Approved: 2023-12-11

Measurement System Identification:

NASA TECHNICAL STANDARD

National Aeronautics and Space Administration

NASA-STD-8719.29

Approved:2023-12-11
Baseline

NASA Technical Requirements for Human-Rating

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Baseline		2023-12-11	Initial Release

FOREWORD

This NASA technical standard provides uniform engineering and technical requirements for processes, procedures, practices, and methods that have been endorsed as standard for NASA programs and projects, including requirements for selection, application, and design criteria of an item. The publication of this standard prepares the way for update of NPR 8705.2C, Human-Rating Requirements for Space Flight Systems, that will address conformity with NPR 1400.1, NASA Directivies and Charters Procedural Requirements, which mandates the exclusion of technical requirements in NASA directives. This NASA technical standard, together with the Human Rating Certification Process and associated requirements addressed in NPR 8705.2C and its' future updates, provides a complete picture of human-rating of applicable space flight systems.

This standard establishes technical requirements necessary to produce human-rated space systems that protect the safety of the crew and passengers on NASA space missions. A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards with sufficient certainty to be considered safe for human operations, and provides, to the maximum extent practical, the capability to safely recover the crew from hazardous situations.

This initial release of the standard is a direct transfer of the requirements from NPR 8705.2 chapter 3, Technical Requirements for Human-Rating, and does not introduce any new requirements or changes to existing requirements. During the comment period for this initial release, numerous comments from NASA technical experts have been accepted as "forward work" for a future revision of this standard with the intention of achieving alignment with NASA's Moon to Mars architecture and evolving paradigms with commercial partnerships.

Requests for information, corrections, or additions to this standard should be submitted to the OSMA by email to Agency-SMA-Policy-Feedback@mail.nasa.gov or via the "Email Feedback" link at https://standards.nasa.gov.

TABLE OF CONTENTS

Document History Log **2**
Foreword **3**
Table of Contents **4**

1. SCOPE **5**
1.1 Purpose 5
1.2 Applicability 5

2. APPLICABLE AND REFERENCE DOCUMENTS **5**
2.1 Applicable Documents 5
2.2 Reference Documents 6
2.3 Order of Precedence 7

3. ACRONYMS AND DEFINITIONS **7**
3.1 Acronyms and Abbreviations 7
3.2 Definitions 8

4. TECHNICAL REQUIREMENTS **13**
4.1 Overview 13
4.2 System Safety Requirements - General 14
4.3 System Safety Requirements -Failure Tolerance 15
4.4 System Control Requirements - General 20
4.5 System Control Requirements - Human-Rated Spacecraft 21
4.6 System Control Requirements - Proximity Operations with Human-Rated Spacecraft 22
4.7 Crew Survival and Abort Requirements 23

NASA TECHNICAL REQUIREMENTS FOR HUMAN-RATING

1. SCOPE

1.1 Purpose

The purpose of this standard is to define technical requirements necessary to produce human-rated space systems that protect the safety of the crew and passengers on NASA space missions.

1.2 Applicability

1.2.1 This standard is applicable to crewed space systems developed or operated by NASA and to crewed space systems used to conduct NASA human spaceflight missions as specified by NPR 8705.2.

1.2.2 This standard is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.

1.2.3 In this standard, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

2. APPLICABLE AND REFERENCE DOCUMENTS

2.1 Applicable Documents

The documents listed in this section are incorporated by reference and contain provisions that constitute requirements of this standard as cited in the text. Use of more recent issues of cited documents may be authorized by the responsible SMA Technical Authority. The applicable documents are accessible via the NASA Technical Standards System at https://standards.nasa.gov or may be obtained directly from the Standards Developing Organizations or other document distributors.

2.1.1 Government Documents

NPR 7150.2	NASA Software Engineering Requirements
NPR 8705.2	Human-Rating Requirements for Space Systems.
NPR 8715.3	NASA General Safety Program Requirements.
NASA-STD-3001 Vol. 1	Space Flight Human-System Standard: Crew Health.
NASA-STD-3001 Vol. 2	Space Flight Human-System Standard: Human Factors, Habitability, and Environmental Health.

FAA-HF-STD-001B	Human Factors Design Standard (HFDS)

2.1.2 Non-Government Documents

None.

2.2 Reference Documents

The documents listed in this section are not incorporated by reference within this standard. These references are included to provide further clarification and guidance.

2.2.1 Government Documents

NPD 7120.4	NASA Engineering and Program/Project Management Policy.
NPD 8700.1	NASA Policy for Safety and Mission Success.
NPD 8900.5	NASA Health and Medical Policy for Human Space Exploration.
NPR 7120.5	NASA Space Flight Program and Project Management Requirements.
NPR 7120.10	Technical Standards Products for NASA Programs and Projects.
NPR 7123.1	Systems Engineering Processes and Requirements.
NPR 8000.4	Agency Risk Management Procedural Requirements.
NPR 8900.1	Health and Medical Requirements for Human Space Exploration.
NASA-STD-5005	Standard for The Design and Fabrication of Ground Support Equipment.
NASA-HDBK-8709.22	Safety and Mission Assurance Acronyms, Abbreviations, and Definitions
NASA/SP-2007-6105, Rv1	NASA Systems Engineering Handbook, 2007.
NASA/SP-2011-3421	Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, 2011.
NASA/SP-2015-3709	Human Systems Integration (HSI) Practitioner's Guide, 2015.

