NASA Procedural Requirements

NPR 8705.2C
Effective Date: July 10, 2017
Expiration Date: July 10, 2022

COMPLIANCE IS MANDATORY

Human-Rating Requirements for Space Systems

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Preface

P.1 Purpose

a. NASA's policy is to protect the health and safety of humans involved in or exposed to space activities, specifically the public, crew, passengers, and ground personnel. This policy is implemented through the application of NASA directives and standards.

b. The significant monetary investment for complex space hardware requires all missions to meet high standards of reliability and mission success. The purpose of this NASA Procedural Requirements (NPR) document is to define and implement the additional processes, procedures, and requirements necessary to produce human-rated space systems that protect the safety of the crew and passengers on NASA space missions.

c. A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards and manages safety risk associated with human spaceflight, and provides, to the maximum extent practical, the capability to safely recover the crew from hazardous situations. Human-rating is not and should not be construed as certification for any activities other than carefully managed missions where safety risks are evaluated and determined to be acceptable for human spaceflight.

d. Human-rating must be an integral part of all program activities throughout the life cycle of the system including (but not limited to) design and development; test and verification; program management and control; flight readiness certification; mission operations; sustaining engineering; and maintenance, upgrades, disposal, and ground processing.

e. This NPR requires applicable space systems as defined in paragraph P.2 to obtain a Human-Rating Certification prior to the first crewed mission and maintain the rating throughout the systems' life cycle.

P.2 Applicability

a. This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to JPL (a Federally-Funded Research and Development Center), other contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the applicable contracts, grants, or agreements.

b. The human-rating requirements in this NPR apply to the development and operation of crewed space systems developed by NASA and used to conduct NASA human spaceflight missions. This NPR may apply to other crewed space systems when documented in separate requirements or agreements.

> *Note 1: The Human-Rating Certification is granted to the crewed space system, but the certification process and requirements affect functions and elements of other mission systems, such as control centers, launch pads, and communication systems. Refer to the definitions in Appendix A for further information. The types of crewed space systems that require a Human-Rating Certification (per this NPR) include, but are not limited to, spacecraft and their launch vehicles, planetary bases, and other planetary surface mobility*

systems that provide life support functions, and Extravehicular Activity (EVA) suits.

Note 2: As defined in this NPR, a crewed space system consists of all the system elements that are occupied by the crew during the mission and provide life support functions for the crew. The crewed space system also includes all system elements that are physically attached to the crewed-occupied element during the mission, while the crew is in the vehicle or system. Each independent element is not required to obtain a Human-Rating Certification - the certification is for the entire crewed space system. However, the NASA 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 A, definition of "crewed space system," for examples as they relate to Human-Rating Certification.

Note 3: Human-Rating Certifications, per this NPR, are based on reference missions. During the reference missions, the crewed space system interfaces with other systems (control centers, launch pads, space communication systems). Some of the requirements in this NPR, such as failure tolerance and inadvertent action requirements, cross the interface to other systems. The implementation of those requirements (across the interface) would be part of the Human-Rating Certification for the crewed space system. Therefore, the other systems that are part of the reference mission, such as control centers and launch pads, do not require a separate Human-Rating Certification per this NPR.

Note 4: When multiple crewed elements are part of the reference mission, the NASA Program Manager may elect to define multiple crewed systems, each with its own Human-Rating Certification.

Note 5: Some Human-Rating Certifications may be based on reference missions with generic capabilities, such as a spacecraft mission to grapple and service satellites, or a station or planetary outpost with the potential for multiple types of visiting vehicles. For these certifications, the NASA Program Manager may develop program documentation (such as interface requirements or mission safety requirements) to implement the requirements and capabilities in this NPR for multiple types of systems that may physically attach to the human-rated system during the mission.

c. The International Space Station (ISS) and Soyuz spacecraft are not required to obtain a Human-Rating Certification in accordance with this NPR. These programs utilize existing policies, procedures, and requirements to certify their systems for NASA missions.

Note: All ISS visiting spacecraft are required to meet the ISS interface requirements (previously called "visiting vehicle requirements"). The Human-Rating Certification for a spacecraft going to ISS considers the ISS as a previously certified system. A spacecraft human-rating does not supersede or obviate the need to meet requirements established by other spacecraft for visitation, docking, and proximity operations.

d. In cases where system applicability, as defined in P.2.1 and P.2.2, is not clear, the Program Manager obtains a determination of applicability for human-rating in accordance with this NPR from

the NASA Administrator, as the authority for human rating.

e. The requirements in this NPR do not apply to a space system provided by a foreign entity unless documented in a bilateral or multilateral agreement with such entity.

f. For space systems that require a Human-Rating Certification, the Program Manager is responsible for compliance with this NPR. The Program Manager uses program requirements documents, specifications, contract clauses, and statements of work to direct contractors to comply with this NPR.

g. In this NPR, all document citations are assumed to be the latest version unless otherwise noted.

h. The requirements in this NPR supersede any conflicting requirements imposed by other NASA procedural requirements and standards.

i. The requirements in this NPR supplement requirements imposed by other Federal Government agencies.

j. In this NPR, a requirement is identified by "shall," descriptive material by "is," and permission by "may."

k. Requests for waivers, deviations, and exceptions to this NPR require the approvals described in paragraph 1.4 of this NPR. In the case of unresolved dissenting opinions, the NASA Administrator, as the authority for human-rating, dispositions the requests.

l. This edition of the NPR addresses the state of knowledge concerning human-rated systems at the time of release. It does not completely address all of the unique requirements that may be required for future capabilities such as lunar surface systems and systems developed for missions to Mars. Future revisions of this NPR are necessary to develop and document those additional requirements.

P.3 Authority

a. The National Aeronautics and Space Act, 51 U.S.C. § 20113(a).

b. NPD 7120.4, NASA Engineering and Program/Project Management Policy.

c. NPD 8700.1, NASA Policy for Safety and Mission Success.

