National Aeronautics and Space Administration

	Document No: HEOMD-003	
	Revision: A	Effective Date: November 9, 2021

Crewed Deep Space Systems Human Rating Certification Requirements and Standards for NASA Missions

Revision/Changes

Revision	Description	Date
Baseline	CR HEO-0011, HEOMD-003, Crewed Deep Space Systems Human Rating Certification Requirements and Standards for NASA Missions, Initial Baseline (Approved at the Directorate Program Management Council (DPMC) on March 9, 2021.	March 9, 2021
A	CR HEO-0018, Added two new requirements for Crew Support and clarified autonomy requirement in support of Sustaining Phase of Artemis. Revised Certification Process section to no longer require a Human Rating Certification Package, rather allow responsible programs to define a Human Rating Plan that leads to the final Certification (Approved at the Directorate Program Management Council (DPMC) on November 9, 2021.	November 9, 2021

TABLE OF CONTENTS

List of Tables

1.0 Introduction

The Crewed Deep Space Systems Human Rating Certification Requirements and Standards for NASA Deep Space Missions is a consolidated set of technical requirements, standards, and processes that National Aeronautics and Space Administration (NASA) Program Managers shall implement for human rating certification of Crewed Deep Space Systems. These requirements are built upon NASA's unique human spaceflight knowledge and experience. The intent of this document is to define the requirements, standards, and human rating certification process and products that will be used to certify systems as acceptably safe to carry NASA or NASA-sponsored crewmembers on deep space missions for those programs that are not governed by NPR 8705.2, Human Rating Requirements for Space Systems. Orion, Space Launch System (SLS), and Exploration Ground Systems (EGS) are governed by NPR 8705.2.

NASA plans to purchase, produce, and/or partner to provide crewed deep space systems as part of NASA's exploration plans and policies. NASA chose to base its certification approach for such systems upon that documented within NPR 8705.2, Human Rating Requirements for Space Systems. Agency policy requires NASA to analyze the risk and decide on necessary steps to ensure safety when putting NASA personnel in harm's way using designs or operations that NASA does not control.

1.1 Philosophy

Protecting the health and safety of humans is of paramount importance for those involved in or exposed to space activities. For NASA, safety is a core value, and NASA recognizes that there can be no successful missions without first ensuring the safety of all personnel including the public, crew, and passengers. Concurrently, NASA recognizes that there can be no human space exploration without assuming some element of risk as human spaceflight will never be risk free. However, risks can be mitigated through the application of the fundamental tenets of human rating where 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..

1.2 Purpose

This document defines the human rating requirements and standards (as determined by the Engineering Technical Authority (E TA), Safety & Mission Assurance Technical Authority (SMA TA)), and Health and Medical Technical Authority (HMTA)) that are to be imposed in the design, development, test, and evaluation (DDT&E), production, and operations to ensure that hardware/software systems are developed and certified to be safe and reliable for, compatible with, and in support of the "Human system" as an integrated system to accomplish the mission. It also defines the processes and products required to certify crewed deep space systems as human-rated, thereby helping to answer the following fundamental question: Looking at all of the hardware, software, and operational aspects that compose the integrated crewed deep space system, will this system accomplish the mission with an acceptable level of human risk? The human rating certification process answers this question by requiring an incremental review of the system design and certification products that provide proof the system is

acceptable with respect to crew safety and crewed operations, including meeting the necessary Technical Authority (TA) design and construction (D&C) standards and requirements. Note that the TA D&C standards and requirements listed in section 6 represent the minimum set of agency level TA requirements that are necessary to achieve an acceptably safe crewed flight, but do not represent the full suite of TA requirements necessary to achieve design certification. The Programs developing the hardware/software systems are expected to impose these requirements and standards and any others they deem necessary in addition to system performance requirements for the mission. They are also expected to develop and successfully execute comprehensive design verification,validation and certification of all of these requirements outside of the scope of this document.

The requirements of this document do not apply to ESD, Orion, SLS, or EGS (since they are governed by NPR 8705.2); however, during the course of a mission(s), some ESD element(s) are part of the crewed deep space system and/or their capabilities may be needed for the system to be certified as human-rated. In such cases the Program Managers will work together with Human Exploration and Operations Mission Directorate (HEOMD) to ensure human-rating certification of the integrated deep space system.

1.3 Verb Application

Statements containing “shall” are used for binding requirements that must be verified and have an accompanying method of verification; “will” is used as a statement of fact, declaration of purpose, or expected occurrence; and “should” denotes a statement of best practice.

2.0 Reference Documents

Document Number	***Title*: Description**
NPR 8705.2C	NASA Human-Rating Requirements for Space Systems
NPR 8715.3C	NASA General Safety Program Requirements

3.0 Approach

3.1 Human Rating Certification Philosophy

Human Rating certification of crewed deep space systems to support/transport NASA or NASA sponsored personnel consists of four separate functions: 1) validation of the technical and performance requirements and standards; 2) verification of compliance with those requirements/standards; 3) incorporation of relevant operational experience, such as that gained from past and current human spaceflight programs, lessons learned data, problem reporting, mishap investigations, etc.; and 4) acceptance of residual technical risk to the crew due to hazards, waivers, non-compliances, etc. First, the NASA Program Managers and Program Technical Authorities (TA) determine the applicability of individual requirements and standards based on the mission being certified and apply the Agency risk posture (for the mission) to arrive at the final set of requirements and standards for human rating certification. Next, Program Managers will lead life cycle and periodic technical reviews to ensure designs are compliant with the human rating requirements or limitations are of acceptable risk. Finally, all waivers and deviations to requirements in this document must be endorsed by the HEOMD

Associate Administrator (AA). The HEOMD AA is accountable for acceptance of risk. All waivers, deviations, and exceptions to requirements in section 4 and 5 must be concurred upon by the Chief of the Office of Safety and Mission Assurance (OSMA), the Chief Engineer, the Chief Health and Medical Officer, and the Center Director, Johnson Space Center (JSC) (or respective delegates) for crew risk acceptance. All waivers and deviations to section 6 of this document must be made available for review by all Technical Authorities and the Center Director, JSC (or delegate) and concurred upon by the responsible Technical Authorities. A HEOMD Division is designated as responsible for planning and execution of crewed missions utilizing multiple systems. That Division, through coordination with the Program Managers, will arrange for incremental and periodic review of certification products as described in section 4 of this document. Throughout the remainder of this document, the use of the term Program Manager includes the responsible HEOMD Division Manager for the mission. The HEOMD Associate Administrator is then responsible for requesting Human Rating Certification from the NASA Associate Administrator for an integrated mission as an element of the overall Certification of Flight Readiness (CoFR) process. The CoFR statement will specifically acknowledge that all requirements and tenets of human rating have been satisfied.

The NASA Program Managers are responsible for ensuring that the operational and design human rating certification requirements and standards are met through the appropriate instrument (agreement milestone, statement of work, contract requirements, engineering and operations plans, etc.). The NASA Program Managers are also responsible for ensuring that the crewed deep space system is in compliance with the Human Rating Certification for each integrated mission. Once systems have been certified, they must be operated and maintained within the boundaries of Certification. Prior to each crewed mission, the Human Rating Certification will be reevaluated for changes to the system or the mission that are outside the boundaries of the previous certifications. During the operations phase, the NASA Program Managers are responsible for monitoring the safety performance by evaluating the risk based on the significance of observed anomalies, by updating its assessments of safety measures to ensure safety requirements continue to be met and ensuring there are established processes for both continuous improvement towards achievement of the safety goals and re-evaluation if safety goals are not achieved.

3.2 Human Rating Certification Applicability

Human rating certification will apply to crewed deep space systems, with the elements of the system being determined by the defined mission(s) as documented in the approved program documentation with concurrence by the Technical Authorities and the Center Director, JSC. A crewed deep space system consists of all the system elements that are occupied by the crew during the mission and any elements that are physically attached while the crew is present. The Division Manager responsible for the mission will maintain a traceability matrix between required Human Rating products and requirements and existing Program requirements, and where necessary derive and allocate further requirements to close gaps in Human-Rating. This matrix described in the Human Rating Certification Plan will ensure complete coverage of requirements and capture each elements contributing function.

For Programs that are not individually certifiable as crewed deep space systems (e.g., the Gateway without Orion and crew present), these requirements will be tailored to the set that is applicable to that

Program and human rating certification will be combined with other appropriate Programs for respective NASA missions.

This document will encompass planned crewed deep space missions including crewed in-space capabilities, crewed landers, and crewed surface systems. It does not address the launch vehicles, ground infrastructure, and/or mission operations systems required for the uncrewed delivery of these mission systems to their destination, for which the checkout and readiness for crew arrival would be evaluated by the responsible program's safety process. As planning for future missions to Mars develop, requirements for crewed landers, surface systems, or transportation systems will be further defined.

Each independent element is not required to obtain a Human-Rating Certification - the certification is for the entire crewed deep space system. However, the Program Manager may elect to seek independent certification of elements of the crewed system if the procurement process makes this approach more logical. See Appendix B, definition of "crewed deep space system," for examples as they relate to Human-Rating Certification.

3.3 Human Rating Configuration Management

HEOMD Systems Engineering and Integration (SE&I) will maintain configuration management and control of the crewed deep space systems human rating certification requirements for NASA deep space missions. The NASA Program Managers responsible for the crewed deep space systems verification and certification will maintain configuration management and control of their specific certification requirements and documents for their systems and/or missions.

3.4 Human Rating Certification Change Authority

After the NASA Associate Administrator has granted human rating certification, all changes that affect the human rating certification will be evaluated and approved by the NASA Program Manager, Technical Authorities, and the Center Director, JSC. If the NASA Program Manager, any of the Technical Authorities, or the Center Director, JSC deem that any changes adversely affect the risk to the crew or that the basis for certification is substantially affected by changes, the Program Manager will ensure the appropriate products in Table 4-1 are updated and, in coordination with the HEOMD AA, will submit a revised request for re-certification and endorsement to the NASA Associate Administrator detailing the change of risk and rationale for acceptability.

