerable levels which will not cause long-term damage or impair ability of the participant to communicate. For personal communication devices, the EVA System spacesuit should limit the maximum A-weighted sound level at the participant's ear created by a personal communication device to 115 Decibel a-Weighted (dBA) or less.

k. System Induced Injury: The EVA System should minimize potential for injury to the participant.

l. Fault Tolerance: The EVA System should be designed such that no single failure precludes the ability of the participant to safely return to vehicle and repress.

m. Incapacitated EVA Occupant Rescue: The EVA System should provide the capability for a single EVA participant to facilitate the translation, ingress, and repress of a single completely incapacitated fellow EVA participant. Both participants should be able to repress simultaneously following the rescue.

n. Decompression Sickness Prevention: The EVA System and operations should be designed in a way as to reduce the probability of Decompression Sickness (DCS) to an acceptable level. A means of treating DCS or rapidly returning impacted participant should be considered.

o. Insight and Operability: The EVA System should provide the capability for each suited participant, ground, and EVA support personnel to monitor, operate, and control all systems and subsystems where: the capability is necessary to execute the mission; the

capability would prevent a catastrophic event; and the capability would prevent an abort or terminate.

p. Ingress and Repress Redundancy: The ingress and repress hardware and operations should be designed such that no single failure will prevent participants from ingressing, repressing, and doffing their suits.

Rationale: The EVA suit should be designed to protect the participant from a variety of hazards, allow for constant communication, and quick recovery and rescue.

Verification Statement: The ability of the EVA system suit to protect participants from hazards should be verified by simulation and testing. The verification should be considered successful when simulation and testing show that the EVA suit provides participants with a safe, habitable, and comfortable environment at all times.

The capability of EVA emergency life support for the suited participants should be verified by testing and demonstration. The verification should be considered successful when testing and demonstration show that EVA suited participants can safely return to and ingress/repress the host vehicle in response to any human or hardware emergencies.

References:

- NASA-STD-3000 Vol 1 section 14.1.3 General EVA Safety Design Requirements. Details on EVA physiology are in section 14.2, and EVA Anthropometry in section 14.3, 14.4 EVA Workstations and Restraints, 14.5 EVA Mobility and Translation, 14.6 EVA Tools, Fasteners, Connectors, 14.7 EVA Enhancement Systems.

2.5.2 Extra Vehicular Activity System Environment Protection

The vehicle and environment where EVA operations will be conducted should be designed to allow for safe EVA operations as applicable. The considerations listed in this section should also be factored in the design of the EVA system so that the EVA suit, other EVA system components, and EVA environment such as space stations or host vehicles are designed with consideration to EVA operations.

The following EVA safety requirements are a compilation of general design features with a focus on the EVA environment that should be included in systems to ensure the safety of the occupants and vehicle equipment:

a. Edges and Protrusions: All space vehicle equipment and structures requiring an EVA interface should either be designed to preclude sharp edges or protrusions or should be covered to protect the participant and the participant's critical support equipment.

b. Hazardous Equipment: Potentially hazardous items that could injure EVA participants or damage EVA equipment by entrapment, snagging, tearing, puncturing, cutting, burning, or abrading should be designed to ensure elimination of, or protection from, the hazard.

c. Ingress/Egress: EVA participants should always have a positive method and means to return to the pressurized module.

d. Power Sources: Special shielding or procedures should be provided to preclude EVA approaches to a nuclear reactor or radioisotope generator power source located in the space vehicle, that may result in additional radiation exposure.

e. Transmitters: Procedures should be developed to protect participants during EVA approaches that may result in harmful exposures to the non-ionizing radiation being emitted from all high-power electromagnetic wave transmitters (microwave, radar, laser, radio, UV/IR visible lamps) on or in the vehicle with exterior antennas or external apertures.

f. Electrical Voltage: The EVA participant should be protected against electric voltage shocks from inadvertent grounding of electric circuits and from electrical discharge resulting from static charge buildup.

Rationale: EVA, and non-EVA, as applicable, participant safety should be the paramount consideration in all EVA tasks.

Verification Statement: The EVA system operating environment should be verified by testing and simulation. The verification should be considered successful when testing and simulation show that all components of the EVA system provide environmental protection during all aspects of EVA operations.

References:

- NASA-STD-3000 Vol 1 section 14.1.3, General EVA Safety Design Requirements. Details on EVA physiology are in section 14.2, and EVA Anthropometry in section 14.3, 14.4 EVA Workstations and Restraints, 14.5 EVA Mobility and Translation, 14.6 EVA Tools, Fasteners, Connectors, 14.7 EVA Enhancement Systems.

2.5.3 Extra Vehicular Activity System Capabilities

The following EVA safety requirements are a compilation of general design features with a focus on the EVA system capabilities that should be included in systems to ensure the safety of the participants and vehicle equipment.

a. Two Way Communications: The EVA system should enable EVA participants and occupants on the vehicle as well as ground controllers to communicate voice and data.

b. Unassisted Suit Operation: The EVA system spacesuit should provide for unassisted operation of all suit functions by the suited participant.

c. Caution and Warning System: The EVA system should detect, indicate, annunciate, externally transmit, and internally communicate significant faults, performance degradation, or excessive resource usage and time remaining for all operating suits and pre-determined mission assets.

d. Metabolic Rate: The EVA system should accommodate the planned participant metabolic rate while maintaining a safe and reasonably comfortable core body temperature.

e. Visual Capabilities: The EVA system spacesuit should provide the participant with safe and accurate visual capabilities and head mobility to perform EVA tasks in both day and night-time conditions, as applicable.

f. Microgravity EVA Self Rescue Capability: The EVA system should permit the participant to perform self-rescue in the event the participant becomes detached from structure.

g. Aids for Body Restraint and Stabilization: The vehicle and EVA system should be designed such that participant stabilization and translation aids are available for planned worksites and translation paths.

Rationale: The EVA system capabilities should be designed to allow for safe EVA operations as applicable to each operator. These system capabilities should allow suited EVA participants to perform safe EVA operations.

Verification Statement: The EVA system's ability to provide participants with a means to conduct safe operations should be verified by testing and simulation. The verification should be considered successful when testing and simulation show that the EVA system allow for two-way communication, unassisted suit operation, caution and warning communication, metabolic rate maintenance, visual capability, self-rescue capability, and body restraint and stabilization.

References:

- NASA-STD-3000 Vol 1 section 14.1.3 General EVA Safety Design Requirements. Details on EVA physiology are in section 14.2, and EVA Anthropometry in section 14.3, 14.4 EVA Workstations and Restraints, 14.5 EVA Mobility and Translation, 14.6 EVA Tools, Fasteners, Connectors, 14.7 EVA Enhancement Systems.