P.4 Applicable Documents

a. NPR 8715.3, NASA General Safety Program Requirements.

b. NASA-Standard-3001 Volume 1: Space Flight Human-System Standard: Crew Health.

c. NASA-Standard-3001 Volume 2: Space Flight Human-System Standard: Human Factors, Habitability, and Environmental Health.

d. FAA HFDS - Human Factors Design Standard.

P.5 Measurement/Verification

Verification of program compliance with the requirements contained within this NPR is performed in conjunction with selected milestone reviews (System Requirements Review (SRR), System Definition Review (SDR), Preliminary Design Review (PDR), Critical Design Review (CDR),

System Integration Review (SIR), and the Operational Readiness Review (ORR)) conducted in accordance with the requirements of NPR 7120.5, NASA Space Flight Program and Project Management Requirements, and NPR 7123.1, NASA Systems Engineering Processes and Requirements. This NPR specifies development of products that are reviewed at each of the selected milestone reviews. The adequacy of those products and the acceptability of progress toward Human-Rating Certification are used to verify compliance with this NPR. In addition, the requirements and processes defined within this NPR are subject to audit and assessment in accordance with the requirements contained within NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.

P.6 Cancellation

NPR 8705.2B, Human-Rating Requirements for Space Systems, dated May 6, 2008.

Chapter 1. Human-Rating Certification Process

1.1 Introduction

1.1.1 NASA's policy is to protect the health and safety of humans involved in or exposed to space activities, specifically the public, crew, passengers, and ground personnel. This policy is implemented through the application of NASA Directives and Standards. The following abbreviated documentation tree (Figure 1) shows where the health, safety, and engineering directives and standards exist in relationship to Agency Program management directives and standards. (Refer to http://www.hq.nasa.gov/office/codeq/doctree/qdoc.htm for a more extensive documentation tree.) This depiction also corresponds to the overall governance structure that establishes checks and balances between Programs and the three Technical Authorities of Engineering, Health and Medical, and Safety and Mission Assurance. This NPR contains requirements under the collective jurisdiction of the three Technical Authorities and the Director, JSC (for crew risk acceptance); however, for administrative purposes, it is located within the Safety and Mission Assurance Directives block of Figure 1.

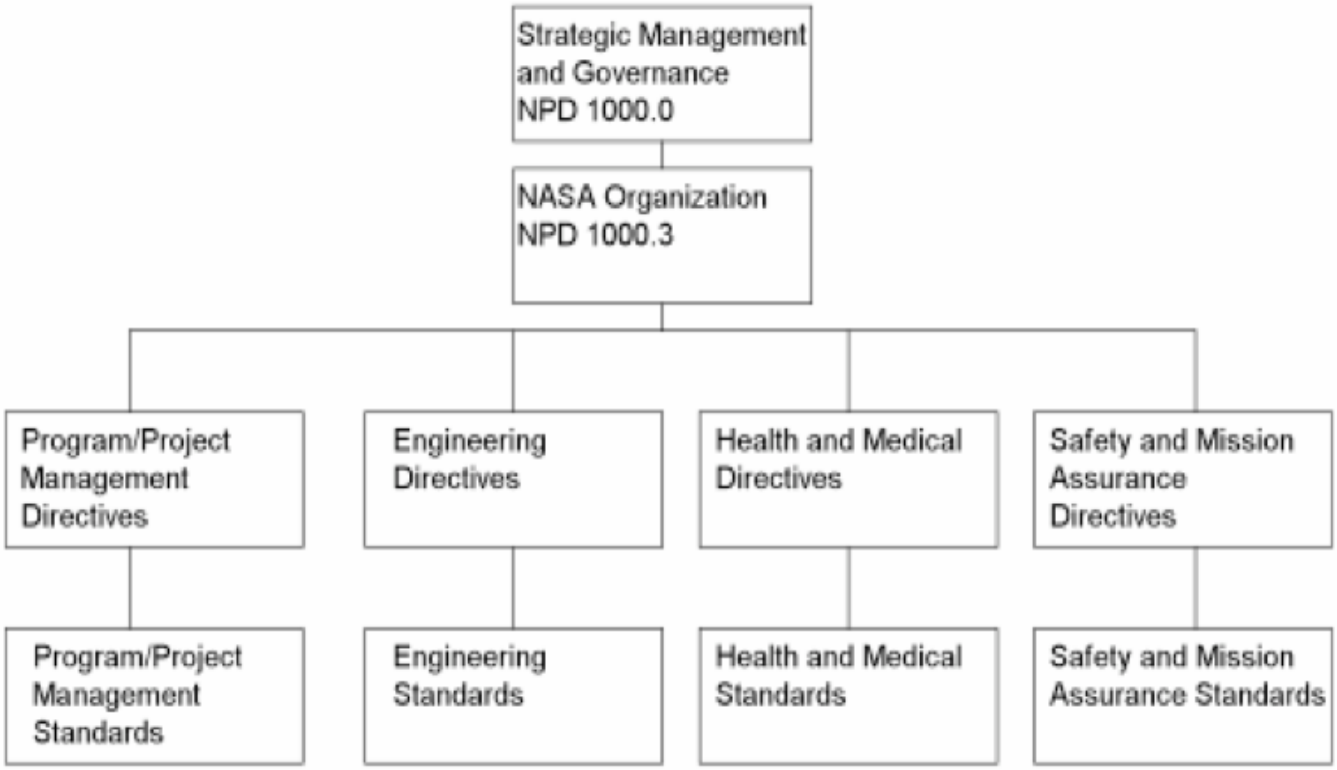

Figure 1. Agency Requirements Framework Related to Human Rating

1.1.2 The significant monetary investment for complex space hardware requires all missions to meet high standards of public safety, reliability, and mission success. The purpose of this NPR is to define and implement processes, procedures, and requirements necessary to produce human-rated space systems that protect the safety of the crew and passengers on NASA space missions. Human-rating further requires implementation of requirements contained in NASA directives that are mandatory for any high value and high-priority space flight program and project conducted by or for NASA, as

well as those standards designated as mandatory by the Office of the Chief Engineer (https://standards.nasa.gov/), Office of Safety and Mission Assurance (http://www.hq.nasa.gov/office/codeq/doctree/doctreec.htm), and the Office of the Chief Health and Medical Officer (http://www.nasa.gov/offices/ochmo/policy_stds/index.html). In addition, and as part of the human rating process defined in this NPR, Technical Authorities may impose other standards to the design concept and its mission on a case-by-case basis. The following diagram (Figure 2) illustrates how this NPR integrates with other NASA directives to provide direction for the Program Manager.