4.0 Crewed Deep Space Systems Human Rating Certification Process, Products and Reviews

The process for Human Rating Certification, including endorsement and the timing of submission of the certification evidence, will be documented in the Human Rating Certification Plan to be developed and updated throughout the life cycle by the responsible Program Manager for each mission with concurrence of the Technical Authorities and the Center Director, JSC.

The Human Rating Certification Plan will describe:

- The Human Rating Process in the context of the mission being certified.
- The mission milestones as they relate to the development milestones for elements used in the mission.
- The expected maturity levels of the Human Rating Certification Products shown in Table 4-1 at the program and enterprise milestones.
- The process to elevate risk to Mission Managers and Certifying Stakeholders.
- The process for developing and reviewing the certification products or reference the authoritative development plan and include the role of stakeholders.
- The cross-program and cross-directorate dependencies that are required to achieve full human rating compliance for a given mission.
- The process to develop a traceability matrix that shows program allocation of each Human Rating requirement and enables the evidence associated with each element in Table 4-1 and requirement in sections 5 through 7 to be located.
- The process for capturing human rating certification products in the identified repository including those products that have broader content than Human Rating, and how the subset applicable to human rating is identified (e.g. Which certification products are tied to human rating requirements).
- The milestone at which mission Human Rating Certification will occur and needs from programs to support this.

The Human Rating Certification Plan must describe a plan for incremental review of the human-rating products and progress toward final human-rating. Table 4-1 provides information on HEOMD and stakeholder expectations for maturity of products across the lifecycle using NPR 7123.1 milestone review strategy as a benchmark. These reviews culminate in approval at ORR or a commensurate agreed-to milestone that the tenets of Human Rating have been met by the integrated system and is acceptably safe to carry NASA crewmembers. Any open verification, manufacturing or operations work is documented and closed out through the flight readiness process. The Flight Readiness Review will ensure all prior open work has been completed, and results in a Certification of Flight Readiness endorsed by all of the Programs, Flight Operations and NASA Technical Authorities, and will be inclusive of a Human Rating Certification. The milestone review products are not intended to duplicate/repackage existing program documentation but rather provide a summarization of approach, top risks, and mitigations, the details of which can be found in the certification product repositories described in the Human Rating Plan. Program Managers shall maintain the Human Rating Certification Configuration, Certification Products and supporting data under configuration management to establish a certification baseline and risk posture. In the event that a fully developed existing system needs certification, a tailored approach to the delivery of the Human Rating Certification products will be developed. Through operational experience, changes to the risk posture of designs and operations may occur and Program Managers will ensure that the design and compliance products are updated each mission to address those changes. Program Managers will assert whether the crewed space system is still operating under a prior human-rating certification each mission. An updated human-rating certification will be required when the HEOMD AA, Program Manager, Technical Authority, or Center Director, JSC (or delegate) deem changes sufficient to warrant re-review or have adversely affected the risk posture.

Table 4-1: Crewed Deep Space Systems Human Rating Certification Products/Evidence

Key: X – One time item, I – Initial release of item; U – Update of item

	Review Phase	SRR	SDR	PDR	CDR	ORR
	Process and Standards					
1	A summary and access to all requested waivers, deviations, and exceptions to the requirements, with justification and disposition, as well as any exemptions to the failure tolerance requirement.	I	U	U	U	U
2	A link to the safety and mission assurance plan and the documented safety analysis processes and results.	I	U	U	U	U
3	A list of applicable standards with any exceptions, deviations, waivers, and significant issues in work, with respect to Section 6.	I	U	U	U	U
	Designing the System					
4	A description of the crewed deep space system for which certification will be requested. Refer to Appendix B - Definitions for the definition of "crewed deep space system".	X				
5	A description of the approach for crew survival during each mission phase is derived from an integrated design and safety analysis; the system capabilities or the trade studies/analysis to determine implementation; and a matrix that traces the capabilities to the program requirements (highest level where the capability is implemented).		I	U	U	U
6	A description of the design philosophy as it relates to utilization of the crew's capabilities to execute the mission, prevent aborts, and prevent catastrophic events.	I	U	U		
7	A description of the implementation of the applicable requirements listed in Chapter 5 of this document and clear	I	U	U	U	U

Key: X – One time item, I – Initial release of item; U – Update of item

	Review Phase	SRR	SDR	PDR	CDR	ORR
	traceability to the highest-level program documentation.					
8	Specify the program Loss of Crew (LOC) requirements as derived from the Agency-level safety goals and safety reporting thresholds, including any allocations to mission phases and system elements as applicable.	I	U	U	U	
9	A summary of the human-in-the-loop usability evaluations for human-systems interfaces, and integrated human-system performance testing to date and how the results influenced the system design. The usability evaluations and integrated human-system performance testing should be consistent with NASA-STD-3001.			I	U	
10	A summary of the results of the integrated design and safety analyses, including current understanding of risks and uncertainties and related decisions regarding the system design and application of testing to include: a. A list of the significant risk contributors to loss of crew 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 crewed deep 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	I	U	U	U	U

Key: X – One time item, I – Initial release of item; U – Update of item

	Review Phase	SRR	SDR	PDR	CDR	ORR
	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					
11	A description of how the crew and ground control workload for the mission will be evaluated.	I	U	U	U	
12	A Human Error Analysis shall be performed for all mission phases to include operations planned for response to system failures consistent with NPR 8705.2C and per NASA-STD-3001 a summary of the human error analysis performed to date and how the results influenced the system design should be included at each design review.	I	U	U	U	U
13	A link to the Human Systems Integration Plan that includes a description of the Human-Systems Integration team and their authority within the program	I	U			
14	A description of the implementation of the applicable Technical Authority Standards from Chapter 6 and clear traceability to the highest-level program documentation.	I	U	U	U	U
	Verifying and Validating the System Capabilities and Performance					

Key: X – One time item, I – Initial release of item; U – Update of item

	Review Phase	SRR	SDR	PDR	CDR	ORR
15	A plan, with rationale, for verification and validation of the following: • Implementation of capabilities identified for crew survivability • Implementation of Operational and Design Technical Requirements in Section 5 of this document. • Critical subsystems, systems, spacecraft, and the integrated crewed deep space system technical and performance requirements, including interfaces with external capabilities and systems. • Critical software performance, security, and safety. (including mission functions, modes, transitions, off-nominal, contingency, stress testing with faults injected) • Integrated Human System Performance • Implementation of standards. A summary of the verification and validation results (with links to the detailed results) shall be provided.	I	U	U	U	U
16	A description of how the crew and ground control workload was validated for the mission, and how the Program identified and implemented necessary mitigations to significant findings.					X
17	A description of how the safety analyses were updated based on the results of validation and verification testing and used to support validation and verification of the design in circumstances where testing was not accomplished.					X
	Flight Testing the System					

Key: X – One time item, I – Initial release of item; U – Update of item

	Review Phase	SRR	SDR	PDR	CDR	ORR
18	A description of the flight test program, including the type and number of test flights that will be performed. The flight test program reviewed at milestones should include a flight test plan for the integrated vehicle, integrated systems, and critical elements including flight test objectives and risk reductions with use of flight tests for validation. (This should be updated and reviewed at design milestones.)		I	U	U	
19	An update to the flight test program to include the flight test objectives with linkage to specific program requirements that are validated by flight test.		I	U	U	
20	A summary of the results of the flight test program to date and each test objective, along with access to the detailed test results.					X
	Certifying and Operating the Human-Rated System					
21	A configuration management and maintenance plan that documents the processes that the program will use to ensure that the crewed deep space system remains in the "as-certified" condition through the end of the life cycle to include system disposal.					X
22	A data collection, management, and analysis plan that documents the processes that the program will use to ensure that the appropriate crewed deep space system data is collected, stored, and analyzed throughout its life cycle in support of the analyses to understand the risks associated with each mission.					X

Key: X – One time item, I – Initial release of item; U – Update of item

	Review Phase	SRR	SDR	PDR	CDR	ORR
23	A summary of all changes that were determined to potentially affect Certification since the NASA Associate Administrator last granted Certification and their resolution (e.g., in-flight anomalies, design changes, manufacturing changes that could affect risk to the crew)					X

5.0 Crewed Deep Space Systems Operational and Design Human Rating Certification Technical Requirements

5.1 Overview

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

5.1.1 Flight Test Program Requirements

The Program Manager shall describe the flight test program in program documentation, which includes the type and number of test flights that will be performed, linkage of flight test objectives to program requirements and flight test results relative to each objective. This may be satisfied through a Program Implementation Plan, Validation and Verification (V&V) plan or other required Program documentation. The flight test program should include the flight test plan for integrated vehicle, integrated systems and critical elements, to include flight test objectives and risk reductions with use of flight tests for validation with objectives linked to program development/verification needs.

The breadth and depth of the flight test program may vary based on a number of factors including system maturity and depth of insight into the design and verification. The test program, which may include a combination of component tests, subsystem tests, system tests, stage tests, vehicle tests must be robust enough to prove confidence in the aspects of the system design, and reduce uncertainties to adequately operate within its established design envelope, not adequately verified by any other method. Since flight tests are typically major factors in program and budget planning, it is important to review the flight test program at a high level early in the development process and at subsequent milestones.

Note: 1) The flight test program provides two important functions. First, the flight test program uses testing to validate the integrated performance of the space system hardware, software, and, for crewed test flights, the human, in the operational flight environment. Second, the flight test program uses testing to validate the analytical models that are the foundation of all other analyses, including those used to define operating boundaries not expected to be approached during normal flight.