2.6 System Safety

2.6.1 System Safety Program Organization

a. A system safety program should be documented, implemented, and maintained to establish a comprehensive and methodical system safety process and ensure continual

validity of system safety analysis, documentation, and data throughout the lifecycle of the system.

b. A system safety organization should be defined in sufficient detail to clearly demonstrate how the goals of the system safety program will be accomplished by sound system safety processes and through collaboration with management, engineering, and other disciplines within the larger organization, as well as pertinent external entities.

c. System safety processes should be in place to ensure and maintain effective communications with appropriate disciplines and organizations to collaborate, identify, and manage new hazards and modified risks.

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.

Verification Statement: The system safety program that defines the system safety organization should be verified by analysis and inspection. The verification should be considered successful when analysis and inspection show that the system safety organization includes internal and external organizational coordination, lines of communication, roles and responsibilities, and processes for decision-making and approvals; and when the system safety processes include initial and continuous hazard management efforts and processes for the management of lifecycle risk.

References:

- **F**AA Order 8000.369C, Safety Management System
- Safety Management System Manual, The Office of Commercial Space Transportation, 2022

2.6.2 System Safety Program Hazard Management

A system safety program's hazard management should systematically identify, define, mitigate with verifications, and manage system and mission hazards to ensure system safety analyses and data are continually validated.

Rationale: The system safety program and hazard management organization ensure (1) an organized and coordinated approach is used to identify and assess hazards, and to either eliminate them, mitigate risk, or accept residual risk; (2) system safety analyses are complete, valid, and current throughout the life cycle of the system; and (3) system safety data is identified, detailed, tracked, collected, analyzed, and retained.

The accepted residual risk is predicated on a configuration that is manufactured, qualified, tested, and operated to ensure the system meets expected performance in its operational life. Thus, a system safety process should be employed that continually evaluates the system to ensure a continued acceptable level of risk. Any proposed changes, deficiencies, or requested deviations/waivers within the integrated system should be assessed to ensure that no new hazards or causes to existing hazards were introduced, and that the existing mitigation strategies are still valid to ensure acceptable risk is maintained. System safety analysis inconsistencies and impacts from post-flight data, anomalies, and mishap investigations need to be addressed and corrective actions implemented to prevent reoccurrence of any anomaly or mishap.

Verification Statement: The system safety program's hazard management system should be verified by analysis and inspection. The verification should be considered successful when analysis and inspection shows that the hazard management system defines the methodology and analysis tools for identifying and assessing risk of system safety hazards with documented mitigation strategies and associated verification evidence, throughout the life cycle of the system.

2.6.3 Management of Lifecycle Risks

The system safety program should be maintained throughout the system lifecycle to continually manage hazards by considering all potential impacts to any proposed changes, deficiencies, or requested deviations or waivers during the design, manufacturing and refurbishment, and operations phases.

Rationale: Management of lifecycle risks is essential for ensuring the continued validity of system safety analyses and data. 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 helps ensure 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.

Verification Statement: Maintenance of the system safety program throughout the system lifecycle should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis show that hazards are managed by considering all potential impacts to any proposed changes, deficiencies, or requested deviations/waivers during the design, manufacturing and refurbishment, and operations phases.

Reference:

- MIL – STD 882E, Department of Defense Standard Practice: System Safety

2.6.4 System Safety Analysis

a. System safety analysis should be initiated at the onset of the system development cycle to identify and characterize each hazard, assess the risk to occupant safety, reduce risks through risk elimination and mitigation measures, and verify that risks have been reduced to an acceptable level.

b. System safety analyses should be continuously updated and validated throughout the life cycle of the system as per the documented system safety program.

c. The documented system safety analyses should be consistent with common space industry practice.

Rationale: System safety analyses, when conducted during system development and throughout the system's lifecycle, eliminate or reduce risk by continuously identifying and mitigating standalone and integrated hazards.

Verification Statement: The system safety analysis should be verified by inspection. The verification should be considered successful when inspection shows that the system safety processes reduce occupant risk to an acceptable level throughout the lifecycle of the system, are updated regularly, and are consistent with common space industry practice.

Reference:

- MIL – STD 882E, Department of Defense Standard Practice: System Safety

2.6.5 Software Safety

a. Hazards from computing systems and software should be integrated into the safety processes and analyses. Any software or data that implements a capability that can present a hazard to an occupant by intended operation, unintended operation, or non-operation should be considered.

b. A software development process and maintenance approach should be documented and maintained for each software component in accordance with industry best practices for its

level of criticality. The process should be commensurate with the level of rigor necessary to ensure safety based on the degree of control and hazard severity of the software, which determine its level of criticality.

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.

Verification Statement: The software system safety program should be verified by inspection. The verification should be considered successful when all hazards are included, and when the software development process is consistent with common industry practice.

Reference:

- MIL – STD 882E, Department of Defense Standard Practice: System Safety
- Joint Services Software Safety Committee, Software System Safety Handbook, Version 1, dated August 27, 2010
- National Aeronautics and Space Administration, NASA-STD-8739.8, Software Assurance and Software Safety Standard
- National Aeronautics and Space Administration, NASA-HDBK-2203, NASA Software Engineering and Assurance Handbook, dated April 4, 2020

2.7 Design Documentation

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

a. Vehicle design 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 occupants,

h. Weather limitations,

i. Landing site limitations,

j. Software and computing system user procedures and operating limitations,

k. Maintenance requirements for hardware and software to ensure continued flightworthiness,

l. Normal operating procedures

m. Emergency procedures, and

n. Vehicle characteristics.

Rationale: To safely operate a space flight system, an operator should have a clear understanding of the vehicle and the vehicle's performance capability, operational limits, hazards, maintenance needs, as well as normal and emergency operations, so that the vehicle is operated as designed and within its capabilities. The emergency procedures normally would include crash, fire, and rescue procedures for the space flight system.

Verification Statement: Design, manufacturing and operational documentation should be verified and maintained such that initial decisions, design changes, and rationale are routinely reviewed and approved by the operator's safety organization. The verification should be considered successful when the operational and system limitations and maintenance requirements are documented.

Reference:

- NASA-STD-3001 – NASA Space Flight Human-System Standard, Volume 2: Human Factors, Habitability, and Environmental Health, Rev C
- NASA Systems Engineering Handbook – 6.0 Crosscutting Technical Management

3.0 MANUFACTURING AND MAINTENANCE

This section includes manufacturing recommendations, including quality control, so the vehicle is manufactured per the vehicle design.

3.1 Quality Manufacturing

3.1.1 Quality Assurance

a. 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.

b. This quality assurance process should implement a quality management system that controls documentation, tracks and resolves non-conformances in processes and materials, and independently audits regularly.

Rationale: Quality assurance processes are essential to ensure that the system is manufactured in accordance with 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, and may increase the likelihood that new hazards may be introduced.

Verification Statement: The Quality Management System should be verified by documention of sufficient detail to ensure appropriate oversight of the manufacturing and quality assurance processes are applied. The verification should be considered successful upon inspection of the records and the records affirm that the processes are in compliance.