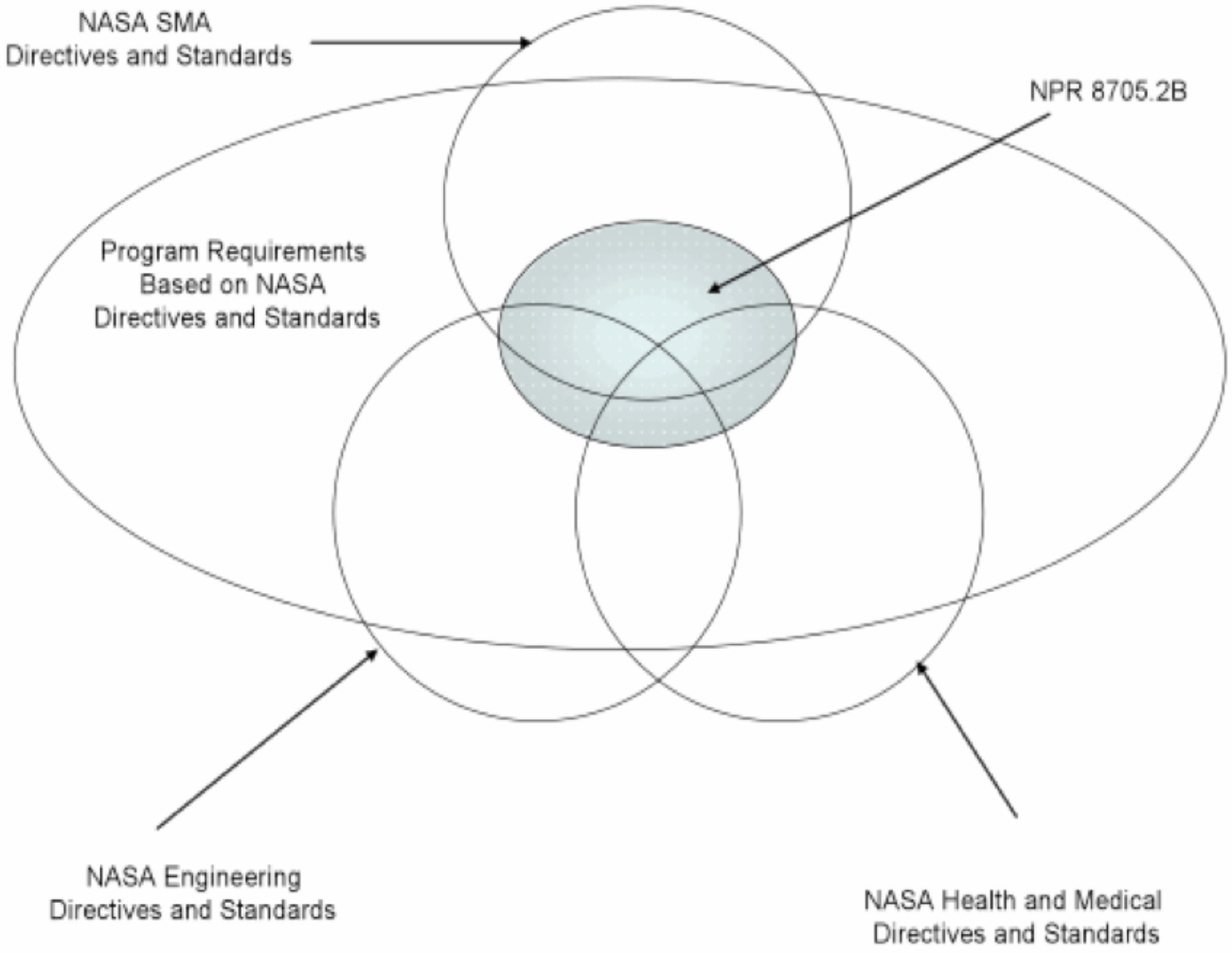

Figure 2. Relationship Among Requirements

1.1.3 It is impossible to develop a set of Agency-level technical requirements that will definitively result in the development of safe systems for all human space missions. Compliance with directives and standards can provide the framework for safety; however, the Program Manager is responsible for providing safe and reliable systems for human missions. The Technical Authorities provide the necessary checks and balances to assure safe and reliable systems. Throughout the design and development process, the program management is responsible for making the decisions that assure the system works, is safe, and is affordable. The Technical Authorities challenge the developers to describe the rationale for their design decisions and help identify hazards and safer alternatives. Recognizing that a certain level of risk needs to be accepted to conduct human spaceflight, this process is guided by Administrator-approved safety goals and thresholds defining long-term

targeted and maximum tolerable levels of risk (minimum tolerable level of safety). These are specified at the system-level rather than at the local level and are expressed in terms of metrics such as the probability of a loss of crew. Safety goals and thresholds must match the type of mission being conducted and are used in addition to other safety criteria, such as the requirement for the system to be failure tolerant and provide crew escape and survival capabilities, to result in a human-rated system. This NPR contains a Human-Rating Certification process to help the Program Manager and the Technical Authorities maintain the focus of the entire development and operation team on crew safety. This NPR also contains a set of technical requirements that establish a benchmark of capabilities for Human-Rated systems. These technical requirements should not be interpreted as all inclusive or absolute. The Program Manager is expected to evaluate the intent of these technical requirements and use the talents of the development and operation team to design the safest practical system that accomplishes the mission within constraints. By doing so, the program is expected to arrive at an optimal solution that represents the best overall value considering cost, schedule, performance, and safety.