NASA-SP-6104	A Perspective on the Human Rating Process of Spacecraft: Both Past and Present, G. Zupp et al., 1995.NASA
NASA-TND-5153	The Use of Pilot Rating in the Evaluation of Aircraft Handling Qualities
NASA-TM-X-65248	System Safety Requirements for Manned Space Flight," NASA Manned Flight Safety Office, January 1969
MIL-STD-1472	Department of Defense Design Criteria Standard - Human Engineering.

2.3 Order of Precedence

2.3.1 Where conflicts exist between this standard and applicable federal regulations, the applicable regulations take precedence.

2.3.2 Where conflicts exist between this standard and applicable Agency directives, the applicable Agency directives take precedence.

2.3.3 Where conflicts exist between this standard and standards that contain provisions that constitute requirements of this standard as cited in the text, this standard takes precedence, except in the case where those standards are to federal regulations.

2.3.4 Where conflicts exist between a requirement that is meant to be applied generally across all technical disciplines and a requirement that is applicable to a specific technical discipline, the requirement that is applicable to a specific technical discipline takes precedence.

2.3.5 Clarification and further resolution of conflicts is resolved by the responsible SMA Technical Authority.

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

EVA	Extravehicular activity
HEA	Human error analysis
HQR	Handling qualities rating
HRCP	Human rating certification plan
JSC	Johnson Space Center
SMA	Safety and mission assurance

3.2 Definitions

Note: The following definitions are from NPR 8705.2 revision C.

Abort. The forced early return of the crew to Earth when failures or the existence of uncontrolled catastrophic hazards prevent continuation of the mission profile and a return to Earth is required for crew survival. The crew is safely returned to Earth in the space system nominally used for entry and landing/touchdown. [source NPR 8705.2]

Automated. Automatic (as opposed to human) control of a system or operation. [source NPR 8705.2]

Autonomous. Ability of a space system to perform operations independent from any Earth-based systems. This includes no communication with, or real-time support from, mission control or other Earth systems. [source NPR 8705.2]

Catastrophic event. An event resulting in the death or permanent disability of a crew member or passenger or an event resulting in the unplanned loss/destruction of a major element of the crewed space system during the mission that could potentially result in the death or permanent disability of a crew member or passenger. [source NPR 8705.2]

Catastrophic hazard. Any hazard that, when uncontrolled, results in a catastrophic event. [source NPR 8705.2]

Crew. Any human on board the space system during the mission that has been trained to monitor, operate, and control parts of, or the whole space system; same as flight crew. [source NPR 8705.2]

Crew escape. See definition for escape.

Crew survival. Capability and ability to preclude crew/passenger fatality or permanent disability. The ability to keep the crew/passengers alive using such capabilities as abort, escape, safe haven, emergency egress, rescue and emergency medical, in response to an imminent catastrophic condition. [source NPR 8705.2]

Crewed element (of the space system). All system elements that are occupied by the crew/passengers during the space mission and provide critical services to the crew/passengers(e.g., life support). The crewed element includes all the subsystems that provide life support functions for the crew/passengers. [source NPR 8705.2]

Crewed space system. The crewed space system consists of all the system elements that are occupied by the crew/passengers during the space mission and provide life support functions for the crew/passengers (i.e., the crewed elements). The crewed space system also includes all elements physically attached to the crewed element during the mission. The crewed space system is part of the larger space system used to conduct the mission. [source NPR 8705.2]

- The following examples are provided for clarification of the definition of crewed space system as it relates to the Human-Rating Certification:

- Application example 1: A launch vehicle for a crewed spacecraft on a NASA mission is part of the crewed space system for Earth ascent. In this example, the Human-Rating Certification applies to the launch vehicle and the spacecraft operating together as a crewed space system during the ascent phase of the reference mission.

- Application example 2: A propulsion module, which is launched into space (un-crewed) and subsequently attached to a crewed spacecraft on a NASA mission, is part of the crewed space system for the Human-Rating Certification. As part of the certification, some of the requirements in this standard will apply to the propulsion module during proximity operations with the crewed spacecraft.

- Application example 3: The launch vehicle for the propulsion module in example 2 (when launched separately from crew) is not part of the crewed space system and will not be part of the Human-Rating Certification.

- Application example 4: When the crew ingresses a vehicle for a launch attempt, the vehicle is physically connected to the launch pad. The entire launch pad is not considered part of the crewed system, but the specific launch pad systems that interact with the crewed vehicle are part of the crewed space system.

Critical software. Any software component whose behavior or performance could lead to a catastrophic event or abort. This includes the flight software as well as ground-control software. [source NPR 8705.2]

Critical (sub)system. A (sub)system is assessed as critical if loss of overall (sub)system function, or improper performance of a (sub)system function, could result in a catastrophic event or abort. [source NPR 8705.2]

Earth ascent abort. An abort performed during Earth ascent, where the crewed spacecraft is separated from the launch vehicle without the capability to achieve a safe stable orbit. The crew is safely returned to Earth in a portion of the spacecraft nominally used for entry and landing/touchdown. [source NPR 8705.2]

Emergency egress. Capability for a crew and passengers to exit the vehicle and leave the hazardous situation or catastrophic event within the specified time. Crew/passenger emergency egress can be unassisted or assisted by ground personnel. [source NPR 8705.2]

Emergency equipment and systems. A set of components (hardware and/or software) used to mitigate or control hazards, after occurrence, which present an immediate threat to the crew or crewed spacecraft. Examples include fire suppression systems and

extinguishers, emergency breathing devices, and crew escape systems. [source NPR 8705.2]