References:

- ISO-9001, Quality management systems — Requirements
- AS9100, Quality Management System – Requirements for Aviation, Space and Defense Organizations

3.1.2 Acceptance Testing of Systems, Subsystems, and Components

a. Each safety-critical system, subsystem, or component 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. Lot testing of consumable safety-critical components (like initiators) should be conducted. A statistically representative sample from a production lot should be acceptance tested for expected performance under the maximum expected operating environment.

c. As an alternative to acceptance testing, 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 can meet 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) that are 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.

Lot testing (or sampling, batch testing) of raw materials and components enhances quality assurance during the manufacturing process. Lot testing is a demonstrated technique to improve efficiency.

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.

Verification Statement: The operator's documentation demonstrating acceptance testing of safety-related flight components to levels that sufficiently cover expected operating environments, test equipment uncertainty, and material quality variation should be verified by inspection. The verification is considered successful when valid acceptance testing avoids over-testing safety critical components. Testing significantly under qualification levels and durations but still over nominal operation levels completes verification.

Reference:

- Test Requirements for Launch, Upper-Stage, and Space Vehicles (SMC-S-016)
- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130)

3.2 Lifecycle Risk Sustainment

Configuration management, control, and tracking should be utilized to ensure system integrity is maintained and ensure the use of correct and appropriate versions of all items and

documentation. The aspects of lifecycle risk sustainment should be consistent with common industry practice.

a. Reuse – See Management of Lifecycle Risk in Section 2.7.2.
b. Refurbishment – Refurbishment methods should consider the determined service life of the system and its components in any plan for potential reuse and include:
    1. Identification, tracking, and replacement of life limited components (e.g., heat shield, parachutes),
    2. Identification and tracking of preventative maintenance items (e.g., items requiring lubrication),
    3. Monitoring of all environments experienced by the system and components to the extent necessary to assess and evaluate the actual life remaining or adjust any inspection periods,
    4. Inspection criteria,
    5. In-service testing to ensure functional capability,
    6. Criteria for identification of timed-out components/items for disposal, and
    7. Instructions on inspection and replenishment of consumables.
c. Retirement Plan – During manufacturing, identification of the components should be incorporated to ensure components reaching the end of lifecycle are removed from service.

Rationale: Lifecycle Risk Sustainment ensures that a system configuration is designed, manufactured, refurbished, and repaired such that the system continually meets expected performance in its operational life and acceptable level of risk is maintained.

Verification Statement: Lifecycle risk sustainment should be verified through inspection. The verification is considered successful when inspection shows defined processes for reuse, refurbishment, and retirement of all components.

3.3 System Maintainability

a. System maintainability should be assessed (i.e., the necessity, frequency, and capability for repairs) and appropriately addressed.
b. To ensure proper maintenance, approaches should consider:
    1. Identification and quantity of replacement parts,
    2. Access panels and ease of access,
    3. Ease of repair and training or certification, and

4. Tool control and calibration.

Rationale: System maintainability ensures that a system configuration is designed, manufactured, refurbished, and repaired such that the system continually meets expected performance in its operational life and acceptable level of risk is maintained.

Verification Statement: System maintainability should be verified through inspection. Verification should be considered successful when inspection shows that defined processes are established and being followed for manufacturing and refurbishment operations, configuration management and control, foreign object debris control and mitigation, system cleanliness, and system maintainability and availability.

References:

- Standard for Software Quality Assurance Plans (IEEE 730-2002)
- NASA Space Flight Human System Standard Volume 2: Human Factors, Habitability, and Environmental Health. Rev. C

3.4 Manufacturing Facilities

Manufacturing facilities should implement best practices and ensure high standard of cleanliness is maintained throughout the manufacturing process. These recommendations and practices include:

1. Environmental Controls: These controls should maintain constant temperatures, humidity and pressure throughout the facility where safety related components are being manufactured. A set of defined requirements should be created and followed to ensure consistent quality.

2. Ventilation Systems: These systems should be implemented throughout the facility to ensure the air is clear from dust, debris and microbes as specified for each safety related component.

3. Cleanliness: Facilities should implement proper cleanliness practices for manufacturing of safety critical components as well as storing these components. Facilities should also create practices that require workspaces handling components to be cleaned periodically per approved process controls.

4. Clean Rooms: Facilities should have controlled clean rooms to manufacture, assemble, and test sensitive hardware.

5. Monitoring Clean Rooms: Facilities should keep a detailed record of air properties and contamination events.

6. Training: Facilities should identify training requirements and implement training for all personnel involved in the manufacturing process. This training should include:

a. Contamination control in all phases of manufacturing,

b. Techniques of clean assembly and packaging,

c. Contamination Control Plan,

d. Monitoring procedures, and

e. Importance of clean room apparel and discipline in clean areas.

Rationale: The cleanliness of facilities contributes to a high quality of parts and components produced. Adoption of industry best practices will promote safer operations as well as more reliability to ensure confidence in the build quality of all products.

Verification Statement: Cleanliness of manufacturing facilities should be verified by inspection. Verification should be considered successful when inspection shows that atmospheric conditions and clean rooms throughout the manufacturing process maintain quality and cleanliness of components and hardware and that all training requirements are implemented.

References:

- Cleanrooms and Associated Controlled Environments (ISO-14644)
- Standard Test Method for Sizing and Counting Airborne Particulate Contamination in Cleanrooms and Other Dust-Controlled Areas (ASTM-F25/F25M-21)

4.0 OPERATIONS

4.1 Management

This section addresses the operations and management of space flight, including mission authority, configuration management, quality assurance, flight readiness, reviews, and investigations.

4.1.1 Flight Operations Authority

An operator should identify and implement clear 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.

It is important to have a hierarchy of authority so that decision authority is delegated to those at appropriate levels. The person making the final decisions should consider a large scope of information and interests. Because of the limited resources available during space flight, such as time and person-hours, concise but accurate information needs to be transmitted to and

understood by the decision-making parties. There should always be a clearly designated final decider for mission decisions on the ground.

Verification Statement: Communication and approval authority procedures should be verified by inspection and demonstration. The verification should be considered successful when inspection and demonstration show that there are clear lines of communication and approval authority for all safety-critical decisions.

References:

- 14 CFR part 450 – Launch and Reentry License Requirements

4.1.2 Flight Crew Decision Authority

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

b. In cases of immediate need, the above designated member of the flight crew, often called the Captain or Commander, will have final authority until time allows a hand-off of the situation back to the overall mission authority designated in 4.1.1.

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 crewmember, independent of ground personnel, is important due to the flight crew's unique situational awareness.

Verification Statement: The operator's process for designating a flight crewmember to have final decision authority should be verified by inspection. The verification should be considered successful when inspection shows that the designated flight crewmember with ultimate decision authority on the vehicle is trained, holds the appropriate qualifications, and is responsible for on-board operations and safety of the flight.

References:

- 14 CFR Part 121 Subpart T – Flight Operations
- 14 CFR Part 91.3 – Responsibility and Authority of the Pilot in Command
- 14 CFR 1214.403 – Code of Conduct for the International Space Station Crew

4.1.3 Flight Readiness

a. 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.

b. If anomalies were experienced in the previous flight, corrective actions should be discussed and implemented as part of the flight readiness procedures.