1.1.4 Above all, human-rating is more than a set of requirements, a process, or a certification - it involves a mindset, instilled by leadership, where each person feels personally responsible for their piece of the design and for the safety of the crew.

1.2 Definition of Human-Rating

1.2.1 In order to understand human-rating, the following question must be

answered: "What is fundamentally different about developing and certifying systems to take humans into space as compared to a multibillion dollar, one of a kind, robotic payload?"

1.2.2 This question has been answered several times over more than 50 years in the development of Mercury, Gemini, Apollo, Skylab, Space Shuttle, and the ISS systems. Lessons learned from these programs lead to the following definitions of human-rated systems and human-rating for this NPR:

a. 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.

b. 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.

c. Human-rating is an integral part of all program activities throughout the life cycle of the system, including (but not limited to) design and development; test and verification; program management and control; flight readiness certification; mission operations; sustaining engineering; and maintenance, upgrades, disposal, and ground processing.

1.2.2.1 Tenet 1 of the definition describes the additional rigor and scrutiny involved in the design, development, certification, and operation of human-rated space systems. Designing a space system, with constraints of mass and volume, often requires compromise to reach a design that can perform the mission, including the safe return of the crew and passengers. In many respects, systems

engineering is about managing compromise. The risks associated with each decision must be understood and carefully considered. Throughout the design and development process, the engineering, safety, and health and medical disciplines external to the program must constantly challenge the developers to articulate the rationale for their design decisions. Once the system is developed and deployed, additional rigor and scrutiny are applied at every mission readiness review. Development and operation teams continually look for ways to reduce the potential for uncontrolled hazards by exploring potential risks and uncertainties. Reducing the uncertainties in the design and operations, exploring all safety risks, and recognizing the potential for hazards obscured by system complexity are all part of a human-rating mindset.

1.2.2.2 Tenet 2 of the definition accounts directly for the presence of humans in the spacecraft or space system. In addition to providing for the basic human needs such as environment, food, and water, the astronauts onboard the spacecraft must be given some level of control over the system. This tenet acknowledges two primary reasons for human control of the space system - improving safety and accomplishing the mission.

1.2.2.3 Tenet 3 of the definition recognizes that the human exploration of space involves inherent risk and, despite our best efforts, unanticipated and unexpected hazards may occur. When developing spacecraft to carry humans, the design team incorporates capabilities and safeguards that allow for the safe return of the crew after system failures prevent mission continuation. Additionally, whenever practical, the system provides capabilities for the crew to survive potentially catastrophic hazards, catastrophic events, and emergency situations.

1.3 Overview of the Human-Rating Certification Process

1.3.1 The Human-Rating Certification Process is based on the certification requirements in Chapter 2 of this NPR. These certification requirements lead the Program Manager through specific aspects of human-rating and document the results in a Human-Rating Certification Package (HRCP). The HRCP contains the relevant information for the Human-Rating Certification decision. Since human-rating is a broad topic, the certification requirements were derived from specific aspects of the human-rating definition in paragraph 1.2 of this NPR. The Human-Rating Certification focuses primarily on the integration of the human into the system and preventing catastrophic events during the mission that affect the safety of the crew and passengers. The key certification elements documented in the HRCP are:

a. The definition of reference missions for certification.

b. The incorporation of system capabilities to implement crew survival strategies for each phase of the reference missions.

c. The implementation of capabilities from the applicable technical requirements in Chapter 3 of this NPR.

d. The utilization of safety analyses to influence system development and design.

e. The integration of the human into the system and human error management.

f. The verification, validation, and testing of critical system performance.

g. The flight test program and test objectives.

h. The system configuration management and related maintenance of the Human-Rating Certification.

1.3.2 The Human-Rating Certification Process is linked to five major program milestones: SRR, SDR, PDR, CDR, and ORR. The program's compliance with the human-rating requirements and the contents of the HRCP are concurred and approved by all three Technical Authorities (Safety, Engineering, and Health and Medical) at each of the five milestones. In addition to the review and concurrence of the HRCP at these milestones, a summary of the status of Human-Rating activities is provided at the SIR, highlighting any significant changes that have occurred since CDR. The Director, Johnson Space Center (JSC) also concurs with and approves the HRCP from a crew risk perspective at each of the five milestones. If one or more of the Technical Authorities or the Director, JSC do not approve the contents of the HRCP at a milestone, the difference of opinion is elevated to the NASA Administrator as the authority for human-rating for disposition. Thus, the Program Manager will be able to ensure satisfactory progress toward the Human-Rating Certification. Appendix D contains a listing of the HRCP contents at the five program milestones. After ORR, the Program Manager submits the HRCP and the request for Human-Rating Certification, with the required concurrences, to the NASA Administrator. After system acceptance, and for the life of the program, the Program Manager and Technical Authorities review the human-rating as part of each flight and mission readiness review. If the Program is not using traditional life cycle milestones, then the Program, in conjunction with the TAs and the Director, JSC (for crew risk acceptance), will agree upon and produce a tailored HRCP matrix for the Program milestones, with the maturity of the products being commensurate with the targeted maturity of the Program at each of those milestones. Subsequent changes to the tailored HRCP matrix must be agreed to by the Technical Authorities, Director, JSC (for crew risk acceptance), and the Associate Administrator.

1.4 Roles and Responsibilities

1.4.1 The following paragraphs define the broad roles and responsibilities related to Human-Rating Certification. Delegation of authority and responsibility outlined in this section is at the discretion of each official. However, in all cases, accountability remains at the highest level.

1.4.2 The NASA Administrator is the authority for human-rating and is responsible for certifying systems as human-rated. In this capacity, the Administrator shall:

a. Establish the Agency's risk tolerance by approving safety goals, safety thresholds, and associated rationale for a specified type of mission at or prior to Program initiation.