Escape. Removal of crew and passengers from the portion of the space system normally used for reentry, due to rapidly deteriorating and hazardous conditions, thus, placing them in a safe situation suitable for survivable return or recovery. Escape includes, but is not limited to, those modes that utilize a portion of the original space system for the removal (e.g., pods, modules, or fore bodies). [source NPR 8705.2]

Failure. Inability of a system, subsystem, component, or part to perform its required function within specified limits. [source NPR 8705.2]

Failure tolerance. The ability to sustain a certain number of failures and still retain capability. [source NPR 8705.2]

Fault. An undesired system state and/or the immediate cause of failure (e.g., maladjustment, misalignment, defect, or other). The definition of the term "fault" envelopes the word "failure," since 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. [source NPR 8705.2]

Hazard. A state or a set of conditions, internal or external to a system, which has the potential to cause harm. [source NPR 8705.2]

Human error. Either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence. [source NPR 8705.2]

Human error analysis (HEA). A systematic approach to evaluate human actions, identify potential human error, model human performance, and qualitatively characterize how human error affects a system. HEA provides an evaluation of human actions and error in an effort to generate system improvements that reduce the frequency of error and minimize the negative effects on the system. HEA is the first step in Human Risk Assessment and is often referred to as qualitative Human Risk Assessment. [source NPR 8705.2]

Human performance. The physical and mental activity required of the crew and other participants to accomplish mission goals. This includes the interaction with equipment, computers, procedures, training material, the environment, and other humans. [source NPR 8705.2]

Human-rated space system. A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards with sufficient certainty to be considered safe for human operations, and provides the capability to safely recover from emergency situations. The concept of human-rating a space system entails three fundamental tenets: [source NPR 8705.2]

1. Human-rating is the process of evaluating and assuring that the total system can safely conduct the required human missions.

2. Human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success.

3. Human-rating includes the incorporation of design features and capabilities to enable safe recovery of the crew from hazardous situations.

Human-rating certification. Human-Rating Certification is the documented authorization granted by the NASA Administrator that allows the program manager to operate the space system within its prescribed parameters for its defined reference missions. Human-Rating Certification is obtained prior to the first crewed flight (for flight vehicles) or operational use (for other systems). [source NPR 8705.2]

Human system integration. The process of integrating human operations into the system design through analysis, testing, and modeling of human performance, interface controls/displays, and human-automation interaction to improve safety, efficiency, and mission success.

Landing. The final phase or region of flight to Earth/Lunar surface consisting of transition from descent, to an approach, touchdown, and coming to rest. [source NPR 8705.2]

Manual control. The crew's ability to bypass automation in order to exert direct control over a space system or operation. For control of a spacecraft's flight path, manual control is the ability for the crew to effect any flight path within the capability of the flight control system. Similarly, for control of a spacecraft's attitude, manual control is the ability for the crew to effect any attitude within the capability of the flight/attitude control system. [source NPR 8705.2]

NASA human spaceflight missions. Terminology used to distinguish human spaceflight missions that require human-rated systems per NPR 8705.2. Any human spaceflight mission where NASA retains the mission decision authority and the responsibility for crew safety is considered a NASA mission. [source NPR 8705.2]

Operator. Any human interacting with the crewed space system during the mission. [source NPR 8705.2]

Override. To take precedence over system control functions. [source NPR 8705.2]

Passenger. Any human on board the space system while in flight that has no responsibility to perform any mission task for that system. Often referred to as "Space Flight Participant." [source NPR 8705.2]

Permanent disability. A non-fatal occupational injury or illness resulting in permanent impairment through loss of, or compromised use of, a critical part of the

body, to include major limbs (e.g., arm, leg), critical sensory organs (e.g., eye), critical life-supporting organs (e.g., heart, lungs, brain), and/or body parts controlling major motor functions (e.g., spine, neck). Therefore, permanent disability includes a non-fatal injury or occupational illness that permanently incapacitates a person to the extent that he or she cannot be rehabilitated to achieve gainful employment in their trained occupation and results in a medical discharge from duties or civilian equivalent. [source NPR 8705.2]

Probabilistic safety critieria. The specification of a criterion for a probabilistic safety metric (e.g., the probability of a loss of crew) and the degree of certainty with which such criteria must be met. [source NPR 8705.2]

Proximity operations. Two or more vehicles operating in space near enough to each other so as to have the potential to affect each other. This includes rendezvous and docking (including hatch opening), undocking, and separation (including hatch closing). [source NPR 8705.2]

Rescue. The process of locating the crew, proceeding to their position, providing assistance, and transporting them to a location free from danger. [source NPR 8705.2]

Risk. The combination of (1) the probability (qualitative or quantitative) including associated uncertainty that the space system will experience an undesired event (or sequences of events) such as internal system or component failure or an external event and (2) the magnitude of the consequences (personnel, public, and mission impacts) and associated uncertainties given that the undesired event(s) occur(s). [source NPR 8705.2]

Risk assessment. An evaluation of a risk item that determines (1) what can go wrong, (2) how likely is it to occur, and (3) what the consequences are. [source NPR 8705.2]

Risk posture. An expression of the agreed upon limits of risk an organization's leadership team is willing to accept in order to achieve one or more of its objectives. It is defined up front and in tandem with the development of objectives, consistently with Risk Leadership principles, and serves as the attitudinal framework for seeking a balance between the likelihood and benefit of achieving the objective(s), vs. the likelihood and severity of risks that may be introduced by the pursuit of achievement. Risk posture may change with time, in reflection of the evolution of leadership team attitudes or because of changes in priorities, but at any particular time, risk posture provides the de-facto basis for risk-informed decision making and continuous risk management. [source NPR 8000.4]