Note: 2) Flight and ground tests are needed to ensure that the data for the analytical models can be used to confidently predict the performance of the space systems at the edges of the operational envelopes and to predict the margins of the critical design parameters.

Note: 3) In order to minimize risk to the crew, it is preferred that an uncrewed flight test be conducted prior to a crewed flight test. It is acknowledged that this may not be feasible for all phases of flight and may not be necessary for some systems.

Rationale: The results of the flight test program may force modifications or changes to the system. It is imperative that any changes are fully understood and properly verified and validated.

5.1.2 Operating within the Certification

5.1.2.1 As part of each flight or mission readiness review, the Program Manager shall review the Human-Rating Certification to include the following:

a. Compliance with the Configuration Management and Maintenance Plan.

b. Verification that the human-rated system will be operated within the certified envelope of the reference mission(s).

c. Anomalies from the previous flight/mission that affect the Human-Rating Certification and their resolution.

d. Design changes, manufacturing (or refurbishment) process changes, and testing changes that were made as part of the Program's safety upgrade and improvement program that are expected to affect risk to the crew.

Rationale: Human-Rating of a space flight system is a process that is embedded throughout the life cycle of a program from development through operations. The applicability of the Human-Rating Certification is part of the program review process, including the program boards and flight readiness reviews. However, more important than the certification or process, human-rating is a state of mind that enables each member of a program design team to constantly work to reduce uncertainties, reduce risk, and design, build, test, and operate the safest practical system for the mission. As a part of this effort, analytical models for the system are updated using the anomaly and operational and flight performance data to accurately reflect the risk associated with future missions.

5.2 System Safety Requirements

5.2.1 The Crewed Deep Space System shall define and meet the program Loss of Crew (LOC) (derived from the Agency Safety Reporting Thresholds (SRTs)) and Loss of Mission (LOM) requirements for each specific NASA mission addressing:

a. Relevant safety-related data, including past spaceflight history and system(s) failures;
b. The dominant risks and their associated uncertainties; and
c. The feasibility of mitigating the dominant risks and uncertainty contributors, whether by redundancy or a reliability-informed approach that emphasizes high reliability and reliability testing
d. Sensitivity analysis for key assumptions

5.2.1.1 The Crewed Deep Space System LOC/LOM requirements shall be decomposed to develop and sub-allocate reliability requirements for hardware systems.

Note: Agency Safety Reporting Thresholds (SRTs) represent the level(s) of risk that requires Administrator notification. The SRT is specified as a mean value, and assumes that corresponding program requirements and probabilistic analysis are established and conducted with consistent assumptions and methods of analysis in order to reach results that can be compared with the threshold. HEOMD will provide support in development of the SRTs and associated rationale for approval by the Administrator.

Note: Probabilistic safety analysis methods provide one basis for the comparison of design options with regards to safety and reliability. Probabilistic safety requirements 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 through use of mean estimates as part of the probabilistic safety requirements or lower level allocations. Even when these metrics are determined in accordance with accepted analysis protocols, it is recognized, however, 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 by 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.

The development of a program Loss of Crew and Loss of Mission requirements must be based on an analysis of achievability for the selected mission and capabilities required. Typically, historical data for similar systems, capabilities, and operations is used to estimate an achievable level of risk for the selected mission, and additional margin may be added to account for uncertainties in future design or mission changes. Modeling assumptions and data must be coordinated with the cognizant systems engineering personnel to ensure accuracy and consistency with design and mission assumptions. NASA personnel are highly encouraged to

work cooperatively with contractor or system-provider personnel as early as possible to define verification approach.

Programs making up the mission will have LOC and LOM requirements imposed that are expected to be verified (compared to the program requirement) by NASA using program approved probabilistic risk assessment techniques. These will be flowed into the overall mission allocation to be compared to the mission level SRT. NASA is expected to allocate hardware reliability requirements to contractors or partners based on the program LOC and LOM requirements, and must include the probability of success for a specified time period. NASA allocations should be to the highest level of the system possible for the contractor or partner, and allow the contractor or partner to make reliability allocations to lower levels of the design.

Design engineers must translate over-all system characteristics, including hardware reliability, into detailed specifications for the numerous parts that make up a complex system. The hardware reliability of an individual unit varies depending on several factors including the type of function to be performed, the complexity of the unit, and the engineering method of accomplishing the function. Hardware reliability allocation is the process of assigning a numerical reliability to units of the system such that the over-all integrated system meets its over-all requirement. Allocations are often made on the basis of considerations such as complexity, criticality, operational profile, environmental conditions, technology maturity, and historical performance. Since allocations are normally required early in the program when little or no program hardware information is available, the allocations may need to be updated periodically through-out the life of the program. NASA personnel are highly encouraged to work cooperatively with contractor or partner personnel as early as possible to determine appropriate hardware reliability allocation methods and reliability allocations.

This could include defining a reliability allocation with a confidence limit when the unit is safety-critical or mission-critical and a single point failure. For these cases, additional reliability qualification or demonstration testing may be deemed necessary to verify the reliability to the specified confidence limit, and testing to failure for specific critical failure modes to demonstrate margins and understand onset and propagation of failure. NASA personnel are expected to work cooperatively with contractor and partner personnel as early as possible to identify potential single failure points (i.e. zero failure tolerance) and determine the appropriate verification approaches.

5.2.2 The Crewed Deep Space System shall provide at least single failure tolerance to catastrophic hazards, with specific levels of failure tolerance and implementation (e.g. similar or dissimilar redundancy) derived via an integration of the design and safety analysis.

a. Exemption A: 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.

b. Exemption B: Other potentially catastrophic hazards that cannot be controlled using failure tolerance are exempted from the failure tolerance requirements with mandatory concurrence from the Technical Authorities and the Center 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. For selected cases where reliability-informed approaches are used, as concurred by the respective programs Technical Authorities and the Center Director, JSC, the allocated reliability requirements shall be verified with appropriate confidence limits using robust reliability approach that is substantially anchored in actual test data verifying margins to environments (natural and induced), life requirements, operational boundaries, and failure modes.

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, when failure tolerance is practical, 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, dissimilar down mode, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures, or additional features that completely 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.

Ultimately, the level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Since redundancy does not, by itself, make a system safe, it is the responsibility of the engineering and safety teams to determine the design that optimizes safety given the mission requirements and constraints. In such a design, both the risk from individual contributors (e.g., hazards or failure modes) and the integrated risk for the mission are below acceptable levels.

Note 1: Redundancy alone does not meet the intent of this requirement. The following are key considerations for high reliability systems, especially for systems with reduced failure tolerance, and are expected to be driving themes for requirements development and verification. These apply for new hardware, use of heritage hardware/systems, as well as derivative designs.

a. Conceives the right system conceptual design early in the life cycle

b. System engineering process that integrates design, reliability and safety in trades as part of risk informed decision making (e.g., PRA)
c. Process for understanding of risk drivers and prioritization (considers time of exposure, time to effect, hazards-shades of grey)
d. Complementary analyses for complete top down and bottom up assessment
e. Imposes safety and reliability requirements to be met through combination of fault tolerance, bounding failure probability, and adhering to proven practices and standards
f. Incorporates redundancy judiciously to enhance reliability, tend to be at the simple end of a complexity measurement scale
g. Identifies opportunity for dissimilar down mode for system level fault tolerance
h. Understands Hazards and Failure Modes (drive additional testing for 0FT reliability-informed approach), develops controls and mitigations
i. Understands critical items list (CIL) and critical processes
j. Utilizes proven practices in design, manufacture, quality, test and operation
k. Environments understood and bound (natural and induced) (component/system qualification testing). Heritage systems must be assessed for compatibility with intended operational environments.
l. Requires understanding of how the system compares to mission requirements including performance, environments, and reliability
m. Testing to verify margins with "test like you fly, fly like you test" philosophy
n. Margins are understood and demonstrated (drives additional testing for 0FT reliability-informed approach)
o. Dispersions of the build/assembly variability are understood and demonstrated (drives additional testing and/or quality and inspection for 0FT reliability-informed approach)
p. Must be robust and have long term sustainability to protect against quality escapes and process changes/errors (critical processes), process controls/defect prevention
q. Continues to iterate through life cycle with higher levels of fidelity as system design matures
r. Controls hardware usage from qualification to flight
s. Flight unit acceptance tested/inspected (ATP)
t. Clear process that shows how these strategies play together to achieve holistic reliability

Note 2: 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 is 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.