Note 1: Agency-level safety goals and thresholds define long-term targeted and maximum tolerable levels of risk to the crew as guidance to developers in evaluating "how safe is safe enough" for a given type of mission. Goals and thresholds are specified at the system-level, rather than at the local (e.g., individual hazard) level, and are expressed in terms of an aggregate measure of risk such as the probability of a loss of crew. Additional goals and thresholds may be set for mission phases, though they should generally be independent of the crewed space system's architecture. The specification can be qualitative or quantitative (probabilistic) in nature. Qualitative statements take the form of a comparison to known benchmarks such as an existing system (e.g., "better than Space Shuttle") such that they can be more easily communicated to internal and external stakeholders.

Note 2: Safety thresholds specify the minimum tolerable/allowable level of crew safety (maximum tolerable level of risk) for the design in the context of its design reference mission. Safety thresholds are to be used by the Agency as criteria for program acquisition decisions. Compliance is verified at program milestones and is an input to the

programmatic key decision points defined in NPR 7120.5, NASA Space Flight Program and Project Management Requirements. Thresholds are not meant to be used as a flight readiness requirement or as part of a certification of flight readiness for first flight or for engineering or developmental test flights, human-occupied or not. Thresholds are defined for both one-time and repeated missions. Safety goals specify the level of safety that is considered acceptable for repeated missions and serve as the long-term target for proactive safety upgrade and improvement programs (see paragraph 1.4.8.g). The concept of a safety goal and accompanying requirement to implement a safety upgrade and improvement program is motivated by the fact that the level of risk associated with initially flown designs is typically unacceptable in the long term and the fact that human spaceflight programs, informed by flight experience and analysis, can achieve significant reductions of risk over the life of a program.

b. Make the determination to certify a system as human-rated.

c. Disposition requests for waivers, deviations, and exceptions to this NPR that are appealed to the NASA Associate Administrator.

1.4.3 The NASA Associate Administrator is the Chair of the Program Management Council and is responsible for making recommendations to the Administrator regarding human-rating. In this capacity, the NASA Associate Administrator shall:

a. Propose, with support from the Chief, Safety and Mission Assurance, the Chief Engineer, the Chief Health and Medical Officer, the responsible Mission Directorate, and the flight crews through the Director, JSC, safety goals, safety thresholds, and associated rationale for approval by the Administrator.

b. Revalidate the safety goals, safety thresholds, and associated rationale at PDR and any other time during the acquisition process when changes to mission, environment, or assumptions call for an adjustment of the probabilistic safety requirements at the program level or when a safety goal is met. Rationale: Safety goals and thresholds are revalidated at specific points in the program life cycle to ensure they remain consistent with stakeholders' expectations in light of changing conditions or updated states of knowledge.

c. At PDR, decide on the Agency's endorsement of progress toward Human-Rating Certification.

d. Endorse requests to certify a system as human-rated.

1.4.4 The Chief, Safety and Mission Assurance, is the Lead Technical Authority for Safety and Mission Assurance and is responsible for assuring the implementation of safety-related aspects of human-rating. The Chief, Safety and Mission Assurance, shall:

a. Prior to SRR, designate the mandatory safety standards and any relevant safety topic areas that require program-level standards.

Rationale: It is the Safety and Mission Assurance Technical Authority's responsibility to mandate the safety-related standards to be used by the program and approve the additional standards selected for use by the program. It is also incumbent on the Safety and Mission Assurance Technical Authority to inform the program of additional relevant safety-related topic areas that require program-level standards. The applicable standards in this NPR are those which the Technical Authorities have deemed mandatory for all human-rated systems. Depending on the type of system being human-rated, it is expected that the Safety and Mission Assurance Technical Authority will mandate additional safety-related standards

for Human-Rating Certification. Standards may be mandated through NASA directives or other written directives to the program.

b. Obtain the required endorsements and approval of the safety goals, safety thresholds, and associated rationale.

c. Evaluate the acceptability of the technical basis for certification documented in the HRCP, and concur or non-concur at designated milestones with the progress toward Human-Rating Certification.

d. Determine the acceptability of the system for Human-Rating Certification.

Note: Designation of acceptability for Human-Rating Certification is accomplished by concurring on the Program Manager's request for Human-Rating Certification.

e. Disposition requests for exceptions, exemptions, deviations, and waivers to the requirements in this NPR, subject to concurrence from the Engineering and Health and Medical Technical Authorities and the Director, JSC. Rationale: The NASA Governance Model emphasizes having a single manager responsible for making and executing decisions. The Chief, Safety and Mission Assurance, as the Responsible Office for this NPR, dispositions requests for exceptions, deviations, and waivers. Since many of the requirements within this NPR cross Technical Authority boundaries or affect risk to the crew, dispositions are subject to concurrence by the Engineering and the Health and Medical Technical Authorities and the Director, JSC as indicated in paragraphs 1.4.5, 1.4.6, and 1.4.9.

f. Determine the validity of the Human-Rating Certification for each mission/flight per the certification requirements of this NPR.

Note: The Human-Rating Certification is reviewed as part of every flight/mission certification. The specific criteria to be reviewed are contained in paragraphs 2.6.3 and 2.6.4. The determination of validity is made by concurring or non-concurring with flight/mission certification.

1.4.5 The Chief Engineer is the Lead Technical Authority for Engineering and is responsible for assuring the implementation of engineering-related aspects of human-rating. The Chief Engineer shall:

a. Prior to SRR, designate the mandatory engineering standards and the relevant engineering topic areas that require program-level standards.

Rationale: It is the Engineering Technical Authority's responsibility to mandate the engineering standards to be used by the program and approve the additional standards selected for use by the program. It is also incumbent on the Engineering Technical Authority to inform the program of additional engineering topic areas that require program-level standards. The applicable standards in this NPR are those which the Technical Authorities have deemed mandatory for all human-rated systems. Depending on the type of system being human-rated, it is expected that the Engineering Technical Authority will mandate additional engineering standards for Human-Rating Certification. Standards may be mandated through NASA directives or other written directives to the

program.

b. Evaluate the acceptability of the technical basis for certification documented in the HRCP, and concur or non-concur at designated milestones with the progress toward Human-Rating Certification.

c. Determine the acceptability of the system for Human-Rating Certification.