Safe haven. A functional association of capabilities and environments that is initiated and activated in the event of a potentially life-threatening anomaly and allows human survival until rescue, the event ends, or repair can be affected. [source NPR 8705.2]

Safety. The absence from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. [source NPR 8705.2]

Safety goal. The level of safety that serves as a long-term target for repeatedly flown missions, specified at the system level in terms of an aggregate measure of risk to the crew such as the probability of a loss of crew. [source NPR 8705.2]

Safety threshold. The minimum tolerable level of safety for a given reference mission, specified at the system level in terms of an aggregate measure of risk to the crew such as the probability of a loss of crew. [source NPR 8705.2]

Space system. The collection of all space-based and ground-based systems (encompassing hardware and software) used to conduct space missions or support activity in space, including, but not limited to, the crewed space system, space-based communication and navigation systems, launch systems, and mission/launch control. Also, referred to as "system" in the technical requirements. [source NPR 8705.2]

Subsystem. A secondary or subordinate system within a system (such as the crewed space system) that performs a specific function or functions. Examples include electrical power, guidance and navigation, attitude control, telemetry, thermal control, propulsion, structures subsystems. A subsystem may consist of several components (hardware and software) and may include interconnection items such as cables or tubing and the support structure to which they are mounted. [source NPR 8705.2]

Technical Authority. The individuals who provide independent oversight of programs and projects in support of safety and mission success, who have formally delegated authority traceable to the Administrator, and are funded independent of Programmatic Authority. [source NPR 8705.2]

4. TECHNICAL REQUIREMENTS

4.1 Overview

4.1.1 A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards with sufficient certainty to be considered safe for human operations, and provides, to the maximum extent practical, the capability to safely recover the crew from hazardous situations within the framework of the chosen risk posture.

4.1.2 The technical requirements in this chapter identify capabilities in three primary categories:

a. System Safety

b. Crew/Human Control of the System

c. Crew Survival and Aborts

4.1.3 These requirements form a high-level compliance framework for human-rating, but are not all-inclusive for every specific space system. Additional requirements or unique considerations may be levied at other system or sub-system levels by applicable Technical Authorities in order to ensure the system fully meets safety considerations for human missions

into space. Full complaince for human rating occurs when all levied requirements or considerations at each level have been appropriately addressed.

Rationale: The reference missions establish a basis and framework that the program can use to establish the operational scenarios and document the strategies that will be used to enhance crew survival. Incorporating and preserving the capability for the crew to safely return from the mission is a fundamental tenet of human-rating. The scenarios should include system failures and emergencies (such as fire, collision, toxic atmosphere, decreasing atmospheric pressure, and medical emergencies) with specific capabilities (such as abort, safe haven, rescue, emergency egress, emergency systems, and emergency medical equipment or access to emergency medical care) identified to protect the crew. Some specific capabilities, such as abort, are mandated by the technical requirements in Section 4 of this NASA Standard. The intent of this requirement is to have the program identify additional capabilities for their specific design that enhance crew survival. Additionally, the program describes how the survival capabilities will be maintained during the scenarios. The broad strategies and the process used to develop both the reference missions and the strategies that respond to the scenarios help to establish a focus within the program of making crew survival an integral element of the design process. Continued challenges to (and deliberations concerning) the scenarios themselves and the assumptions, analyses, and design decisions that flow from these scenarios are essential to successfully obtaining Human-Rating Certification.

4.1.4 Furthermore these requirements were intentionally written to force the design team to bound the complex problem of human safety. The design team should evaluate the intent and rationales of these technical requirements and use their knowledge, experience, and talents to appopriately apply these requriements to deliver the safest practical system that accomplishes the mission within constraints. They may be guided (directly or indirectly) by safety goals and thresholds defining long-term targeted and minimum tolerable levels of safety (maximum tolerable levels of risk).

4.1.5 The technical requirements are presented in sections to clearly identify the applicable mission phase and applicable system type. The term "space system" (defined in Section 3.2) includes the crewed space system and all space-based and ground-based systems that functionally interact with the crewed space system during the mission.

4.2 System Safety Requirements - General

4.2.1 The space system shall provide a safe environment for crew habitation.

Rationale: Protection from the hazardous environment of space or the hazardous environment at the planetary surface is fundamental to crew survival. Also, the space system should be inherently safe or designed to minimize risk (e.g., no exposed sharp edges, no exposed high temperature surfaces). This requirement includes protection from known environments such as space radiation hazards and lunar dust. Providing a habitable environment is also fundamental to the integration of the human into the space system. In order for the crew to contribute to the safe conduct of the mission, their basic habitability needs to be met. Satisfying the applicable standards listed in

paragraph 2.2.1 constitutes a safe, habitable environment for the purposes of this requirement.

4.2.2 The space system shall meet probabilistic safety criteria derived from the Agency-level safety goals and safety thresholds with a specified degree of certainty.