Note 3: In typical spacecraft designs, the capabilities needed to perform critical functions are predominantly implemented in flight software. Software malfunctions that are the result of hardware faults can usually be isolated to a specific device and are detected by such means as

self-checking logic on multiple processors and output voting used with redundant computer sets. The most insidious failure mode is the result of a software common mode failure in which every instance of the same software image executing on multiple devices encounters the same unexpected condition simultaneously (task overrun, stack overflow, divide by zero, etc.) or in a cascading sequence, adversely affecting the proper operation of the software and precluding the ability of redundancy management schemes from isolating the problem to a specific device. In a worst-case scenario, the only option for restoring complete functionality might be to restart one or more flight computers, which, depending upon the mission phase in which the fault is encountered, may exceed the time to effect for catastrophic hazards. Even with rigorous software development processes with an extensive verification and validation campaign, past missions have shown that software-related failures can and do occur. In order to control and mitigate software common mode failures, there are required risk minimization activities within the software engineering requirements and software assurance and software safety standard listed in section 6 as well as three options for control/mitigation strategies (System Failure Tolerance, Recover/Repair, and Risk Acceptance). If Risk Acceptance is the selected option, the acceptance rationale should describe the risk minimization activities and address how these items are being implemented or provide compatible alternatives that meet their intent.

a. System Failure Tolerance

- *What - A system design that fully controls a hazard should a software common mode failure occur*
- *When to use - Whenever possible, this is the preferred strategy. Providing a fully functional redundant set of capabilities to avoid a catastrophic hazard (which may include dissimilar software) is viewed as an equivalent risk and meets the intent of failure tolerance requirements.*
- *How to Implement*
    - *Incorporate dissimilarity to mitigate the effects of common cause software errors*
    - *Incorporate functional redundancy within the system to completely control the respective catastrophic hazard*
    - *Document as control(s) in respective hazard report(s) with appropriate verifications*

*b**. Recover/Repair***

- *What - Process and design mitigation to recover and/or repair software and system state after software common mode failure occurs before a catastrophic hazard is realized*
- *When to use- When the time to criticality before a catastrophic hazard occurs is sufficient to recover the software*
- *How to Implement*
    - *The analysis performed as part of the risk reduction activities includes the time to criticality determination.*
    - *Document recovery/repair plan and supporting design features if applicable in the respective hazard report(s) with appropriate verifications*

c. Accept Risk (Exemption)

- *What - characterize the risk and provide flight rationale*
- *When to use*

  - *If unreasonable to implement failure tolerance at the system level*
  - *If, as part of the Hazard Analysis processes, it is determined that there are flight phases in which hazard controls and mitigations do not provide sufficient time to prevent a catastrophic event due to common cause software failures ('blackout zones' due to time to effect)*
- *How to Implement*
  - *Define and provide a design strategy to assure control for the occurrence of software common mode failures. Implementation needs to be able to ensure the software can be recovered regardless of the faulted state. Strategies should address items such as task restart and exception handling on a flight phase basis.*
  - *Exemptions must be processed in accordance with program requirements and guidance*
  - *Identify specific rationale, based on software process controls and assurance, demonstrating acceptable risk of software common cause failure*

Note 4: Ultimately, the Program Manager and respective programs 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) Recognize the importance of the hazards being controlled; (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 for important characteristics of the item. This approach to hazard control takes advantage of existing standards or standards approved by the Program Management and concurred on by the respective programs 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 Program Manager and concurrence by the respective programs 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.

Note 5: Failure tolerance exemptions. The Program Manager must approve and the Technical Authorities, and the Center Director, JSC (for crew risk acceptance), must all concur that the appropriate design standards and other controls are in place to reduce the risk of hazard occurrence to an acceptable level. Disagreements among the concurring authorities may be elevated to the next higher level for resolution. The process by which this assessment is performed and approved is specified by program documents.

The specific data required to justify a failure tolerance exemption will depend on the specific hazard cause and exemption requested. Exemptions may require specific additional supporting data tailored to the exemption request. However, the following contains guidelines that are typical information required by the reviewing authorities for Exemption B items. Exemption A items are typically satisfied by review of guidelines d-f. For a system to fully comply with Exemption A, it is expected to continue to operate within the full set of margins (1.4 safety factor, 4x live, etc.) as those imposed for nominal operations. The information presented for an exemption request should be similar to the rationale and supporting data for a waiver.

a. *However, an exemption request submitted as part of the hazard report is not a waiver to the failure tolerance requirement, and a failure tolerance exemption is not a substitute for a waiver to additional applicable design requirements (see d. below). Why is an exemption needed? What benefit does it offer? Be reasonably specific regarding the impacts of implementing failure tolerance. In cases where the impact of implementing failure tolerance is not clear, the concurring authorities may request failure tolerance design options to be identified and the impacts characterized. In addition, the system safety risk of options with and without failure tolerance may be requested as well. For those limited cases where implementing failure tolerance is clearly impractical (e.g. "part a", primary structure), exemption rationale should focus on methods by which risk is controlled or mitigated (items below) and not focus on "why" the exemption is required or developing design trades.*

b. *What is the duration of exposure to the hazard? Shorter durations may support lower risk of hazard occurrence.*

c. *What is the time to effect from when the hazard occurs until the effects manifest? If there is less than acceptable time to detect and react to the hazard, this would dictate additional reliance on the robustness of design controls, possibly necessitating a change in the control strategy.*

d. *What are the specific design requirements and standards that apply to the exemption? The use of a conservative analytical approach to the design reduces the risk. Use of higher margins in the design may offset the need to modify the control strategy. Deviations and*

waivers to the approved design requirements or standards may result in a need to change the control strategy.

e. *What are the design environments that apply to the exemption? New design environments or existing environments with significant unknowns may dictate the need for a change in the control strategy. Transportation, handling, and installation environments should be considered.*

f. *What are the test and verification plans? Deviations or waivers to Program-approved qualification and acceptance testing requirements may result in the need to modify the control strategy. Usage of analyses, rather than tests, may necessitate a modification of the control strategy.*

g. *Does the design have previous flight history and what is the record of performance? In cases where there is an established record (i.e., extensive ground and flight history in relevant environments) of proven performance, less demand exists to modify the control strategy. In cases where there are unexplained or unresolved failures, this may indicate the need to modify the control strategy.*

h. *Address results from qualitative (e.g., FMEA) and quantitative (e.g., reliability predictions) reliability analyses, and identify proposed numerical reliability requirements applicable to the item or system, with confidence limits (if applicable), and the proposed testing program to verify those requirements.*

i. *What is the contribution of the control strategy to system risk is as determined via the application of PRA? Is there an increase or decrease in system risk?*

j. *What information supports the producibility of the design within acceptable risk? For example, the use of qualified vendors, control of critical processes, control of materials and piece parts, and use of AS9100-equivalent Quality Management Systems (QMS).*

k. *Address any operational limitations beyond those normally required to execute the mission, requirements for flight crew, or ground operator actions to control the hazards.*

l. *Address the ability to perform maintenance and restoration of critical functions prior to time to effect, with margin. Such a strategy must consider the availability of spare parts, tools, procedures, and training.*

5.2.2.1 Each Crewed Deep Space System program shall define, and contractually implement, requirements and guidelines for interpretation and application of the failure tolerance requirement using, as a minimum, the guidelines and the notes per the rationale of requirement 5.2.2.

5.2.3 The Crewed Deep Space System shall provide the appropriate failure tolerance capability defined in 5.2.2 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 document and consistent with NPR 8715.3, include crew fatality and the unplanned loss of a major element of the crewed deep 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.

5.2.4 The Crewed Deep Space System shall be designed to tolerate inadvertent operator action (minimum of one inadvertent action), as identified 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 ground and mission operations. The appropriate level of protection (i.e., one, two, or more inadvertent actions) is determined by an integrated human error and hazard analysis.

5.2.5 The Crewed Deep Space System shall tolerate inadvertent operator action, as described in 5.2.4, 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.

5.2.6 The Crewed Deep 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: According to current software standards, the software system will be designed, developed, and tested to:
1) Prevent hazardous software behavior.
2) Reduce the likelihood of hazardous software behavior.
3) 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.

5.2.7 The Crewed Deep Space System shall provide the capability to detect and annunciate faults to the crew at any location that affect critical systems, subsystems, and/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. To meet the intent of this requirement, this annunciation must be received by the crew in a timely fashion, regardless of their location in the habitable volume commensurate with the time to effect of the fault.

5.2.8 The Crewed Deep Space System shall provide the capability to isolate and recover from faults during 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. However, in these cases, isolation of the fault should prevent the catastrophic event.

5.2.9 The Crewed Deep 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 with the concurrence of the Program Technical Authorities.

5.2.10 The Crewed Deep 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 external systems(e.g., mission control, Earth) to perform functions that are required to keep the crew alive. For systems with long-time-to-effect hazards that occur while a crew return vehicle is present, control of those hazards may not require autonomy, as the crew can safely return to Earth in another crewed spacecraft.

5.2.11 The Crewed Deep 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

5.2.12 The Crewed Deep Space System shall be designed to manage human error according to the following precedence:

a. Design the system to prevent human error in the operation and control of the system.
b. Design the system to reduce the likelihood of human error and provide the capability for the human to detect and correct or recover from the error.
c. Design the system to limit the negative effects of errors

5.2.13 The Crewed Deep Space System shall determine crew survival capabilities (derived from hazard scenarios) during each phase of the mission and implement crew survival capabilities where feasible based on trade studies/analysis.

Rationale: The intent of the requirement is to determine what crew survival capabilities are available during each mission phase, perform trade studies to determine the feasibility of implementing crew survival methods and to incorporate such capabilities where practical.

5.3 System Control Requirements – General

5.3.1 The Crewed Deep Space System shall provide the capability for the crew to monitor, operate, and control the crewed deep 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. This information informs the crew decision on whether the system is performing adequately, or if intervention is necessary. Monitoring also 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.

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

Rationale: This is a specific capability necessary for the crew to control the crewed deep space system. While this capability should be derived by the program per paragraph 5.3.1, the critical nature of software control and automation at the highest system level dictates specific mention in these requirements. 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 Manager and respective programs' Technical Authorities will determine the appropriate implementation of this requirement – and document in certification products.

5.3.3 The Crewed Deep 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 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.

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.

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.

5.4 System Control Requirements – Human-Rated Spacecraft

5.4.1 The Crewed Deep Space System shall provide the capability for the crew to manually control the flight path and attitude of their spacecraft.

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 1: 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 spacecraft, 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 2: 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 validated in a cockpit environment to ensure they are adequate to support manual control and operations.

5.4.2 The Crewed Deep Space System 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.

5.5 System Control requirements – Proximity Operations and Human-Rated Spacecraft

5.5.1 The Crewed Deep Space System shall provide the capability for the crew to monitor, operate, and control an un-crewed 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

Note 3: The capability for the crew to monitor, operate and control the un-crewed spacecraft continues after docking through the point when the un-crewed spacecraft is fully integrated into the "new" vehicle stack, the un-crewed vehicle's GNC systems are safed and/or transitioned from a free-flying vehicle mode, and the integrated stack has achieved active attitude control for the new configuration and undocking and separation and active attitude control of the integrated stack through exit of the prescribed safe zone.