Note: Designation of acceptability for Human-Rating Certification is accomplished by concurring on the Program Manager's request for Human-Rating Certification.

d. Determine the acceptability of requests for exceptions, exemptions, deviations, and waivers to the requirements in this NPR.

Note: The Chief, Safety and Mission Assurance, as the Responsible Office for this NPR, dispositions requests for exceptions, deviations, and waivers. Since many of the requirements within this NPR cross Technical Authority boundaries or affect risk to the crew, dispositions are subject to concurrence by the Engineering and the Health and Medical Technical Authorities and the Director, JSC. Determination of acceptability is made by concurring or non-concurring on the request.

e. Determine the validity of the Human-Rating Certification for each mission/flight per the Certification Requirements of this NPR.

Note: The Human-Rating Certification is reviewed as part of every flight/mission certification. The specific criteria to be reviewed are contained in the paragraphs 2.6.3 and 2.6.4. The determination of validity is made by concurring with flight/mission certification.

1.4.6 The Chief Health and Medical Officer is the Lead Technical Authority for human health and performance and is responsible for assuring the implementation of human health and performance aspects of human-rating. The Chief Health and Medical Officer shall:

a. Prior to SRR, designate the mandatory human health and performance standards and the relevant human health and performance topic areas that require 'program level' standards.

Rationale: It is the Health and Medical Technical Authority's responsibility to mandate standards for human health and performance to be used by the program and approve the additional standards selected for use by the program. It is also incumbent on the Health and Medical Technical Authority to inform the program of additional human health and performance topic areas that require program-level standards. The applicable standards in this NPR are those which the Technical Authorities have deemed mandatory for all human-rated systems. Depending on the type of system being human-rated, it is expected that the Health and Medical Technical Authority will mandate additional human health and performance standards for Human-Rating Certification. Standards may be mandated through NASA directives or other written directives to the program.

b. Evaluate the acceptability of the technical basis for certification documented in the HRCP, and concur or non-concur at designated milestones with the progress toward Human-Rating Certification.

c. Determine the acceptability of the system for Human-Rating Certification.

Note: Designation of acceptability for Human-Rating Certification is accomplished by concurring on the Program Manager's request for Human-Rating Certification.

d. Determine the acceptability of requests for exceptions, exemptions, deviations, and waivers to the requirements in this NPR.

Rationale: The Chief, Safety and Mission Assurance, as the Responsible Office for this NPR, dispositions requests for exceptions, deviations, and waivers. Since many of the requirements within this NPR cross Technical Authority boundaries or affect risk to the crew, dispositions are subject to concurrence by the Engineering and the Health and Medical Technical Authorities and the Director, JSC. Determination of acceptability is made by concurring or non-concurring on the request.

e. Determine the validity of the Human-Rating Certification for each mission/flight per the certification requirements of this NPR.

Note: The Human-Rating Certification is reviewed as part of every flight/mission certification. The specific criteria to be reviewed are contained in the paragraphs 2.6.3 and 2.6.4. The determination of validity is made by concurring with flight/mission certification.

1.4.7 The Associate Administrator for the responsible Mission Directorate shall:

a. Ensure that the Agency-level safety goals, safety thresholds, and associated rationale, as approved by the Administrator, are documented in the Formulation Authorization Document and Program Commitment Agreement.

b. Ensure the inclusion of probabilistic safety requirements derived from the Agency-level safety goals and safety thresholds in the appropriate Program-level documents.

c. Provide the Program Manager with resources to sustain a safety upgrade and improvement program for the duration of the program or until the safety goals have been met.

Note: See the rationale for the related requirement in paragraph 1.4.8.g.

d. Endorse the progress toward Human-Rating Certification at SRR, SDR, CDR, and ORR.

e. Provide programmatic concurrence on progress toward Human-Rating Certification at each designated milestone.

f. Determine the acceptability of the system for Human-Rating Certification.

Note: Designation of acceptability for Human-Rating Certification is accomplished by concurring on the Program Manager's request for Human-Rating Certification.

g. Obtain Technical Authority, Director JSC (for crew risk acceptance), and Associate Administrator approval on any tailored HRCP matrix and any subsequent changes.

1.4.8 The Program Manager is responsible for providing, maintaining, and operating the human-rated system. The Program Manager shall:

a. Develop and maintain, under configuration control, the HRCP with the products defined by the certification requirements in Chapter 2 of this NPR.

b. Provide a summary of the status of human-rating activities at the SIR highlighting any significant changes that have occurred since the CDR.

Rationale: There can be a significant time period between CDR and ORR. This status summary ensures that human-rating remains visible during this time period, but without requiring a formal update and delivery of the HRCP.

c. Comply with the certification and technical requirements in this NPR.

d. Prepare requests for waivers, deviations, and exceptions in accordance with NPR 8715.3.

e. Obtain the Human-Rating Certification per the certification requirements in this NPR.

f. Maintain and operate the human-rated system within the Human-Rating Certification per the requirements in this NPR.

g. Implement and maintain a safety upgrade and improvement program to address risks to crew safety identified via flight experience and safety analysis for the duration of the program or until the safety goals have been met.

Note 1: The concept of a safety goal and accompanying requirement to implement a safety upgrade and improvement program is motivated by the fact that the level of risk associated with initially flown designs is typically unacceptable in the long term and the fact that human spaceflight programs, informed by flight experience and analysis, can achieve significant reductions of risk over the life of a program.

Note 2: In cases where a safety goal is met prior to the end of a program, the Agency will revalidate its safety goals (see paragraph 1.4.3.b). At such points, the Agency may choose to relieve the program of its requirement to maintain a continuous investment in safety upgrades and improvements. However, paragraph 2.2.3 requires the program to maintain a safety analysis process to identify, evaluate, and mitigate risks or deficiencies for the life of the program regardless of the satisfaction of applicable safety goals.

1.4.9 The Director, JSC is responsible for accepting the risk to the crew for spaceflight missions conducted with the human-rated system. In this capacity, the Director, JSC shall:

Rationale: Involving humans in spaceflight adds an additional consideration, consenting to

take the risks related to the system and the mission. The Director, JSC is part of the supervisory chain for the actual risk takers and serves to formally consent to take the risks associated with the human-rated system. Subject to the requirements of any international agreements, this consent also applies to international crew members.