Note: Probabilistic safety analysis methods provide one basis for the comparison of design options in context of integrating design and safety analyses. Probabilistic safety requirements, based on Agency-level safety goals, safety thresholds, and associated rationale as defined by the Associate Administrator for the responsible NASA Mission Directorate and approved by the NASA Administrator, establish criteria for safety metrics such as loss of crew probabilities that are an outcome of such analyses. The analyses must consider the uncertainty associated with calculated values and the degree of certainty that the probabilistic criteria are met. The required degree of certainty is specified as part of the probabilistic safety requirements. Even when these metrics are determined in accordance with accepted analysis protocols, it is still recognized that as an analytical tool, probabilistic safety analysis methods rely on assumptions and are subject to uncertainties. Calculated values of such safety metrics are, therefore, not in themselves sufficient to determine that a system is safe. Consequently, compliance with probabilistic requirements can only be an element of the case to be made that a system provides an acceptable level of safety. Key considerations include:

a. A list of the significant risk contributors that together constitute the majority of the total risk to which the crew is subjected.

b. The appropriate hazard controls and mitigations to reduce the risk to the crew, including the level and implementation of failure tolerance to catastrophic events for the space system.

c. Specific rationale for dynamic flight phases where dissimilar redundancy, backup systems, or abort capabilities are not available to limit the likelihood of a catastrophic event or the loss of crew.

d. The effectiveness of crew survival capabilities under conditions and time constraints to be encountered during high-risk accident conditions and their impact on the risk to the crew.

e. The level of risk to the crew and associated uncertainty determined via analysis performed in accordance with accepted probabilistic safety analysis protocols and supported by documented evidence including ground and flight test data.

4.3 System Safety Requirements -Failure Tolerance

4.3.1 The space system shall provide at least single failure tolerance to catastrophic events, with specific levels of failure tolerance and implementation (similar or dissimilar redundancy) derived via an integration of the design and safety analysis (required by NPR 8705.2).

4.3.1.1 Failure of primary structure, structural failure of pressure vessel walls, and structural failure of pressurized lines are exempted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.

4.3.1.2 Other potentially catastrophic hazards that cannot be controlled using failure tolerance are exempted from the failure tolerance requirements with mandatory concurrence (as required by NPR 8705.2) from the Technical Authorities and the Director, JSC (for crew risk acceptance) provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.

Rationale: The overall objective is to arrive at the safest practical design to accomplish a mission. Since space system development will always have mass, volume, schedule, and cost constraints, choosing where and how to apply failure tolerance requires integrated analyses at the system level to assess safety and mission risks, guided by a commonly understood level of risk tolerance at the system and local (individual hazard) levels.

First and foremost, the failure tolerance is applied at the overall system level - to include all capabilities of the system. While failure tolerance is a term frequently used to describe minimum acceptable redundancy, it may also be used to describe two similar systems, dissimilar systems, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures or additional features designed to mitigate the effects of failures. Even when assessing failure tolerance at the integrated system level, the increased complexity and the additional utilization of system resources (e.g. mass, power) required by a failure tolerant design may negatively impact overall system safety as the level of failure tolerance is increased.

The level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Redundancy does not soley make a system safe. It is the responsibility of the engineering and safety teams to determine the when redundancy must be included, how to best implement it, or alternatively why a single string design approach is sufficient. The resulting design should optimize safety given the mission requirements and constraints.

Note: Redundancy alone does not meet the intent of this requirement. When a critical system fails because of improper or unexpected performance due to unanticipated conditions, similar redundancy can be ineffective at preventing the complete loss of the system. Dissimilar redundancy can be very effective provided there is sufficient separation among the redundant legs. (For example, dissimilar redundancy where the power for all redundant capability was routed through a common conduit would not survive a failure where the conduit was severed). It is also highly desirable that the spaceflight system performance degrades in a predictable fashion to allow sufficient

time for failure detection and, when possible, system recovery even when experiencing multiple failures.

There are examples of dissimilar redundancy in current systems. For Earth reentry, the Soyuz spacecraft has a dissimilar backup ballistic entry mode to protect for loss of the primary attitude control system and a backup parachute for landing. Other examples include backup batteries for critical systems that protect for loss of the primary electrical system and the use of pressure suits during reentry to protect for loss of cabin pressure.

Ultimately, the program and Technical Authorities evaluate and agree on the failure scenarios/modes and determine the appropriate level of failure tolerance and the practicality of using dissimilar redundancy or backup systems to protect for common cause failures.

Where failure tolerance is not the appropriate approach to control hazards, specific measures need to be employed to: (1) Identify applicable hazards and their associated controls; (2) Ensure robustness of the design; and (3) Ensure adequate attention/focus is being applied to the design, manufacture, test, analysis, and inspection of the items. In the area of design, in addition to the application of specifically approved standards and specifications, these measures can include identification of specific design features which minimize the probability of occurrence of failure modes, such as application of stringent factors of safety or other design margins. For manufacture, these measures can include establishing special process controls and documentation, special handling, and highlighting the importance of the item for those involved in the manufacturing process. For test, this can include accelerated life testing, fleet leader testing program, testing to understand failure modes or other testing to establish additional confidence and margin in the design. For analysis (in lieu of tests), these measures can include correlation with testing representative of the actual configuration and the collection, management, and analysis of data used in trending failures, verifying loss of crew requirements, and evaluating flight anomalies. For inspection, these measures can include identification of specific inspection criteria to be applied to the item or the application of Government Mandatory Inspection Points or similar audits for important characteristics of the item. This approach to hazard control takes advantage of existing standards or standards approved by the Technical Authorities to control hazards associated with the physical properties of the hardware and are typically controlled via application of margin to the environments experienced by the design or system properties effected by the environment. Acceptance of these approaches by the Technical Authorities avoids processing waivers for numerous hazard causes where failure tolerance is not the appropriate approach. This includes, but is not limited to, Electro-Magnetic Interference, Ionizing Radiation, Micrometeoroid Orbital Debris, structural failure, pressure vessel failure, and aerothermal shell shape for flight.