5.5.2 The Crewed Deep Space System shall provide the capability for direct voice communication between crewed spacecraft (2 or more) during proximity operations.

Note: Direct voice communication means that the signal is not routed through mission control or another communication relay satellite.

5.6 Crew Survival and Abort Requirements

5.6.1 Earth – Lunar Transit and Lunar Orbit Systems

5.6.1.1 The Crewed Deep 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.

5.6.2 Lunar Descent Systems

5.6.2.1 The Crewed Deep Space System shall provide the capability to autonomously abort the lunar descent and execute all operations, including rendezvous with appropriate spacecraft, 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.

5.6.3 Lunar Surface Systems

5.6.3.1 The Crewed Deep 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

5.6.3.2 The Crewed Deep Space System shall provide the capability to safely abort lunar surface operations, including EVA, and execute all operations (including intermediate step(s)) required for a safe return to Earth.

Rationale: During lunar surface operations, the crew may need to make a rapid return to its place of origin where medical care can be provided in order to prevent a catastrophic event and allow for incapacitated crew member rescue.

5.6.4 Lunar Ascent and Lunar Surface Systems

5.6.4.1 The Crewed Deep Space System shall provide the capability to return the crew with a single depressurized cabin in the crew return chain from any lunar surface location and execute all operations (including intermediate steps) required for a safe return to Earth.

Rationale: Pressure suits are provided for all flight phases because of the dire consequences of losing a habitable atmosphere. NASA's lunar systems need to be able to return the crew to Earth in the event that one of the crewed space systems becomes compromised and not able to maintain a habitable atmosphere. This means vehicle systems will have to operate with a depressurized cabin, execute commanded maneuvers and continue to support crew suit life support to the point of crew egress or transition to another spacecraft. While this requirement is intended to only cover a single habitable environment loss per mission and not compounding failures, each element must be independently capable of supporting a depressurized return, as the initiating depressurization event could occur at any point in the crew return chain. Since transfer from one crewed spacecraft to another is nominally conducted with pressurized compartments, this requirement is intended to drive features that allow for crew to safely transfer from an unpressurized spacecraft element into one that will hold pressure, such as an unpressurized lander crew cabin into the Gateway and/or Orion, or return to Earth in an Orion that is not capable of maintaining a habitable atmosphere, but otherwise of adequate integrity to return to Earth.

This requirement does not apply to loss of pressure integrity of the EVA space suit system and is intended for "shirt-sleeve" environments provided by spacecraft.

5.6.4.2 The Crewed Deep Space System shall provide the capability to complete the lunar ascent maneuver after initiation without crew assistance or external communication.

Rationale: The crew may not be able to execute ascent maneuver in timely manner. Other mission elements, such as external communication sources, may not be available to assist the crew in returning from the lunar surface when a rapid return is desired.

5.6.5 Earth Orbit Systems

5.6.5.1 The Crewed Deep 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 deep space system should provide a backup capability for entry to protect for loss of the primary attitude control and guidance system. An integrated design and safety analysis can be performed to develop rationale for scenarios where this may not be applicable.

5.6.6 Crew Support

5.6.6.1 The Crewed Deep Space System shall provide the capability to return an incapacitated crewmember from the point of incapacitation to Earth.

Rationale: An ill or injured crewmember could become stranded if there are not reasonable accommodations made in the design of vehicles and support equipment to facilitate the manipulation, medical care, and transport of the incapacitated crewmember. This includes consideration of lifting aids, attach points, restraints, crew positioning, and medical stabilization. Which scenarios are protected for, and accommodations made will be derived from a crew survivability analysis required by 5.2.13.

5.6.6.2 The Crewed Deep Space System shall provide a lunar surface safe haven for the crew until the next lunar ascent opportunity in the event a surface habitat becomes uninhabitable.

Rationale: Even with system failure tolerance, a surface habitat may no longer be viable, and the crew will need to shelter in place in remaining surface assets or the return vehicle until the launch window opens for the next nominal departure. These assets will need adequate consumables to accommodate this additional crew for this period. Safe haven is a contingency capability, and therefore may involve rationing food and water, lack of exercise, and lack of access to nominal crew support systems during the safe haven period where the safe haven habitat is not nominally expected to support such a period. Safe haven is defined as a separate pressurized volume in which the crew can survive until crew ingress into a safe environment.

6.0 Technical Authority Mandatory Standards and Requirements

This section lists the documents that contain requirements applicable to development and operational activities. These requirements have been designated by NASA as the superset of requirements for NASA human spaceflight missions in deep space.

The NASA Program Manager and the TAs are responsible for determining the application of these standards and requirements to the specific mission(s). The assessment shall be performed against the current revision in effect on the date the Program's system requirements are initially baselined. Some of the applicable standards have been tailored such that only a subset of the sections is levied. The applicability column designates those sections of the revision listed. If new document revisions have since been released, the program shall work with the cognizant program Technical Authority to determine applicability. If the applicable section numbers have changed in the latest revision or new requirements have been added, it is incumbent on the programs to ensure the appropriate sections are identified when levying a new revision. The below listed requirements are in addition to all applicable federal/state/local/tribal laws.

The mandatory NASA TA documents are separated into 3 types:

- Type 1 documents are those that contain requirements the Program must meet as written.

- Type 2 documents are those that contain requirements that the Program can either choose to adopt or propose an alternate. The Program will be allowed to propose alternate requirements and documents that they consider to meet or exceed the intent of the Type 2 document. Any Applicable Document listed within a Type 2 document is considered to be a Type 2 document as indicated within the context of the Type 2 document unless specifically noted. The NASA TAs will evaluate the equivalency of the requirements and documents proposed by the Program. It will be the responsibility of the Program Manager to demonstrate that a proposed alternate requirement or document fully meets the intent and the requirements of the document(s) listed herein, and obtain formal NASA Technical Authority approval at appropriate delegated level.
- Type 3 documents are those that represent some of the 'best practices' observed by or normally used by NASA over the substantial development history of both human and robotic spaceflight missions. There are many more NASA Handbooks on requirements implementation and test methodology that are available that can reduce the programmatic risk. However, the Program does not need to either formally adopt the documents or recommend an alternate.

NASA Policy Documents (NPD) and NPR documents can be found at: http://nodis3.gsfc.nasa.gov/. NASA Standards and reference Handbooks can be found at: https://standards.nasa.gov/nasa-technical-standards.

6.1 Mandatory Health and Medical TA Requirements and Documents

HMTA "Type 2" requirements and documents are fully applicable except as noted in Table 6-2. Note: The number in the "Applicability" column of Tables 6-2 indicates which chapters and paragraphs are applicable to the "Program" for further inclusion and tailoring into requirements; or directly tailored to the provider. Unless otherwise noted, all paragraphs within the chapter and all sub-paragraphs under the paragraph listed have the same applicability as the listed chapter or paragraph.

Table 6-1: Type 1 Health and Medical TA Documents

Document Number	Document Name	Applicability
	None	

Table 6-2: Type 2 Health and Medical TA Documents

Document Number	Document name	Applicability
NASA-Standard-3001 Volume 1	NASA Space Flight Human-System Standard Volume 1: Crew Health	Fully Applicable.
NASA-Standard-3001 Volume 2	NASA Space Flight Human System Standard Volume 2:	Fully Applicable.

Document Number	Document name	Applicability
	Human Factors, Habitability, and Environmental Health	

Table 6-3: Type 3 Health and Medical TA Documents

Document Number	Document Name	Applicability
NASA/SP-2010-3407	Human Integration Design Handbook	Reference
NASA/SP-2015-3709	Human Systems Integration (HSI) Practitioner's Guide	Reference
NASA/TP-2014-218556	Human Interface Design Process	Reference

6.2 Mandatory Engineering TA Requirements and Documents

Engineering TA requirements and documents are fully applicable except as noted in Tables 6-4, 6-5, and 6-6.

Table 6-4: Type 1 Engineering TA Documents

Document Number	Document Name	Applicability
	None	

Table 6-5: Type 2 Engineering TA Documents

Document Number	Document name	Applicability
AIAA S-111	Qualification and Quality Requirements for Space Solar Cells	Fully Applicable
AIAA-S-112	Qualification and Quality Requirements for Space Solar Panels	Fully Applicable
ANSI/AIAA-S-080	Space Systems - Metallic Pressure Vessels, Pressurized Structures and Pressurized Components	Fully Applicable (For Reference: also a child in SMA standard NPD 8710.5D and 8715.1)

Document Number	Document name	Applicability
ANSI/AIAA-S-081	Space Systems - Composite Overwrapped Pressure Vessels	Fully Applicable (For Reference: also a child in SMA standard NPD 8710.5D and 8715.1)
ANSI/ESD S20.20	For the Development of an Electrostatic Discharge Control Program for - Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)	Fully Applicable (For Reference: also a child in SMA standard NPD 8730.5B)
GP 10008 (TBR-HEOR-001)	Gateway Subsystem Specification for Power	Only Applicable Section is Appendix F of Revision B
GP 11461	Gateway Program Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment	Fully Applicable
GP 11464	Gateway Electromagnetic Environmental Effects (E3) Requirements	Fully Applicable
IPC-2220 series per Performance Class 3.	Family of Printed Board Design Documents	Fully Applicable per Performance Class 3. 2221: B 2222: A 2223: E 2224: BL 2225: BL 2226: A
IPC-6010 Series	Family of Printed Board Performance Documents	Fully Applicable 6011: BL 6012: DS 6013: D with Amendment 1 6015: BL 6017: BL 6018: CS