Note: The responsibilities of the Director, JSC at the program level with respect to these human-rating requirements are limited in scope to this crew risk perspective. As described in paragraphs 1.3.2 and 1.5.2.1.d, in the event of disagreement between the Program and the Director, JSC concerning consent to take risk with respect to human-rating, the matter is elevated via the institutional authority chain to the NASA Administrator, as the authority for human-rating, for disposition.

a. From a crew risk perspective, evaluate the acceptability of the technical basis for certification documented in the HRCP, and concur or non-concur at designated milestones with the progress toward Human-Rating Certification.

Note: The determination of an acceptable level of risk to the crew at each of these milestones is accomplished by endorsing the HRCP at the program milestones.

b. From a crew risk perspective, determine the acceptability of the system for Human-Rating Certification.

Note: Designation of acceptability for Human-Rating Certification is accomplished by concurring on the Program Manager's request for Human-Rating Certification.

c. Determine the acceptability of the risk to the crew for each mission. Rationale: The determination of an acceptable level of risk to the crew is part of each mission or flight certification process, which includes a review of the Human-Rating Certification.

d. Determine from a crew risk perspective the acceptability of residual safety risk associated with requests for exceptions, exemptions, deviations, and waivers to the requirements of this NPR.

1.4.10 The Agency Standing Review Board for the program, as defined in NPR 7120.5, shall review the products described in the certification requirements at the program milestones indicated in the certification requirements.

1.4.11 Individuals with Delegated Technical Authority shall act on behalf of the Lead Technical Authorities in the implementation of the Human-Rating Certification process only to the extent agreed and documented between that individual and the Lead Technical Authority being represented.

Rationale: It is understood that there are some details of the Human-Rating design process for which it would be impractical to burden the Lead Technical Authorities with frequent discussions and decisions. NDP 1000.3 and NPR 7120.5 allow for delegation of the Technical Authority role in these circumstances. Many aspects of the Human-Rating Certification process, however, are highly visible and require direct involvement of the Lead Technical Authorities. It is, therefore, prudent to agree to and document the limits of the delegated Technical Authority.

1.5 Human-Rating Certification Summary Timeline

1.5.1 Figure 3 depicts an overview of the process and the participants involved in the Human-Rating Certification.

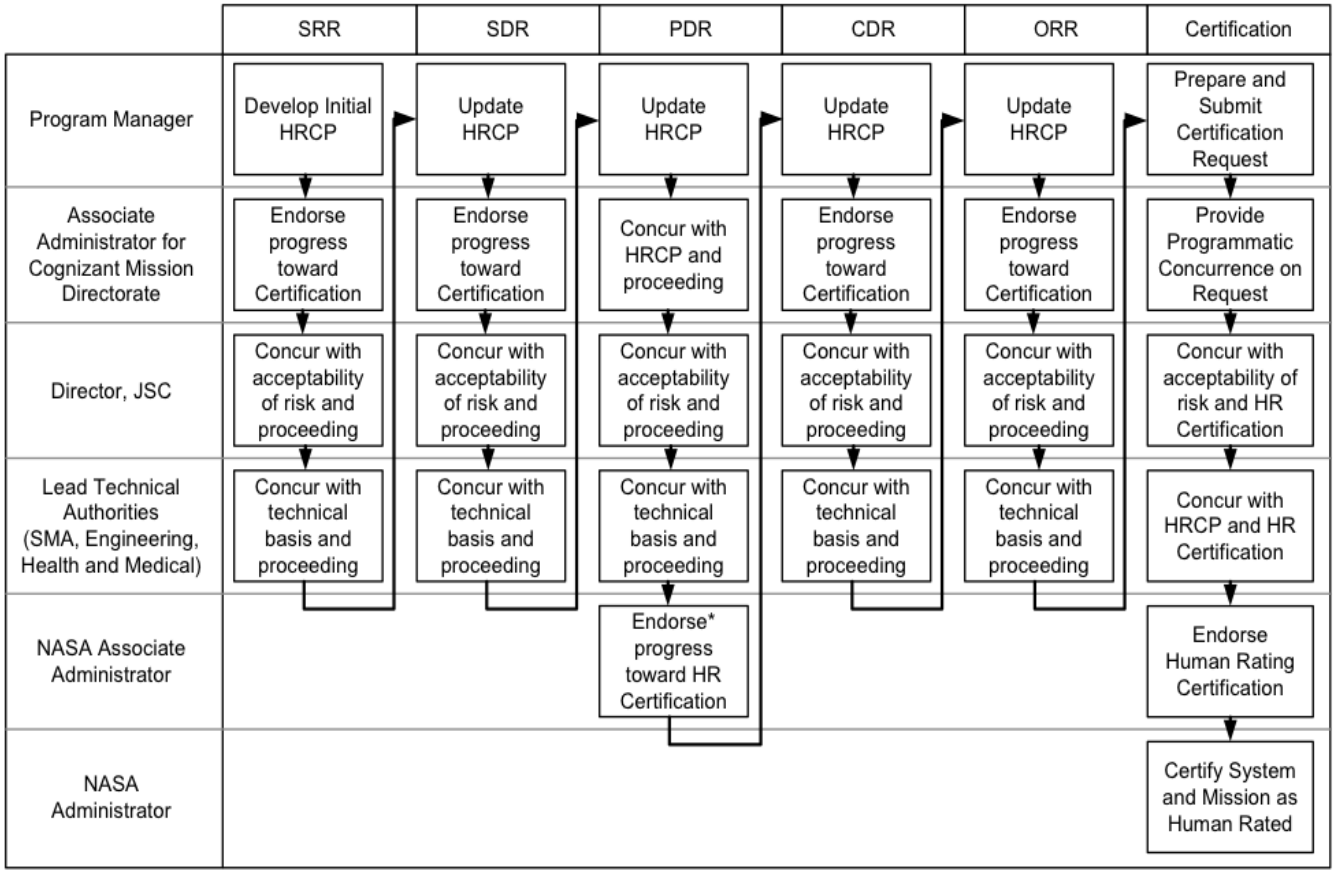

Figure 3. Human-Rating Certification Process Flow

* Note: The human-rating certification is also reviewed as part of each subsequent Readiness Review