4.3.2 The space system shall provide the failure tolerance capability without the use of emergency equipment and systems.

Rationale: Emergency systems and equipment, such as fire suppression systems, fire extinguishers and emergency breathing masks, launch and entry pressure suits, and systems used exclusively for launch aborts, should not be considered part of the failure tolerance capability since these emergency systems and equipment cannot definitely prevent a catastrophic initiating event. In the example of the fire extinguisher, the fire can burn out of control and overwhelm the capability of the extinguisher. Emergency systems are there 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. Catastrophic events, as defined in this standard and consistent with NPR 8715.3, NASA General Safety Program Requirements, include crew fatality and the unplanned loss of a major element of the crewed space system during the mission that could potentially lead to death or permanent disability of the crew or passengers.

Note: An early mission termination utilizing nominal systems and operations is not considered to be part of emergency equipment and systems; and may, therefore, be considered part of the failure tolerance of the system. However, when aborts are used to remove the crew from a catastrophic event (e.g., abort on Earth ascent in the presence of a launch vehicle explosion), the catastrophic event has not been prevented, and the abort system (even though it may save the crew and passengers) cannot be considered as a leg of failure tolerance to the catastrophic event.

4.3.3 The space system shall be designed to tolerate inadvertent operator action (minimum of one inadvertent action), as verified by a human error analysis, without causing a catastrophic event.

Note: An operator is defined as any human that commands or interfaces with the space system during the mission, including humans in the control centers. The appropriate level of protection (i.e., one, two or more inadvertent actions) is determined by the integrated human error and hazard analysis per NPR 8705.2.

4.3.4 The space system shall tolerate inadvertent operator action, as described in Section 4.3.3, in the presence of any single system failure.

Rationale: The intent of this requirement is to provide a robust human-system interface design that cannot be defeated by a system failure. Where the system is designed to protect for more than one inadvertent action, the level of protection after a single system failure may be reduced - but still protects from a single inadvertent operator action.

4.3.5 The space system shall provide the capability to mitigate the hazardous behavior of critical software where the hazardous behavior would result in a catastrophic event.

Note 1: According to current software standards, the software system will be designed, developed, and tested to:

Note 2: Prevent hazardous software behavior.

Note 3: Reduce the likelihood of hazardous software behavior.

Note 4: Mitigate the negative effects of hazardous software behavior. However, for complex software systems, it is very difficult to definitively prove the absence of hazardous behavior. Therefore, the crewed system has the capability to mitigate this hazardous behavior if it occurs. The mitigation strategy will depend on the phase of flight and the time to effect of the potential hazard. Hazardous behavior includes erroneous software outputs or performance.

4.3.6 The space system shall provide the capability to detect and annunciate faults that affect critical systems, subsystems, or crew health.

Rationale: It is necessary to alert the crew to faults (not just failures) that affect critical functions. A fault is defined as an undesired system state. A failure is an actual malfunction of a hardware or software item's intended function. The definition of the term fault envelopes the word failure, since faults include other undesired events such as software anomalies and operational anomalies.

4.3.7 The space system shall provide the capability to isolate and recover from faults identified during system development or mission operations that would result in a catastrophic event.

Note: This capability is not intended to imply a failure tolerance capability or expand upon the failure tolerance capability. The intent is to provide isolation and recovery from faults where the system design (e.g., redundant strings or system isolation) enables the implementation of this capability. Also, any faults identified during system development should be protected by isolation and recovery. However, it is acknowledged that not all faults that would cause catastrophic events can be detected or isolated in time to avoid the event. Similarly, system design cannot ensure that once the fault is detected and isolated that a recovery is always possible. In cases where recovery is not possible, isolation of the fault needs to be sufficient on its own to prevent the catastrophic event.

4.3.8 The space system shall provide the capability to utilize health and status data (including system performance data) of critical systems and subsystems to facilitate anomaly resolution during and after the mission.

Rationale: Access to health and status data is a key element of anomaly resolution during the mission, which could prevent the crew from executing an abort or prevent the situation from developing into a catastrophic event. Resolving anomalies between missions is just as important. This requirement intentionally does not specify a crash survivable data recorder. That determination is left for the program. The program also determines what data should be available to facilitate anomaly resolution.

4.3.9 The crewed space system shall provide the capability for autonomous operation of system and subsystem functions which, if lost, would result in a catastrophic event.

Note: This capability means that the crewed system does not depend on communication with Earth (e.g., mission control) to perform functions that are required to keep the crew alive(refer to the definition for Autonomous in Section 3.2).

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

Note: Fire extinguishers are one example of the type of equipment needed for immediate response to a fire emergency. Ready access means that the crew is able to access the equipment in the time required without the use of tools. The ready access time will depend on the phase of flight and the time to effect of the hazard. Ready access also accounts for suited crew members if the equipment could be needed during a mission phase or operation where the crew is suited. A contamination clean-up kit is an example of equipment needed for follow up and recovery operations.

4.4 System Control Requirements - General

4.4.1 The crewed space system shall provide the capability for the crew to monitor, operate, and control the crewed space system and subsystems, where:

a. The capability is necessary to execute the mission; or

b. The capability would prevent a catastrophic event; or

c. The capability would prevent an abort.