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. If anomalies occurred on prior flights, the flight readiness review can serve as a final opportunity to ensure new operational procedures have been incorporated into appropriate checklist and documentation. The final flight readiness review can reinforce awareness of technical changes that have been made to the vehicle and their impacts on the upcoming flight activities.

Verification Statement: The operator's completion of readiness procedures and closure of any outstanding issues should be verified by inspection. The verification should be considered successful when the inspection shows documented flight readiness and implementation of corrective actions.

References:

- NASA Space Flight Program and Project Management Handbook (NPR 7120.5), 2010.
- NASA System Engineering Process and Requirements (NPR 7123.1A).

4.1.4 In-flight Anomaly Investigation, Tracking, and Resolution

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

b. The anomaly resolution process and any actions necessary for the continuation of safe flight and completion of the mission, should include the operator's safety organization and be approved by the operator's mission decision authority.

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

1. Document the anomaly;
2. Identify the root cause of the anomaly;
3. Implement any actions necessary for subsequent safe flight; and
4. Review and brief any corrective actions during any subsequent flight readiness review (see section 4.1.3).

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. Corrective actions are necessary to address any changes that can affect safety. 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 or safety organization error.

Verification Statement: The anomaly resolution process for all phases of the mission should be verified through inspection. The verification should be considered successful when inspection shows execution of the recommended actions listed above.

References:

- NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping (NPR8621.1D)

4.1.5 Post-flight Data Review

The operator should conduct a post-flight data review to assess and implement corrective actions prior to the next flight. The post-flight data review should include at a minimum:

- Any discrepancy or anomaly that occurred during the launch countdown and flight;
- Any deviation from safety-critical processes or procedures;
- Any flight environment not consistent with the maximum predicted environment as required; and
- The occupant experience including workload, ergonomics, medical assessment, personal hygiene, and crew environments.

Rationale: Assessing the key design assumptions, flight, procedures, environments, and occupant experience is important for continuous improvement of the flight system, operations, and occupant safety. The post-flight data review should address the vehicle design and performance, and operations on the ground and on the vehicle. The post-flight data review should help the operator change designs or operations, as necessary, to keep occupants safe.

Verification Statement: Design or operational changes based on the post-flight data review should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis shows that the post-flight data review includes all minimum data required to make corrective actions.

Reference:

- Guideline for Forming and Operating Failure Review Boards and Anomaly Review Boards. Goddard Technical Handbook (GSFC-HDBK-8700). 2019.
- NASA System Engineering Process and Requirements (NPR 7123.1A)

4.1.6 Mishap Investigation

An operator should investigate and document the root cause of any mishap 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 mishap prior to the completion of an investigation, and the adoption of preventive measures, could jeopardize the safety of occupants. The safety organization's review and approval of the preventative measures prior to the next flight ensures the safety of occupants.

Verification Statement: The mishap plan should be verified through inspection. The verification should be considered successful when inspection shows that the mishap plan includes the mishap investigation requirements and preventative measures.

Reference:

- 14 CFR 450.173 Mishap plan - reporting, response, and investigation requirements

4.2 System Safety

This section addresses system safety as it relates to space flight operations.

4.2.1 System Safety Program

An operator should implement system safety processes, as outlined in section 2.6.1.

4.2.2 System Safety Analysis

An operator should:

a. Conduct operations system safety analyses, as outlined in section 2.6.4; and

b. Review all existing hazards and, as necessary, revise/update the system safety analyses, as outlined in section 2.6.2.

4.2.3 Payload Safety

Prior to each flight, an operator should identify and mitigate payload hazards via system safety processes and approaches outlined in section 2.6.

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, fire, or other hazardous events. 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.

Verification Statement: The payload hazards for each flight should be verified by inspection and analysis. The verification should be considered successful when inspection and analysis show that the payload integration processes, facilities and checklists are in compliance. The verification is also successful when inspection and analysis show review of the completed checklist evaluating late payload exchanges.

Reference:

- NASA Payload Safety Requirements (NASA-STD 8719.24). 2022.

4.3 Planning, Procedures, and Rules

This section addresses the recommended planning, procedures, and rules that should be in place for human space flight to protect occupant safety.

4.3.1 Operating Within Constraints

An operator should operate the system within the latest approved 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).

Verification Statement: The vehicle operating limitations and procedures should be verified by inspection. The verification is considered successful when the records show the operator has continuously updated and distributed changes to vehicle's operating limitations. The verification is also considered successful when post flight review is conducted to identify any operating limit exceedances.

Reference:

- NASA Systems Engineering Handbook
- Constraint and flight rule management for space mission operations. https://ntrs.nasa.gov/api/citations/20110010860/downloads/20110010860.pdf

4.3.2 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.

Verification Statement: Consistency of the operations products within the limits of the system should be verified by inspection. Verification should be considered successful when inspection shows that all products that are necessary to operate the system, such as plans, procedures, processes, schedules, and supporting information, are consistent with the operating limits of the system and are distributed to flight and ground crew.

Reference:

- NASA Systems Engineering Handbook
- NASA-TM-2005-214062 – Exploration Systems Architecture Study. 7.0 Operations

4.3.3 Procedures

An operator should have procedures for safety-critical operations that ensure the system 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.

Verification Statement: The procedures for safety-critical operations should be verified by inspection, table-top exercises, and simulation. The verification should be considered successful when inspection, table-top exercises, and simulation show that the system is operated within established limits.

References:

- Federal Aviation Administration - Airman Certification Standards
- Department of the Navy - Naval Air Training and Operating Procedures Standardization (NATOPS)

4.3.4 Integrated Operations Coordination

An operator should coordinate all plans and procedures for safety-critical integrated operations among all affected entities, such as a launch and reentry vehicle operator, a spacecraft operator, and any launch and landing facilities.

Rationale: Space flight operations often involve multiple entities, such as a launch and reentry vehicle operator, a spacecraft operator, and launch and landing facilities. 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.

Verification Statement: The coordination of safety-critical plans and procedures should be verified by inspection, table-top exercises, or coordinated simulations. The verification should be considered successful when inspection, table-top exercises, or coordinated simulations show that plans and procedures have been coordinated with all entities.

Reference:

- Space Doctrine Note, Operations - U.S. Department of Defense. https://media.defense.gov/2022/Feb/02/2002931717/-1/-1/0/SDN%20OPERATIONS%2025%20JANUARY%202022.PDF
- Enabling Human Space Exploration Through Integrated Operational Testing - NASA. https://www.nasa.gov/sites/default/files/atoms/files/ready_evaworkshop2019_coan.pdf

4.3.5 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, including rest rules, 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.

c. Occupant activities should be coordinated to not interfere with rest requirements for flight crew, ground controllers, or safety-critical ground operations personnel.