Document Number	Document name	Applicability
IPC J-STD-001GS	Space and Military Applications Electronic Hardware Addendum to IPC J-STD-001G Requirements for Soldered Electrical and Electronic Assemblies	Fully Applicable (For Reference: also a child in SMA standard NASA-STD-8739.4A)
IPC J-STD-001G/ Amendment 1	Requirements for Soldered Electrical and Electronic Assemblies	Fully Applicable (For Reference: also a child in SMA standard NASA-STD-8739.4A)
NPR 7120.5	NASA Space Flight Program and Project Management Requirements	Fully Applicable
NASA-STD-5012	Strength and Life Assessment Requirements for Liquid-Fueled Space Propulsion System Engine	Fully Applicable
NASA-STD-7009	Standard for Models and Simulations	Fully Applicable
NASA-STD-4003	Electrical Bonding For NASA Launch Vehicles, Spacecraft, Payloads, And Flight Equipment	Fully Applicable
JSC 20793	Crewed Space Vehicle Battery Safety Requirements	Fully Applicable
JSC 62809	Human Rated Spacecraft Pyrotechnic Specification	Fully Applicable
JSC 65828	Structural Design Requirements and Factors of Safety for Spaceflight Hardware	Fully Applicable

Document Number	Document name	Applicability
JSC 65829	Loads and Structural Dynamics Requirements for Spaceflight Hardware	Applicable Sections of Revision A for Deep Space Loads only Include: Sections 1.0-4.1, 4.3.1 paragraph LD0021-2, 4.3.2.2.4, 4.3.3, 5.1.1 para. LD0034, 5.1.2, 5.1.4, 5.1.5 paragraph LD0045, 5.1.6, 5.1.7.1, 5.1.7.1.1, 5.2.1 paragraphs LD0051 + LD0058 + LD0066 + LD0068. Note: the entire standard is applicable when launch vehicle loads are considered.
JSC 67035	Best Practices and Guidelines (BP&G) for Thin Wall Pressure Boundaries (TWPB) for Human Spaceflight Applications	Fully Applicable
MIL-STD-981	Design, Manufacturing and Quality Standards for Custom Electromagnetic Devices for Space Applications	Fully Applicable
NASA-STD-1006 (TBR-HEOR-002)	Space System Protection Standard	Fully Applicable
NASA-STD-5017	Design and Development Requirements for Mechanisms	Fully Applicable
NASA-STD-5018	Strength Design and Verification Criteria for Glass, Ceramics, and Windows in Human Spaceflight Applications	Fully Applicable
NASA-STD-5019	Fracture Control Requirements For Spaceflight Hardware	Fully Applicable
NASA-STD-5020	Requirements for Threaded Fastening Systems in Spaceflight Hardware	Fully Applicable

Document Number	Document name	Applicability
NASA-STD-6016	Standard Materials and Processes Requirements for Spacecraft	Fully Applicable (For Reference: also a child in SMA standard NASA-STD-8739.4A)
NASA-STD-6030 (TBR-HEOR-003)	Additive Manufacturing Requirements for Spaceflight Systems	Fully Applicable
NASA-STD-7012 (TBR-HEOR-004)	Leak Test Requirements	Fully Applicable
NPR 7150.2	NASA Software Engineering Requirements	Fully Applicable
SLS-SPEC-159	Cross-Program Design Specification For Natural Environments (DSNE)	Fully Applicable
SMC-S-010	Space and Missile Systems Center Standard, Parts, Technical Requirements for Electronic Parts, Materials, and Processes Used In Space Vehicles	Only the EEE Parts Sections are applicable. Below are the sections of SMC-S-010 revision (2013) that are NOT applicable for EEE parts. 1. Paragraphs 4.1.2, 4.3.1.2, 4.3.2 2. Paragraphs 4.5 and 4.7 including their sub paragraphs 3. Sections 100, 110, 120 and 1700 through 3500 inclusive. 4. Appendix D 5. Section 1500, Paragraphs 2.4, 3.3, 3.4 and 3.5.3.6 All other parts of the document are applicable.
SMC Standard SMC-S-016	Test Requirements for Launch, Upper-Stage, and Space Vehicles	Fully Applicable

Table 6-6: Type 3 Engineering TA Documents

Document Number	Document Name	Applicability Comments
ASTM F1192	Guideline for measuring single-event phenomena induced by heavy ions	Reference
ASTM F1892	Standard Guide for Ionizing Radiation (Total Dose) Effects Testing of Semiconductor Devices	Reference
ASME Y14.100	Engineering Drawing Practices	Reference
CPIA - 655	Guidelines for Combustion Stability Specifications and Verification Procedures for Liquid Propellant Rocket Engines	Reference
FAA AC 20-136	Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning	Reference
GRC-AES-AMPS-DOC-006	Modular Electronics Standard for Space Power Systems	Reference
IEC 61000-4-2	Electromagnetic Compatibility (EMC) Testing and Measurement Techniques-Electrostatic Discharge Immunity Test for Human Body Model (HBM) subassemblies, assemblies and equipment discharge levels	Reference
Ionizing Radiation Displacement Damage references	1) "Design Challenges for Optical Payloads Used in the Space Radiation Environment" 2015 IEEE NSREC Short Course; and 2) "Total Ionizing and Non-Ionizing Dose Radiation Hardness Assurance" and "Strategies for SEE Hardness Assurance—From Buy-It-And- Fly-It to Bullet Proof," 2017 IEEE NSREC Short Course.	Reference
IPC-2152	Standard for Determining Current Carrying Capacity in Printed circuit Board Design	Reference

Document Number	Document Name	Applicability Comments
IPC-CM-770	Component Mounting Guidelines for Printed Boards	Reference
JEDEC JESD57	Test Procedures for the Measurement of SEE in Semiconductor Devices from Heavy-Ion Irradiation	Reference
JSC-08080-2	JSC Design and Procedural Standards	Reference
MSFC-SPEC-3717	Specification for Control and qualification of Laser Powder Bed Fusion Metallurgical Process,	Reference
MIL-STD-130	Department of Defense Standard Practice, Identification Marking of U.S. Military Property	Reference
MIL-STD-750	Test Methods for Semiconductor Devices	Reference Applicable sections are: Test Methods 1017, 1019, and 1080
MIL-STD-750/Test Method 1080		Reference Cautionary note: For gallium nitride (GaN) and silicon carbide (SiC) device technologies since they are not currently covered by Mil-Aero or community consensus standards.
MIL-STD-883	Microcircuits TM 1017: Neutron irradiation TM 1019: Ionizing radiation (total dose) test procedure	Reference
MSFC-STD-3716	Standard for Additively Manufactured Spaceflight Hardware by Laser Powder Bed Fusion in Metals,	Reference
NASA-HDBK-2203	NASA Software Engineering Handbook	Reference
NASA-HDBK-4002	Mitigating In-Space Charging Effects-A Guideline	Reference

Document Number	Document Name	Applicability Comments
NASA-HDBK-4007	Spacecraft High-Voltage Paschen and Corona Design Handbook	Reference
NASA/JPL paper	Testing Guideline for Single Event Gate Rupture (SEGR) of Power MOSFETs, by Leif Sheik	Reference
NASA-STD-5005	Standard for the Design and Fabrication of Ground Support Equipment	Reference Applicable sections of Rev D, change 1are: 4.2.3.2a; 4.3.1; 4.6.2.1a; 5.1.2.a (1) & (2); 5.1.2.d; 5.2.3 a(1, 2,3), b,c; 5.2.1.2 a, b, c, d; 5.2.7; 5.2.8. a, b, c; 5.2.11. a, b; 5.2.11.2; 5.3.7 5.4.1.3; 6.3.1.3.1. a; 6.3.1.3.2.a; 6.3.1.3.2.h; 6.4.1; and 6.4.8.
NASA/TM-2018-220074	Guidelines for Verification Strategies to Minimize Risk Based on Mission, Environment, Application and Lifetime	Reference
SAE ARP 5414	Aircraft Lightning Zoning	Reference
SAE ARP 5577	Aircraft Lightning Direct Effects Certification	Reference
SAE ARP 5412	Aircraft Lightning Environment and Related Test Waveforms.	Reference
SAE EIA-649-2	Configuration Management Requirements for NASA Enterprises	Reference
SMC-S-025	Evaluation and Test Requirements for Liquid Rocket Engines	Reference to Section 8

6.3 Mandatory SMA TA Requirements and Documents

SMA TA "Type 2" requirements and documents are fully applicable except as noted in Table, 6-8. Note: The number in the "Applicability" column of Tables 6-7, 6-8, and 6-9 indicates which chapters and paragraphs are applicable. Unless otherwise noted, all paragraphs within the chapter and all sub-paragraphs under the paragraph listed have the same applicability as the listed chapter or paragraph.