Rationale: This capability flows directly from the definition of human-rating. Within the context of this requirement, monitoring is the ability to determine where the vehicle is, its condition, and what it is doing. Monitoring helps to create situational awareness that improves the performance of the human operator and enhances the mission. Determining the level of operation over individual functions is a decision made separately for specific space systems. Specifically, if a valve or relay can be controlled by a computer, then that same control could be offered to the crew to perform that function. However, a crew member probably could not operate individual valves that meter the flow of propellant to the engines, but the function could be replaced by a throttle that incorporates multiple valve movements to achieve a desired end state (reduce or increase thrust). Meeting any of the three stated conditions invokes the requirement. The first condition recognizes that the crew performs functions to meet mission objectives and, in those cases, the crew is provided the designated capabilities. This does not mean that the crew is provided these capabilities for all elements of a mission. Many considerations are involved in making these determinations, including capability to perform the function and reaction time. The second and third conditions recognize that, in many scenarios, the crew improves the performance of the system and that the designated capabilities support that performance improvement.

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

Rationale: This is a specific capability necessary for the crew to control the crewed space system. While this capability should be derived by the program per paragraph 4.3.1, the critical nature of software control and automation at the highest system level dictates specific mention in this standard. Therefore, the crew has the capability to control automated configuration changes and mode changes, including automated aborts, at the system level as long as the transition to manual control is feasible and will not cause a catastrophic event. The program and Technical Authorities will determine the appropriate implementation of this requirement - which is documented in the program's Human Rating Certification Plan (HRCP) and evidenced by HRCP deliverables.

4.4.3 The space system shall provide the capability for humans to remotely monitor, operate, and control the crewed system elements and subsystems, where:

a. The remote capability is necessary to execute the mission; or

b. The remote capability would prevent a catastrophic event; or

c. The remote capability would prevent an abort.

Rationale: This capability will likely be implemented using a mission control on Earth. Logically, there will be times when the crew is unavailable to monitor, operate, and control the system. If the crew vacates one element of the system or transfers to another Human-Rated system as part of the reference mission, there is a capability for humans to monitor the unoccupied elements. In some of these cases, the crew may be able to perform this function from their new location. In other cases, mission control may perform this function.

Note: This capability is not intended to force 100 percent of communication coverage for all elements of the system. The communication coverage is planned to implement the capability to meet the three conditions.

Note: For EVA suits, this capability does not mean that the EVA suit requires constant monitoring between EVAs (missions). If the suit is powered off and stowed, periodic checks or inspections may be all that is required.

4.5 System Control Requirements - Human-Rated Spacecraft

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

Rationale: The capability for the crew to control the spacecraft's flight path is a fundamental element of crew survival. The most robust satisfaction of this requirement is provided by direct manual control of the vehicle flight path, through an independent flight control system (bypassing the affected vehicle guidance, navigation, and flight control system failures). A minimum implementation of manual control allows for the

crew to bypass the automated guidance of the vehicle by interfacing directly with the flight control system to effect any possible flight path within the capability of the flight control system. Limiting the crew to choices presented by the automated guidance function is not a valid implementation of manual control.

Note: For phases of flight where there is no active control of the spacecraft, such as when under passive parachutes, then manual control cannot be provided and this requirement would not apply. For a space station, when there is no propulsion system available for reboost, then manual control of the flight path (orbital parameters) cannot be provided, and this requirement would not apply. During the atmospheric portion of Earth ascent (approximately the first 100,000 feet), where the trajectory and attitude are tightly constrained to maintain positive structural and thermal margins, the trajectory and attitude constraints are not typically available independent of guidance. In this case, if the only option is for the crew to follow guidance then nothing is gained by manual control over automated control.

Note: Manual control cannot be safely or accurately performed without the situational awareness tools to provide status, feedback, and flight control direction. Safe operation requires both accuracy of crew inputs and piloting handling qualities to meet human rating requirements. Tools include, but are not limited to, telemetry, displays, video, instrumentation, and windows. Tools will be verified in a cockpit environment to ensure they are adequate to support manual control and operations.

4.5.2 The crewed spacecraft shall exhibit Level 1 handling qualities (Handling Qualities Rating (HQR) 1, 2 and 3), as defined by the Cooper-Harper Rating Scale, during manual control of the spacecraft's flight path and attitude for crew manual control events when the vehicle has not had failures which result in degraded flight control.

Rationale: Level 1 handling qualities are the accepted standard for manual control of flight path and attitude in military aircraft for the majority of flight scenarios. Level 1 handling qualities will allow the crew to effectively control the spacecraft when necessary for mission completion or to prevent a catastrophic event. Level 2 handling may be acceptable for cases where either the inherent difficulty of the flight scenario suggests Level 2 is acceptable or when vehicle failures have resulted in a degraded flight control. Reference NASA TND-5153 for the Cooper-Harper Rating Scale.

4.6 System Control Requirements - Proximity Operations with Human-Rated Spacecraft

4.6.1 The space system shall provide the capability for the crew to monitor, operate, and control an uncrewed spacecraft during proximity operations, where:

a. The capability is necessary to execute the mission; or

b. The capability would prevent a catastrophic event; or

c. The capability would prevent an abort.

Note 1: Proximity operations cover several scenarios, but this term is specifically defined as two (or more) systems operating in space (not on a planetary surface) within the prescribed safe zone for either system.

Note 2. When an uncrewed space system is the active spacecraft performing proximity operations with a crewed spacecraft, this requirement includes the capability for the crew to monitor the trajectory of the uncrewed system. At a minimum, the crewed system will have the capability to send basic trajectory commands to hold/stop, continue, and breakout to the uncrewed spacecraft. Active means the spacecraft is changing the flight trajectory and orbital parameters to effect the desired result during proximity operations.