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 all 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 uninterrupted rest periods necessary to allow a return to duty fully capable.*

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

c. *Coordination of activities is important so that occupants do not disturb others during rest periods and contribute to fatigue.*

Verification Statement: Duty limitations and rest rules should be verified by inspection. The verification should be considered successful when inspection shows that rest cycles are appropriate to the operation, including required uninterrupted non-duty time before flight duty responsibilities begin. Rest compliance will be met when procedures for all flight crew, ground controllers, and safety-critical ground operations personnel include the required uninterrupted non-duty time.

Reference:

- 14 CFR 431.43(c)(4)

4.3.6 Maintenance and Preventive Maintenance

An operator should perform and document maintenance and preventive maintenance requirements throughout the system life-cycle for both hardware and software in accordance with the operational documentation, outlined in section 2.7, to ensure readiness for safe flight.

Rationale: Maintenance and preventive 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.

Verification Statement: Performance and documentation of all maintenance and preventive maintenance should be verified by inspection. The verification should be considered successful when inspection shows that maintenance for hardware, software, and firmware is as prescribed in the operational documentation.

Reference:

- NASA Maintenance Concept for Space Systems, Technique PM-3

4.3.7 Flight Commit Criteria and Flight Abort Rules

An operator should document operational rules and criteria that identify the system's condition and the capability that should exist 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 flight commit criteria and flight abort 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.

Verification Statement: Flight commit criteria and flight abort rules should be verified by inspection. The verification should be considered successful when inspection shows that the flight commit criteria and flight abort rules include steps pertaining to or assessing the health and safety of the crew and space flight participants.

References:

- Range Flight Safety Requirements (NASA-STD-8719.25). 2018.
- AFSPCMAN 91-710
- 14 C.F.R. 450.165, Flight commit criteria
- 14 C.F.R. 450.108(f), Flight abort

4.3.8 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. Communication procedures should include recording safety-critical communication channels.

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. Recording of safety-critical communications channels is important for potential mishap investigations or for lessons-learned training.

Verification Statement: Communications procedures should be verified by inspection and simulation. Verification should be considered successful when inspection and simulation show a

communications protocol between personnel performing safety-critical operations and that communications are recorded.

References:

- AFSPCMAN 91-710

4.3.9 Landing Sites

a. An operator should identify a primary and a minimum of one contingency landing site for all occupied vehicles prior to flight.

b. An operator should identify the criteria for determining when a primary or contingency site will be used.

c. An operator should coordinate with all relevant authorities in advance to secure the primary and contingency landing sites.

d. An operator should have in place resources to conduct nominal post-landing procedures, as well as emergency operations as required.

Rationale: The identification of landing sites is necessary for the safe conduct of a flight. Having a contingency landing site, or sites, protects against scenarios that may prevent landing at the primary landing site such as weather conditions. In addition, clear criteria for a landing site's use are necessary because space flight operations are often time critical. Procedures, agreements, and resources prepared ahead of flight will facilitate use of any contingency sites.

Verification Statement: Coordination and agreements for primary landing sites and any foreseeable contingency landing sites should be verified by inspection. Verification should be considered successful when inspection shows that primary and contingency sites are identified, the criteria for their use are identified, and all relevant authorities and resources are in place for all sites.

Reference:

- Commercial Space Integration into the NAS (CSINAS) Concept of Operations

4.3.10 Collision and Conjunction Analysis

a. For flights above 150 kilometers, an operator should establish window closures needed to ensure that the launch or reentry vehicle, any jettisoned components, or payloads do not exceed a probability of collision of 1×10^{-6}.

b. On-orbit, an operator should establish conjunction risk thresholds and maneuver to avoid objects that exceed the risk.

c. Before maneuvering to a new orbit, an operator should have the trajectory and new orbit screened to ensure conjunction risk criteria is not exceeded.

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 timeframe, a launch can be delayed to avoid an object that has a high risk of collision with the vehicle. While on-orbit, 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 spacecraft's occupants on a collision course with another object.

The goal is to provide reasonable protection while minimizing operational impacts. 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. The International Space Station, at about 400km altitude, maneuvers several times a year to avoid exceeding the on-orbit collision probability. A smaller vehicle on a 2-week flight would need significantly less.

Collision avoidance is not needed for flights with a planned maximum altitude less than 150 kilometers, because there are few orbital objects below that altitude.

Verification Statement: Conjunction analysis and avoidance procedures for on-orbit maneuvers and potential collisions should be verified by analysis and inspection. Verification is considered successful when analysis and inspection show that the launch or reentry collision avoidance and conjunction procedures meet the risk criteria established.

Reference:

- 14 CFR 450.169, Launch and reentry collision avoidance analysis requirements

4.3.11 Selection of Safe Flight Profile

An operator should design the mission profile to limit the probability of collision with objects 10 cm and larger to less than 0.001 (1 in 1,000) during the mission's orbital lifetime.

Rationale: The mission profile can be adjusted during the planning stage to avoid debris-dense orbits. Planning the mission profile to avoid debris could prevent most costly collision avoidance maneuvers while on-orbit.

Verification Statement: The probability of collision over the orbital lifetime should be verified by analysis. The verification should be considered successful when the analysis shows that the probability of collision with known orbital objects over the entire mission is within criteria.

Reference:

- U.S. Government Orbital Debris Mitigation Standard Practices, November 2019 Update.

4.3.12 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 contingency 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 2.3.1.

Verification Statement: The procedures for an early end of flight should be verified by inspection and simulation. The verification should be considered successful when inspection and simulation show that a safety-critical function becoming zero failure tolerant results in termination of the mission.

References:

- 14 CFR 121.565, Engine inoperative: Landing; reporting
- 14 CFR 135.69 Restriction or suspension of operations: Continuation of flight in an emergency
- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130), Sections 4.3.2.2.2, Control Critical Hazards, and 4.3.2.3, Failure Tolerance

4.3.13 Vehicle 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.

b. An operator should budget and monitor the required propellant for a nominal attitude control, deorbit, and reentry.

c. 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 occupants to prepare 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.

Verification Statement: The plan for budgeting and monitoring the required consumables needed for carrying out safe flight should be verified by analysis. Verification should be considered successful when analysis shows that the plan accounts for all possible mission scenarios and include sufficient margin for consumables.

Reference:

- On-orbit propulsion system performance of ISS visiting vehicles. (n.d.). - https://ntrs.nasa.gov/api/citations/20130013168/downloads/20130013168.pdf

4.3.14 Cabin Hygiene

An operator should implement cabin hygiene procedures and processes to prevent occupant exposure to microbial or fungal contamination and foreign object debris, which could lead to an incapacitating illness or serious injury. To maintain cabin hygiene, occupants should be supplied with personal hygiene and grooming provisions. All personal hygiene kits should be appropriate for the duration of the mission.

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 (FOD) 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. Personal cleanliness and grooming are also important to maintain overall cabin hygiene.