Table 6-7: Type 1 SMA TA Documents

Document Number	Document Name	Applicability
	None	

Table 6-8: Type 2 SMA TA Documents

NASA-STD-8719.14	Process for Limiting Orbital Debris	Fully Applicable** with the exception of flights under licensure by other Federal Agency that has authority to oversee orbital debris mitigation Note that NPR 8715.6 (Rev B) provides for other Federal Agencies to assume responsibility for oversight of orbital debris mitigation. Prior to claiming such an exemption, NASA will obtain written confirmation from the Federal Agency claiming authority that assumes responsibility for the oversight of orbital debris mitigation for future missions covered by this document. Note: The approved environmental model for orbital debris assessments is ORDEM 3.1, rather than ORDEM 3.0 as stated in section 4.2.3.1 of Revision B of the standard.
NASA-STD-8729.1	NASA Reliability And Maintainability (R&M) Standard For Spaceflight And Support Systems	Fully Applicable
NASA-STD-8739.1	Workmanship Standard for Polymeric Application on Electronic Assemblies	Fully Applicable
NASA-STD-8739.14	NASA Fastener Procurement, Receiving Inspection, and Storage Practices for NASA Mission Hardware	Fully Applicable for control of fasteners

NASA-STD-8739.4	Workmanship Standard for Crimping, Interconnecting Cables, Harnesses, and Wiring	Fully Applicable Note: Per NPD 8730.5B, Appendix A, compliance is required with either this standard or IPC®/WHMA-A-620B and its space addendum IPC®/WHMA-A-620B-S
NASA-STD-8739.5	Workmanship Standard For Fiber Optic Terminations, Cable Assemblies, and Installation	Fully Applicable
NASA-STD-8739.6	Implementation Requirements for NASA Workmanship Standards	Fully Applicable
NASA-STD-8739.8	Software Assurance and Software Safety Standard	Fully Applicable
NASA-STD-8739.10	Electrical, Electronic, And Electromechanical (EEE) Parts Assurance Standard	Fully Applicable
NASA-STD-8739.12	Metrology and Calibration	Fully Applicable
NID 8715.129	Biological Planetary Protection for Human Missions to Mars	Fully Applicable
NPD 8730.2	NASA Parts Policy	Chapters 1, 5.e, and 5.f.1 - .5.f.4, , 5.f.5**- 5.f.6, Attachment B, and Attachment C of Revision C
NPD 8730.5	NASA Quality Assurance Program Policy	Sections 1.b, 1.c, 5.d, 5.e, Attachment A of Revision B* *Note that this document is not applicable if the program has chosen to apply NPR 8735.2 revision C or later
NPR 7150.2	NASA Software Engineering Requirements	Sections 2.1.2, 2.1.6, 3, 4, and 5 of Revision C
NPR 8000.4	Agency Risk Management Procedural Requirements	1.2.1.4 - 1.2.1.6, 1.2.4.1 - 1.2.4.7, 2.1, 2.2.3, 2.3.1, , 3.2, 3.3, 3.4, 3.5, Appendix C of Revision B

NPR 8621.1	NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping	Fully Applicable
NPR 8705.5	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects	Sections 2.2.1.a-e, 2.2.2.a-c, 2.3.2, 2.4.2.a-d, 2.5.2.a-i, 2.6.2.a-c, 2.7.2.a-c, 2.7.3, 2.8.1.a-g, 3.3.2.a-b, 4.6.1.a-i, 4.7.1.a-e, 4.8.a, 5.2.1.a-d of Revison A
NPR 8705.6	Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments	Sections 2.2.7, 2.3.5.a-e, 3.2.6, and 3.2.7 of Revision D
NPR 8715.24 (TBR-HEOR-005)	Planetary Protection Provisions for Robotic Extraterrestrial Missions	Fully Applicable
NPR 8715.3	NASA General Safety Program Requirements	Sections 1.5 - 1.7.1, 1.13, 1.14 (for NASA participation in hazardous work activities that are outside NASA operational control), 2, 6**, and 9 of Revision D (Updated with Change 3). *For sections 2.5.1.2.a and 2.5.1.2.c, SSTP does not require the concurrence of the governing PMC, but instead the same level of concurrence as other programmatic changes that could affect crew safety **NPR 8715.3 chapter 6 – nuclear flight safety for space nuclear systems is now governed by National Security Presidential Memorandum 20 for space nuclear systems (e.g., Radioisotope Heater Unit Units, fission devices, etc.); a new NPR to replace chapter 6 is in preparation. Until released, the existing NPR, with some clarifications as documented in NPI 8715.93, NASA Policy Instructions: Impacts of NSPM-20 on NASA Nuclear Flight Safety Requirements and Practices, remains in effect for all flights involving space nuclear systems or other radioactive

		material.
NPR 8715.6	NASA Procedural Requirements for Limiting Orbital Debris and Evaluating the Meteoroid and Orbital Debris Environments	With the exception of flights under licensure by other Federal Agency that has authority to oversee orbital debris mitigation, the following paragraphs of Revision B apply: P.2, 1.3.2, 1.3.6, 2.4, 3.1.1-3.1.2, 3.1.3, 3.1.4, 3.2.1-3.2.4, 3.2.7, 3.2.8, 3.2.10 (applicable only for return-to-Earth scenarios), 3.2.11, 3.3.1 (applicable to missions orbiting Earth, Moon, or Mars or in the vicinity of Sun-Earth or Earth-Moon Lagrange Points), 3.3.2 (applicable to Earth-orbiting spacecraft), 3.3.3 (applicable to missions around the Moon or Mars or in the vicinity of Sun-Earth or Earth-Moon Lagrange Points), 3.3.4-3.3.6, and 3.4.1 (applicable for controlled, commanded, or targeted reentries only).
NPR 8735.1	Exchange of Problem Data Using NASA Advisories and the Government-Industry Data Exchange Program (GIDEP)	Sections 2.3, 3.1.6, 3.2.4 – 3.2.5, 3.3.3, 3.4.1, 3.4.3, 3.4.6, 3.5.1, and Appendix C of Revision D
NPR 8735.2	Management of Government Quality Assurance Functions for NASA Contracts	Fully Applicable

Table 6-9: Type 3 SMA TA Documents

Document Number	Document Name	Applicability Comments
NASA-HDBK-8709.22	Safety & Mission Assurance Acronyms, Abbreviations, & Definitions	Reference Note that various definitions within this document are relied upon by a requirement(s) within another applicable Type 2 requirements document (e.g., NASA-STD-8739.6 relies upon definitions within this standard).
NASA-HDBK-8739.23	NASA Complex Electronics Handbook for Assurance Professionals	Reference

7.0 International System Interoperability Standards

The standards provided here have been collaboratively prepared with the goal of defining interfaces and environments to facilitate cooperative deep space exploration endeavors. These standards focus on topics prioritized for early phase of exploration planning and will evolve over time. Each HEO Program shall meet the intent of the standards in Table 7-1 in the context of the defined missions for assurance of vehicle-to-vehicle, portable equipment and payload interface compatibility. The responsible Division will allocate standards to its Programs in accordance with its interoperability approach, and relevant adjudication and tailoring approval authority. The applicable Division's System Engineering Management Plan (SEMP) will define the approach that will be used by their Programs to assess applicability of the standards, to evaluate meets the intent in the Program IRDs, and to evaluate applicability of revisions to standards.

Table 7-1: International System Interoperability Standards Documents

Document Number	Document Name	Applicability Comments
HEOMD-003-01	International Avionics System Interoperability Standards (IASIS)	Fully applicable.
HEOMD-003-02	International Communication System Interoperability Standards (ICSIS)	Fully applicable.

Document Number	Document Name	Applicability Comments
HEOMD-003-03	International Environmental Control and Life Support Systems (ECLSS) Interoperability Standards (IECLSSIS)	Fully applicable.
HEOMD-003-04	International Space Power System Interoperability Standards (ISPSIS)	Fully applicable.
HEOMD-003-05	International Thermal System Interoperability Standards (ITSIS)	Fully applicable.
HEOMD-003-06	International Rendezvous System Interoperability Standards (IRSIS)	Fully applicable.
HEOMD-003-07	International External Robotic Interface Interoperability Standards (IERIIS)	Fully applicable.
HEOMD-003-08	International Software System Interoperability Standards (ISwSIS)	Fully applicable.
IDSS IDD	International Docking System Standard Interface Definition Document	Fully applicable.

Appendix A: Acronyms

Acronyms	Phrase
AA	Associate Administrator
AIAA	American Institute of Aeronautics and Astronautics
ANSI	American National Standards Institute
ARP	Aerospace Recommended Practice
CDR	Critical Design Review
CoFR	Certification of Flight Readiness
D&C	Design and Construction
DPMC	Directorate Program Management Council
DRM	Design Reference Mission
EEE	Electrical, Electronic, and Electromechanical
EGS	Exploration Ground Systems
ESD	Electrostatic Discharge
ESD	Exploration Systems Development
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FMEA	Failure Modes & Effects Analysis
GIDEP	Government Industry Data Exchange Program
GSFC	Goddard Spaceflight Center
HEOMD	Human Exploration and Operations Mission Directorate
HFDS	Human Factors Design Standard
HMTA	Health and Medical Technical Authority
IPC	IPC – Association Connecting Electronics Industries
ISS	International Space Station
JPL	Jet Propulsion Laboratory
JPR	JSC Procedural Requirement
JSC	Johnson Space Center
MIL	Military
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Document
NPR	NASA Procedural Requirement
ORR	Operational Readiness Review
OSMA	Office of Safety and Mission Assurance
PDR	Preliminary Design Review

Acronyms	Phrase
PRA	Probabilistic Risk Assessment
R&M	Reliability and Maintainability
SAE	SAE International
SE&I	Systems Engineering and Integration
SDR	System Design Review
SLS	Space Launch System
SMA	Safety and Mission Assurance
SRR	System Requirements Review
STD	Standard
TA	Technical Authority

Appendix B: Definitions

Term	Definition
Abort	The forced early return of the crew to a nominal or contingency landing site when failures or the existence of uncontrolled catastrophic hazards prevent continuation of the mission profile and a return is required for crew survival. The crew is safely returned to a landing site in the space system nominally used for entry and landing/touchdown. Same as Mission Abort.
Analysis	A verification method utilizing techniques and tools such as math models, prior test data, simulations, analytical assessments, etc. Analysis may be used in lieu of, or in addition to, other methods to ensure compliance to specification requirements. The selected techniques may include, but not be limited to, engineering analysis, statistics and qualitative analysis, computer and hardware simulations, and analog modeling. Analysis may be used when it can be determined that rigorous and accurate analysis is possible, test is not cost effective, and verification by inspection is not adequate.
Automated	Automatic (as opposed to human) control of a system or operation.