4.6.2 The crewed space system shall provide the capability for direct voice communication, ship-to-ship without relay through another system, between crewed spacecraft (two or more) during proximity operations.

4.7 Crew Survival and Abort Requirements

4.7.1 Earth Ascent Systems

4.7.1.1 The space system shall provide the capability for unassisted crew emergency egress to a safe haven during Earth prelaunch activities.

4.7.1.2 The space system shall provide abort capability from the launch pad until Earth-orbit insertion to protect for the following ascent failure scenarios:

a. Complete loss of ascent thrust/propulsion.

b. Loss of attitude or flight path control.

Rationale: Flying a spacecraft through the Earth's atmosphere to orbit entails inherent risk. Three crewed launch vehicles have suffered catastrophic failures during ascent or on the launch pad (one Space Shuttle and two Soyuz spacecraft). Both Soyuz crews survived the catastrophic failure due to a robust ascent abort system. Analysis, studies, and past experience all provide data supporting ascent abort as the best option for the crew to survive a catastrophic failure of the launch vehicle. As specified in 4.7.1.3, the ascent abort capability incorporates some type of vehicle monitoring to detect failures and, in some cases, impending failures.

Note: NASA/SP-2011-3421, Chapter 14, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, 2011, provides guidance on the evaluation of abort capability effectiveness in the context of probabilistic safety analyses.

4.7.1.3 The crewed space system shall monitor the Earth ascent launch vehicle performance and automatically initiate an abort when an impending catastrophic failure is detected.

Note: Launch vehicle performance monitoring may include specific system or subsystem performance. The program will determine the appropriate parameters to monitor in the

launch vehicle. Not all potentially catastrophic failures can be detected prior to manifestation. Similarly, system design and analysis cannot guarantee the crew will survive all catastrophic failures of the launch system, but the abort system should provide the best possible chance for the crew to survive. When an impending catastrophic failure of the launch vehicle is detected, the time to effect requires the abort system to be initiated automatically. Also, if the catastrophic failure itself is detected by a monitoring system, the abort is initiated automatically. This is not intended to require independent implementation by the crewed space system of capabilities inherent to the launch vehicle (the launch vehicle is part of the crewed space system).

4.7.1.4 Earth Ascent Abort

4.7.1.4.1 The space system shall provide the capability for the crew to initiate the Earth ascent abort sequence.

Note: The ability to inhibit an automated abort initiation is described in paragraph 4.3.2.

4.7.1.4.2 The space system shall provide the capability for the ground control to initiate the Earth ascent abort sequence.

Rationale: The crew and ground control will likely have access to more data than an automated abort system. Therefore, both the crew and ground control have the capability to initiate the abort when necessary for crew survival.

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

Rationale: Prior to destruction of the launch vehicle by means of a range safety destruct (flight termination) system, the abort system is initiated. An automated initiation of the abort sequence provides the best chance for crew survival while protecting the public from a range safety violation. It is left to the program to determine which range safety command (arm or fire) will result in the initiation of the abort sequence.

4.7.2 Earth Orbit Systems

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

Note: Where possible, the crewed space system should provide a backup capability for entry to protect for loss of the primary attitude control and guidance system. Integration of design and safety analyses, per NPR 8705.2, addresses scenarios where this may not be applicable.

4.7.3 Earth - Lunar Transit and Lunar Orbit Systems

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

4.7.4 Lunar Descent Systems

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

Note: The extent of abort coverage is to be determined by the program. The goal is 100 percent coverage during the descent.

4.7.5 Lunar Surface Systems

The space system shall provide the capability for the crew on the lunar surface to monitor the descent and landing trajectory of an uncrewed spacecraft and send commands necessary to prevent a catastrophic event.

Note: This capability assumes the arrival is within the safe zone of the crew or crewed surface systems.

4.7.6 Lunar Ascent Systems

Note: Reserved for potential future development.

4.7.7 Earth Reentry Systems

4.7.7.1 The crewed space system shall provide the capability for unassisted crew emergency egress after Earth landing.

Note: This requirement assumes the crew is able to function in a 1-g environment. Unassisted means without help from ground or rescue personnel or equipment.

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

Rationale: If the crew is physically unable to egress the spacecraft or does not choose to egress the spacecraft due to a hazardous environment outside, then the spacecraft provides a safe haven until the arrival of recovery forces. This requirement is not intended to establish the boundaries of the hazardous environment (for example, the maximum sea state) or the duration of the safe haven. The program, with concurrence from the Technical Authorities, specifies these conditions in their requirements documents. The nominal return to Earth will have well established timelines and expectations for the habitation conditions inside the spacecraft. Conversely, after an ascent abort or emergency return to Earth, the timeline may be less certain and the expectations of comfort will be different from the nominal mission return.

4.7.7.3 The space system shall provide recovery forces with the location of the spacecraft after return to Earth.

Rationale: In the event of a contingency, the spacecraft may not return to the nominal preplanned location. Experience has shown that the system needs to provide a means for recovery forces to be provided with the spacecraft location. The ISS Expedition 6 crew returned to Earth in a Soyuz spacecraft. A system failure caused the Soyuz to downmode to a ballistic entry. When this happened, the Soyuz landed 'short' of the targeted landing zone. The system could not provide the recovery forces with an accurate location and the crew was placed in a survival situation while waiting for recovery. Subsequently, the Soyuz system was modified with a location system for recovery forces. This system was successfully utilized on Expedition 15, when another ballistic entry occurred.