Verification Statement: Cabin cleanliness procedures and cabin hygiene procedures for pre-flight and in-flight should be verified by inspection. Verification should be considered successful when inspection shows that cleanliness levels for assembly and subassembly are implemented using a contamination control plan and FOD prevention program. Verification is also successful

when a post-flight FOD record is maintained and there is availability and sufficiency of personal hygiene kits for all occupants.

References:

- Standard Materials and Processes Requirements for Spacecraft (NASA-STD-6016A)
- ASTM E1548: Standard Practice for Preparation of Aerospace Contamination Control Plans.

4.3.15 Atmospheric Conditions

Refer to section 2.1.1.

4.3.16 Extra Vehicular Activity Operations

Operations and training should be conducted to allow for safe Extra Vehicular Activity (EVA) as applicable. Non-EVA participant safety should also be considered, as EVA operations can affect them as well.

a. EVA operations should include tethering or other method to ensure participants remain safely secured to structures at all times to prevent an EVA participant from becoming inadvertently detached from the vehicle or structure. Redundancy for tethering methods, foot restraints, rescue system such as SAFER (Simplified Aid for EVA Rescue) jet packs or other method should be used to ensure attachment of EVA participant to a vehicle or structure should one method fail.

b. EVAs should be planned to account for stand-off distances from equipment or structures such as sharp edges that could puncture the suit, antennas that could result in hazardous radiation to the EVA participant and nozzles that could injure participants when thrusting.

c. EVAs should be planned such that incapacitation (medical or otherwise) does not preclude safe return of an EVA participant. This is most commonly accomplished via a "buddy system" of having two EVA participants each capable of rescuing the other if incapacitated.

d. Training for the EVA activity should address all normal operations and potential hazards of putting the participants in a hostile space environment such as depressurization from EVA suit punctures, tethering operations, avoidance of keep out areas, critical suit life support controls, mission specific training, etc.

Rationale: EVA is any activity performed by a pressure-suited participant in unpressurized or space environments. EVA begins with depressurization of the airlock or space module and ends with repressurization of the space module or airlock after participant ingress. This includes any internal activities where a pressure-suited participant may be operating in normal modes of

operation (e.g., airlocks, passageways, unpressurized work areas, donning/doffing areas) and abnormal modes of operation (e.g., unpressurized modules).

Pressure suits are typically massive and bulky, and limit performance more than a shirtsleeve environment does. Limitations of suited operations include:

- *Sensory degradation (limited field of view, tactile feedback, acoustics)*
- *Limited crewmember mobility and dexterity, force application, and endurance*
- *Limitations on working volume and access*
- *Long preparation and clean-up times*
- *Consumables*

Improving suited visual performance, reach, range of motion, strength, and mobility are key to improving overall EVA performance. In addition, it is important to ensure that the acoustic and lighting environment are ideal for suited conditions and consider the design of the suit and expected operations.

Verification Statement: The mitigation of potential EVA hazards should be verified by analysis and inspection. The verification should be considered successful when analysis and inspection show that emergency procedures are sufficient for suited occupants to safely return to and ingress/repress the spacecraft in response to any human or hardware emergencies.

References:

- NASA-STD-3000 Vol 1 section 14.1.1 General EVA Information
- NASA SP-2010-3407/REV1 Human Integration Design Handbook, 2014
- International Space Station ISS EVA Systems Checklist, 2005
- Safety Design for Space Systems Chapter 22, Extravehicular Activity Safety (Musgrave, 2009)

4.3.17 Food and Water

Refer to section 2.1.2.

4.3.18 Body Waste and Vomitus Management

Refer to section 2.1.4.

4.3.19 Biological Waste and Wet Trash Management

Refer to section 2.1.5.

4.3.20 Probability of No Penetration by Micrometeoroids or Orbital Debris

Refer to section 2.3.10.

4.3.21 Control of Glare and Reflection

Refer to section 2.4.11.

4.4 Medical Considerations

This section addresses medical considerations the operator should take into account when planning a human space flight mission and assessing occupants.

4.4.1 Flight Crew Medical Fitness for Flight

a. Within 6 months of an orbital space flight, each flight crewmember should have a medical examination by a licensed physician board-certified in aerospace medicine to identify any medical, psychological, or physiological condition (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 crewmember should have a medical examination by a licensed physician board-certified in aerospace medicine to identify any medical, psychological, or physiological condition (acute or chronic) that could lead to incapacitation or inability to perform safety-critical operations.

c. Flight crew should have a follow-up medical examination within fourteen (14) days prior to flight to confirm no decline in medical, psychological, or physiological status.

d. The flight crew should perform a medical self-assessment day of flight.

e. A flight crewmember should not fly if they have a known medical, physiological, or psychological condition (acute or chronic) that would invalidate the previous physical or make them unable to perform safety-critical operations.

f. A flight crewmember 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.

g. Each flight crewmember 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, to perform safety-critical operations.

Rationale: NASA astronauts are subjected to extensive medical and psychological testing 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 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 crewmember 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). A follow-up medical examination within 14-days of flight allows additional opportunity to detect conditions, whether acute or chronic, that may prevent flight crew from performing their duties. This medical follow-up examination may be conducted in-person or virtually.

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, 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 crewmember should assess their own personal fitness for flight (such as illness, medications, stress, alcohol, fatigue, appetite, and emotions) 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 crewmember 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 crewmember demonstrate an ability to withstand the stresses of space flight to ensure the flight crewmember can perform his or her duties in the environment in which they plan to operate. Past methods for demonstrating this ability 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 crewmember can successfully perform their safety-critical operations.

Verification Statement: Medical fitness evaluations and any follow up measures should be verified by inspection. The verification should be considered successful when all crewmembers' health status is in an approvable state based upon documented recommendations from the operator, the crewmember themselves, and the medical professionals that evaluated them.

References:

- NASA-STD-3001 – Crew Health, Vol. 1, Rev B

4.4.2 Space Flight Participant Medical Consultation

a. Proximate to flight, the operator should require each space flight participant to consult with a physician, trained or experienced in aerospace medicine, to ascertain their personal medical risks from the space flight profile and vehicle.

b. The operator should provide space flight participants with a list of recommended physicians trained in aerospace medicine and who are familiar with the vehicle's specific operational environment.

c. The operator should provide a medical checklist unique to its vehicle operations and any potential contingency operations for physicians to evaluate the space flight participants for space flight.

d. The operator should require the space flight participant to complete a self-conducted or physician directed medical assessment on the day of 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 proximate to flight, 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.

The medical checklist criteria should be similar to or more thorough than criteria used for other high intensity experiences such as aerobatic flight, strenuous exercise, and high-responsibility-high-stress environments. The checklist should evaluate criteria such as those in FAA Medical Certification, as well as chronic or acute illness, medication, alcohol consumption, fatigue, stress, emotional state, G-tolerance, cardiovascular and respiratory health, hypoxia, vision, hearing, motion sickness, and pregnancy. The ability to perform as-needed physical tasks (such as in a contingency or emergency scenario) should be evaluated. The medical examiner or the vehicle operator may determine additional medical criteria for the particular flight profile.