Term	Definition
Autonomous	Ability of a space system to perform operations independent from any ground-based systems or other external command and control center. This includes no communication with, or real-time support from mission control, other ground systems, or other crewed space vehicle.
Bounding Failure Probability	The uncertainty associated with the mean probability of failure estimate that includes an upper and lower bound represented as the 5th and 95th percentiles of a probability distribution.
Catastrophic Event	An event potentially resultingin the death or permanent disability of a crewmember.
Catastrophic Hazard	Any hazard that, when uncontrolled, results in a catastrophic event.
Crew or Crewmember	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.
Crewed Deep Space Systems	Includes deep space crewed in-space transportation, deep space crewed landers, deep space extra-vehicular mobility units, and deep space crewed surface systems including interfaces with control centers and communications infrastructure. The crewed space system consists of all the system elements that are occupied by the crew/passengers during the space mission as well as all elements physically attached to the crewed element during the crewed mission.

Term	Definition
Crewed Deep Space Systems Certification	Certification is the documented authorization granted by the Associate Administrator that allows the use of the crewed deep space systems within its prescribed parameters for its defined mission. Certification of crewed deep space systems to support/transport NASA or NASA sponsored personnel consists of four separate functions: 1) validation of the technical and performance requirements and standards 2) verification of compliance with those requirements/standards 3) consideration of relevant operational experience, such as that gained from past and current human spaceflight programs, problem reporting, mishap investigations, etc. 4) acceptance of residual technical risk due to hazards, waivers, non-compliances, etc.
Crewed Spacecraft	The crewed spacecraft 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 spacecraft also includes all elements physically attached to the crewed element during the mission. The crewed spacecraft is part of the larger space system used to conduct the mission.
Critical	A modifier that must be taken in context of usage. Refer to NASA-HDBK-8709.22 for the meaning within that context.
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.
Deep Space	Being or related to activities conducted beyond Earth's entry interface after separation from a launch vehicle.
Demonstration	A verification method that is generally a basic confirmation of performance capability, differentiated from testing by the lack of detailed data gathering.

Term	Definition
Element	When pertaining to the make-up of the Crewed Deep Space System, an element or crewed element is a spacecraft or surface system.
Emergency	Either a spacecraft or medical emergency unless specifically stated.
Emergency Egress	Capability for a crew to exit the vehicle and leave the hazardous situation or catastrophic event within the specified time.
Emergency Equipment and Systems	Systems (Ground or Flight) that exist solely to prevent loss of life in the presence of imminent catastrophic conditions. Examples include fire suppression systems and extinguishers, emergency breathing devices, and crew escape systems. Emergency systems are not considered a leg of failure tolerance for the nominal, operational equipment and systems, and do not serve as a design control to prevent the occurrence of a catastrophic condition. Emergency equipment and systems are not required to be designed and tested to the full range of functional, performance and certification requirements defined for the nominal, operational equipment and systems

Term	Definition
Endorsement	Concurrence that: • The Human Rating Certification evidence is satisfactory and represents acceptable progress toward formal certification in conjunction with flight readiness determination • All related items identified at the previous milestone have been satisfactorily resolved and documented • All waivers and exceptions to certification requirements or technical requirements have been reviewed and satisfactorily dispositioned. Final Endorsement constitutes agreement that the Program has satisfactorily completed the crewed space certification activities including the technical requirements for human-rated systems, except as noted within the approved waivers and exceptions identified as applicable to Human Rating.
Failure Tolerance	The ability to sustain a certain number of failures and still retain a specific capability (e.g. capability to control hazards, capability to continue the mission, etc.). A component, subsystem, or system that cannot sustain at least one failure is not considered to be failure tolerant.
Habitable	The environment that is necessary to sustain the life of the crew and to allow the crew to perform their functions in an efficient manner. These environments are described in NASA-STD-3001.
Hazard	A state or a set of conditions, internal or external to a system, that has the potential to cause harm (Source - NPR 8715.3).
Hazard Analysis	The process of identifying hazards and their potential causal factors.

Term	Definition
Health & Status Data	Data including Emergency, Caution, and Warning data that can be analyzed or monitored describing the ability of the system or system components to meet their performance requirements.
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.
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.
Human Rating	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. Human-rating consists of three fundamental tenets: 1) Human-rating is the process of designing, 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.
Incapacitated Crewmember	Crewmember with injury or illness requiring temporary or continuous assistance from one or more fellow crewmembers to perform tasks (e.g. Ingress Lander, Fasten seat harness, etc.) required to return to Earth.

Term	Definition
In-space	Being or related to activities conducted beyond Earth's entry interface after separation form a launch vehicle and not within the atmosphere of other celestial bodies.
Inspection	A method of verification or validation through the use of visual observations, physical measurement techniques, review of design, review of records, or review of other verification activities.
Interoperability	The ability of two or more systems to physically interact; exchange data, information, or consumables; or share common equipment while successfully performing intended functions.
Loss of Crew	Death or permanently debilitating injury to one or more crewmembers.
Loss of Mission	Loss of or the inability to complete the primary mission objectives
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 affect 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 affect any attitude within the capability of the flight/attitude control system.
Mission	The mission begins with entry of the crew into the spacecraft, includes launch, orbital operations, and entry and ends with successful delivery of the crew to NASA after landing.
NASA Crew	The NASA crewmembers or the NASA sponsored crewmembers. These include international partner crewmembers.
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."

Term	Definition
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 the final phase of rendezvous within the prescribed safe zone up to docking, undocking, and separation and active attitude control of the integrated stack through exit of the prescribed safe zone.
NASA Program Manager	The program manager is responsible for the formulation and implementation of the program. This includes responsibility and accountability for the program safety; technical integrity; technical, cost, and schedule performance; risk acceptance; and mission success. Note: responsibility for program management and certification may shift throughout the lifetime of a program
Reliability	The probability that a system of hardware, software, and human elements will function as intended over a specified period of time under specified environmental conditions.
Rendezvous	The flight phase of executing a series of onorbit maneuvers to move the spacecraft into the proximity of its target.
Rescue	The process of locating the crew, proceeding to their position, providing assistance, and transporting them to a location free from danger.
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).
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.

Term	Definition
Safe Haven	Safe haven is a contingency crew survival capability, and therefore may involve rationing food and water, lack of exercise, and lack of access to nominal crew support systems during the safe haven period where the safe haven habitat is not nominally expected to support such a period.
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.
Software	Software: (1) computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system (2) all or a part of the programs, procedures, rules, and associated documentation of an information processing system (3) program or set of programs used to run a computer (4) all or part of the programs which process or support the processing of digital information (5) part of a product that is the computer program or the set of computer programs. The software definition applies to software developed by NASA, software developed for NASA, software maintained by or for NASA, COTS, GOTS, MOTS, OSS, reused software components, auto-generated code, embedded software, the software executed on processors embedded in programmable logic devices, legacy, heritage, applications, freeware, shareware, trial or demonstration software, and open-source software components.
System Disposal	An end-of-mission process for moving a spacecraft (if necessary) to an orbit or trajectory considered acceptable for orbital debris limitation. Includes capabilities to de-energize, depressurize and/or inert systems where disposal locations (e.g. lunar lander near lunar surface basecamp) may expose crew or crewed systems to long term risks.

Term	Definition
Technical Authority	The NASA individual who specifically maintains technical responsibility for establishment of, changes to, and waivers of requirements in a designated area. There are three Technical Authorities: Engineering, Safety and Mission Assurance, Health and Medical.
Test	A method of verification in which technical means, such as the use of special equipment, instrumentation, simulation techniques, and the application of established principles and procedures are used for the evaluation of components, subsystems, and systems to determine compliance with requirements. Test will be selected as the primary method when analytical techniques do not produce adequate results; failure modes exist which could compromise personnel safety, adversely affect flight systems or payload operation, or result in a loss of mission objectives; or for any components directly associated with spacecraft to spacecraft interfaces. The analysis of data derived from tests is an integral part of the test program, and should not be confused with analysis as defined above. Tests will be used to determine quantitative compliance to requirements and produce quantitative results.
Spacecraft	A vehicle designed to operate, with or without a crew, and maintain a controlled flight pattern above Earth's lower atmosphere.
Validation	Proof that the product accomplishes the intended purpose. May be determined by a combination of test, analysis, and demonstration.
Verification	Proof of compliance with a requirement or specifications based on a combination of test, analysis, demonstration, and inspection.
Verification Plan	A formal document listing the specific technical process to be used to show compliance with each requirement.
Waiver	A written authorization allowing relief from a requirement.

APPENDIX C OPEN WORK

C1.0 To Be Determined (TBD)

Table C1-1 lists the specific To Be Determined items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed. The TBD item is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., TBD-HEOR-xxx). As each TBD is resolved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBDs will not be renumbered.

Table C1-1 To Be Determined Items

TBD	Section	Description

C2.0 To Be Resolved (TBR)

Table C2-1 lists the specific To Be Resolved issues in the document that are not yet known, but a credible point of departure value is offered. The TBR is inserted as a placeholder wherever the required data is needed. The TBR issue is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., TBR-HEOR-xxx). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBRs will not be renumbered.

Table C2-1 To Be Resolved Issues

TBR	Section	Description
TBR-HEOR-001	6.2	Impact of addition of GP 10008, Gateway Subsystem Specification for Power, Appendix F to be evaluated
TBR-HEOR-002	6.2	Impact of addition of NASA-STD-1006, Space System Protection Standard to be evaluated
TBR-HEOR-003	6.2	Impact of addition of NASA-STD-6030 Additive Manufacturing Requirements for Spaceflight Systems to be evaluated
TBR-HEOR-004	6.2	Impact of addition of NASA-STD-7012 Leak Test Requirements to be evaluated
TBR-HEOR-005	6.2	Impact of NPR 8715.24 Planetary Protection Provisions for Robotic Extraterrestrial Missions