Verification Statement: The medical requirements for space flight participants' physical readiness to fly should be verified by inspection. The verification should be considered successful when inspection shows that the operator has a list of qualified medical personnel available for space flight participants, all space flight participants have been medically evaluated, and any follow-up measures prior to the space flight participant's flight are documented. Additionally, inspection shows that the operator documents the day of flight medical assessment completed for each space flight participant.

Reference:

- NASA-STD-3001 – Crew Health, Vol. 1, Rev B

4.4.3 Flight Crew Medical Assessment After Flight

a. Flight crew should have a post-flight medical screening to assess the impact of the flight, the scope of which should depend on the duration of flight and the flight profile, to implement any necessary corrective actions.

b. A record of the post flight assessment should be maintained to preclude potential incidents in the future.

Rationale: A qualified physician should verify post flight health of crew because flight conditions may have degraded the physiological or psychological condition. The qualified physician should determine the level of physical or psychological examination depending on the duration of the flight. Any adverse and unintentional physiological or psychological effects that occur from pre-flight operations through post-flight activity should be noted so that corrective actions can be taken prior to future operations.

Verification Statement: Flight crew post-flight medical assessments should be verified by inspection. The verification should be considered successful when inspection shows that the operator documents and implement any design or operational changes based on the flight crew post-flight medical assessments.

References:

- NASA-STD-3001 – Crew Health, Vol. 1, Rev B

4.4.4 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 flight early; and
c. Identify the medical criteria for ending flight early due to illnesses or medical emergencies.

Rationale: A medical condition or illness could prevent a flight crewmember from performing safety-critical operations. An infectious disease could also be spread from a space flight participant to a flight crewmember, preventing the crewmember from being able to perform their 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 operator 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, should be done to ensure the safety of occupants.

Verification Statement: The plan to isolate occupants prior to flight should be verified by inspection. Verification should be considered successful when inspection shows that quarantine and medical planning are appropriate for that mission profile.

References:

- ISS Crew Transportation and Services Requirements Document (CCT-REQ-1130) chapter 3.6.4 Health Stabilization

4.4.5 Emergency Operations Management

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

a. Launch escape, if applicable;

b. Flight abort, if applicable;

c. Occupant rescue and recovery;

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

e. Preservation of data and physical evidence for use in any anomaly or mishap investigation; and

f. Simulations and dress rehearsals for system emergencies.

Rationale: In an emergency, 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 can 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 mishap so that it can be prevented in the future.

Verification Statement: The Emergency Operations Management plan should be verified by inspection. Verification should be considered successful when inspection shows that the emergency procedures consider all possible emergency scenarios and include procedures relevant to the scenario.

References:

- 14 CFR 450.173(d), Emergency response requirements
- NPR 8705.2C – Human-Rating Requirements for Space Systems

4.5 Training

This section addresses training needs of flight crew, space flight participants, ground controllers, and safety-critical ground operations personnel.

4.5.1 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 operations are properly completed.

Verification Statement: Training requirements, completion standards, and currency requirements should be verified by inspection. The verification should be considered successful when inspection shows that the training documentation includes all safety critical roles and the training each role is to receive.

References:

- 14 CFR Part 460.5 – Crew qualifications and training

4.5.2 Safety-Critical Training

An operator should ensure that all flight crew, ground controllers, and safety-critical ground operations personnel are adequately trained and fully capable of performing their duties in a competent manner. An operator should retain completed safety-critical training records.

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

Verification Statement: Formal training records and evidence of satisfactory completion should be verified by inspection. Verification should be considered successful when inspection shows that necessary certification, licensing, or currency requirements are met prior to performance of safety and mission critical tasks.

Reference:

- 14 CFR Part 460.5 – Crew qualifications and training

4.5.3 Instructor Qualification

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

Rationale: Safe operations of the system are highly dependent upon the knowledge, experience, and currency of the instructors executing safety-critical operations training. Instructors should demonstrate knowledge of the system and the skill set to convey information such that trained personnel can execute the mission as necessary.

Verification Statement: Currency requirements for instructors conducting safety-critical training should be verified by inspection. Verification should be considered successful when inspection shows that the instructors are qualified in the applicable subject matter.

Reference:

- 14 CFR Part 450.149 - Safety-critical personnel qualifications

4.5.4 Space Flight 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 Space Flight Resource Management, and any other applicable 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 potential is especially true during dynamic, complex, or high stress situations. Space Flight Resource Management (SFRM) training helps the flight crew and ground controllers make good, informed decisions using all available resources, with emphasis on communication. Also known as Crew Resource Management in the aviation industry, SFRM is the effective use of all available resources by individuals, crews, and teams to accomplish a mission or task safely and efficiently. SFRM also identifies and manages conditions leading to error. The goal of SFRM is to improve mission effectiveness by minimizing crew preventable errors, maximizing crew coordination, and optimizing risk management. SFRM behavioral skill training includes topics such as decision making, assertiveness, mission analysis, communication, leadership, adaptability/flexibility, and situational awareness. In addition, training to recognize internal and external threats, errors, and undesired vehicle states to act as a trigger to implement SFRM skills all enhance mission effectiveness.

Verification Statement: The SFRM training program should be verified by inspection. The verification should be considered successful when inspection shows that the training program includes initial and recurrent classroom and practical and simulator training.

References:

- Advisory Circular - Crew Resource Management Training (AC 120-51E)
- Advisory Circular – Flight crew Member Line-Operational Simulations: Line-Oriented Flight Training, Special Purpose Operational Training, Line Operational Evaluation (AC 120-35D)
- Advisory Circular - Advanced Qualification Program (AC 120-54A)

4.5.5 Aerospace Physiology Training

Occupants should receive initial and recurrent aerospace physiology training, including aerospace environment, physiological stress factors (environmental, operational, and self-imposed), aerospace operations, aerospace medicine, and aerospace human factors issues.

Rationale: Space flight may have negative effects on human physiology such that occupants 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 space 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. For example, hypoxia awareness training may include an altitude chamber flight where flight crew and space flight participants can experience the effects of hypoxia in themselves and others so that they may recognize the symptoms and take action to mitigate them. In addition, extravehicular activity decompression sickness training includes the use of Nitrox by NASA if EVA operations will be conducted. Training also provides each individual with basic knowledge of aerospace medicine and operations in order to respond appropriately during these conditions.

Verification Statement: The aerospace physiology training program should be verified by inspection. The verification should be considered successful when inspection shows that initial and recurrent aerospace physiology training, including classroom and practical training, is completed for all occupants.

Reference:

- NASA Space Flight Human-System Standard: Volume 1: Crew Health (NASA-STD-3001 Vol. 1), Chapter 5.7, Physiological Exposure Mission Training

4.5.6 Psychological Training

Occupants should receive initial and recurrent psychological training, as appropriate, to address the psychological stressors and social interactions that may arise in all phases of a mission.

This training should include training and support for effective individual adaptation, crew integration, and team dynamics; training for medical as indicated in support of behavior and performance issues; and cross-cultural training support as indicated for international missions.

Rationale: Space flight and the stress of the space flight environment may have negative effects on human psychology such that occupants may become incapable of completing safety-critical operations. Psychological training may be more appropriate for orbital missions but could apply to suborbital missions for some occupants.

Verification Statement: The psychological training program should be verified by inspection. The verification should be considered successful when inspection shows that initial and recurrent psychological training, including classroom and practical training, is completed for all occupants.

Reference:

- NASA Space Flight Human-System Standard: Volume 1: Crew Health (NASA-STD-3001 Vol. 1), Chapter 5.6, Psychological Mission Training

4.5.7 Medical Training

Training for occupants should include the use and location of onboard medical equipment and supplies. Occupants should also be trained to recognize and take alternative measures when necessary medical attention exceeds the capability of the occupants and onboard equipment. The operator should examine supplies to ensure they are unexpired.

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 could 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 occupants or onboard equipment. It is important for the occupants to recognize such injuries or medical conditions in order to take alternative measures to protect themselves, such as an early return to Earth.

Verification Statement: The medical training program should be verified by inspection. The verification should be considered successful when inspection shows that classroom and practical medical training is completed for all occupants and that all medical supplies are unexpired.

References:

- NASA Space Flight Human-System Standard: Volume 1: Crew Health (NASA-STD-3001 Vol. 1), Chapter 5.2, Astronaut Training
- NASA Space Flight Human-System Standard: Volume 1: Crew Health (NASA-STD-3001 Vol. 1), Chapter 5.2.1, Crew Medical Officer Medical Training

4.5.8 Communications Training

Prior to flight, an operator should instruct each occupant on communications protocols, and prohibition against verbal interference with flight crew or safety critical ground operations personnel in performance of their safety-critical duties.

Rationale: Space flight participants should not verbally interfere with a crew member in the performance of their safety-critical operations aboard the spacecraft. During launch, flight crew may be considered part of the flight safety system, verbal interference, or failure to follow crew instruction, could impact safety of occupants. Space flight participants can also be a resource to respond to non-nominal events.

Verification Statement: The communications training program should be verified by inspection. The verification should be considered successful when inspection shows that classroom and practical communications training is completed for all occupants.

Reference:

- NIH - Health Standards for Long Duration and Exploration Spaceflight: Ethics Principles, Responsibilities, and Decision Framework. 3, Health Risks
- NPR 8705.2C – Human-Rating Requirements for Space Systems
- NASA-STD-3001 – 10.5, Communications Systems, Vol. 2, Rev C

4.5.9 Emergency Training (AST-1906)

Training for occupants should include emergency procedures along with 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 occupants on the location of onboard emergency survival equipment, and how and when to use it will allow the occupants to expeditiously access and use the equipment that may be required during extreme conditions. Training on personal survival equipment should be included so that equipment located on life vests or life preservers for example, will be covered. Additionally, training should include use of emergency equipment for pre- and post-flight scenarios.

Verification Statement: The emergency training program should be verified by inspection. The verification should be considered successful when inspection shows that classroom and practical emergency training is completed for all occupants, including the use and location of emergency equipment.

Reference:

- 14 CFR Part 460
- NIH - Health Standards for Long Duration and Exploration Spaceflight: Ethics Principles, Responsibilities, and Decision Framework. 4, Risk Acceptance and Responsibilities in Human Spaceflight and Terrestrial Activities
- NPR 8705.2C – Human-Rating Requirements for Space Systems

5.0 DEFINITIONS

NOTE: These definitions apply to this document only and are not meant to interpret any regulatory language.

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.

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. Analysis 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 any condition during licensed or permitted activity that deviates from what is standard, normal, or expected, during the verification or 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 the 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 Audit means verifying the product meets its functional and performance requirements and functions as intended. Conducting audits and quality checks ensures the integrity of the product. Functional and Physical Configuration Audits are examples of formal audit activities used to establish the product baseline. The physical configuration audit is a technical review of the CI to verify the "as-built" matches the approved baseline technical documentation.

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.

Configuration Identification means the systematic process of selecting product attributes, organizing associated information about the attributes, and stating those attributes. It includes assigning and applying unique identifiers for the product and its associated documentation, as well as maintaining document revision relationships to the product configurations. These attributes mature through each of the lifecycle phases and, at key milestones during those phases, are validated and incorporated into the baseline.

Configuration Management Planning means the configuration management strategy, implementation activities, and standard practices for performing configuration management for the project of interest.

Configuration Status Accounting (CSA) means the systematic recording and reporting of system or product configuration status. CSA reports not only communicate status, but also support conduct of formal configuration audits when design documentation is not available or has not been updated to the current configuration.

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.

Contingency 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.

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. EVA begins with depressurization of the airlock or space module and ends with repressurization of the space module or airlock after ingress.

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 crew that is on board a vehicle during a launch or reentry.

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.

Ground System means a subset of the space flight system that encompasses mission control, launch and recovery sites, and any ground-based operations supporting the mission.

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 a preventive measure or mitigation put in place for systems or operations to reduce the severity of a hazard or the likelihood of the hazard occurring.

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.

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.

Landing Site means the area within which a vehicle is expected to land on Earth.

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.

Mishap means any event, or series of events during pre-flight, flight, or post landing resulting in any of the following:

(1) A fatality or serious injury to an occupant;

(2) A malfunction of a safety-critical system;

(3) A failure of the operator's safety organization, safety operations, or safety procedures with respect to occupant safety;

(4) High risk of causing a serious or fatal injury to an occupant;

(5) Unplanned permanent loss of a vehicle; or

(6) Failure to complete a mission as planned.

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, in reference to launch vehicle performance, trajectory, or stage impact point, a launch vehicle flight where all vehicle aerodynamic parameters are as expected, all vehicle internal and external systems perform exactly as planned, and there are no external perturbing influences other than atmospheric drag and gravity.

Occupant means flight crew, government astronaut, 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 holder of a license or permit under 51 U.S.C. Subtitle V, chapter 509.

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.

Quality Management System means a set of policies, processes, and procedures required for planning and operation of launch, transport, and reentry system. ISO 9001 is an example of a Quality Management System.

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 safe performance or operation. A safety-critical system, subsystem, component, condition, event, operation, process, or item, is one whose proper recognition, control, performance, or tolerance, is essential to ensuring public safety and the safety of property.

Safety-Critical Ground Operations Personnel means any personnel that have a safety-critical role prior to, during, or after a flight operating or potentially operating systems from the earth.

Safety-Critical Personnel means any personnel that have a safety-critical role prior to, during, or after a flight.

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.

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

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.

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

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 a collection or an integrated composite of personnel, products, subsystems, elements, and processes that when combined accomplish a function and will safely carry occupants on a planned space flight.[4]

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, reentry vehicle, equipment, and supplies, but excludes payloads.

Verification means an evaluation to determine that safety measures derived from a system safety process are effective and have been properly implemented. Verification provides measurable evidence that a safety measure reduces risk to acceptable levels.

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