1.5.2 The following paragraphs provide a summary of the key events at each milestone in the process.

1.5.2.1 At SRR, SDR, PDR, CDR, and ORR:

a. The Associate Administrator for the responsible Mission Directorate endorses progress toward Human Rating Certification at SRR, SDR, CDR, and ORR and provides programmatic concurrence at all milestones. The Associate Administrator endorses progress toward Human-Rating Certification at PDR.

b. The Lead Technical Authorities and the Director, JSC concur or non-concur with the progress toward Human-Rating Certification using the endorsement form (Appendix E). Approval of the HRCP also constitutes approval of formal presentations to the Review Board that were made to satisfy certification requirements.

c. In the event that one or more of the Technical Authorities or the Director, JSC do not concur with the progress toward Human-Rating Certification at a milestone, the HRCP status will be elevated to

the NASA Administrator as the authority for human-rating for disposition.

d. In addition to the formal review milestones above, at the SIR, the Program Manager provides to the Technical Authorities and the Director, JSC a summary of the status of human-rating activities, highlighting any significant changes that have occurred since the CDR. The summary is provided for information purposes, and no formal review of this summary is necessary.

1.5.2.2 After ORR and prior to the Readiness Review for the first crewed flight/mission:

a. The Program Manager prepares the Human-Rating Certification (Appendix F), which includes the duration of the certification.

b. The request for Human-Rating Certification and the HRCP are concurred with by the Associate Administrator for the responsible Mission Directorate for certification.

c. The Director, JSC and the Lead Technical Authorities concur or non-concur with the HRCP and the request for Human-Rating Certification.

d. The request for Human-Rating Certification and the HRCP are routed to the Associate Administrator for endorsement.

e. The request for Human-Rating Certification and the HRCP are submitted to the NASA Administrator, as the authority for human-rating, for disposition. The request for the Human-Rating Certification should be dispositioned prior to, or concurrent with, the Readiness Review for the first crewed flight/mission.

1.5.2.3 As part of each subsequent Readiness Review for the Human-Rated System, the Program Manager, the Technical Authorities, and the Director, JSC 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.

Chapter 2. Human-Rating Certification Requirements

2.1 Overview

The Human-Rating Certification requirements are designed to lead the Program Manager through the certification process and define the contents of the HRCP. The certification requirements are divided into five categories:

a. Process and Standards

b. Designing the System

c. Verifying and Validating the System Capabilities and Performance

d. Flight Testing the System

e. Certifying and Operating the Human-Rated System

2.2 Process and Standards

2.2.1 HRCP. The Program Manager shall develop and maintain an HRCP for crewed space systems that require NASA Human-Rating Certification.

Note 1: The contents of the HRCP are specified in the following certification requirements. The HRCP reflects the program's progress toward Human-Rating Certification at various milestones and, therefore, is maintained under configuration management control to clearly document changes. When multiple systems of the same configuration are produced from the same design, a single HRCP may apply to all the systems. Paragraph 2.6.4 applies when design changes, configuration changes, block updates, or other changes are incorporated.

Note 2: The Human-Rating Certification is granted to the crewed space system, but the certification process and requirements affect functions and elements of other mission systems, such as control centers, launch pads, and communication systems. Refer to the definitions in Appendix A for further information.

2.2.2 Human-Rating Waivers, Deviations, and Exceptions. At SRR, the Program Manager shall summarize, in the HRCP, all requests for waivers, deviations, and exceptions to the certification and technical requirements in this NPR, as well as any exemptions to the failure tolerance requirement and provide access to the program documentation that contains the waivers, deviations, and exceptions. (This is updated at SDR, PDR, CDR, and ORR.)

Note: For the purposes of this NPR, the term "exception" is equivalent to and interchangeable with a "Determination of nonapplicability" as described in NPR 8715.3, NASA General Safety Program Requirements. The method for documenting approved

exceptions should be described in the Safety and Mission Assurance Program summary (see 2.2.4). Requests for waivers, deviations, and exceptions are submitted in accordance with the requirements contained within NPR 8715.3. The Safety and Mission Assurance Technical Authority dispositions requests for waivers, deviations, and exceptions to the requirements of this NPR. Approved exceptions indicate that a requirement is not applicable and do not represent a non-compliance. The HRCP documents all requests for exceptions, deviations, and waivers submitted for approval by the Technical Authorities and includes the final disposition from the Technical Authorities. Existing program configuration management processes and systems may be used to track these exceptions, deviations, and waivers and support documentation within the HRCP. Individual waivers, deviations, and exceptions to the applicable standards are not to be included in the HRCP.

2.2.3 Safety Analysis Processes. At SRR, the Program Manager shall document in the HRCP, implement, and maintain (for the life of the program) a process for identifying hazards, understanding risk implications of the hazards, modeling hazard scenarios, quantifying and ranking risks to crew safety, and mitigating risks and deficiencies.

Note 1: The intent is that this process for identifying and understanding the hazards (including those resulting from software behavior and human error) and defining and modeling the scenarios (refer to NPR 8715.3) to assess and rank associated crew safety risks, becomes an integral part of the overall iterative design and development process that eliminates hazards, controls the initiating events or enabling conditions related to hazards, and mitigates the resulting effects related to the hazard. This encompasses the use of the reference missions for scenario definition and hazard identification. Integration and consistency between these efforts and any other engineering modeling and assessment activities are also essential.

Note 2: Common approaches or tools for performance of this activity include, but are not limited to, traditional safety and reliability analysis techniques (Hazard Analyses, Fault Tree Analyses, Failure Modes and Effects Analysis, Damage Modes and Effects Analysis, Critical Items Lists), Probabilistic Risk Assessment (PRA) including causes due to human health and human error, Human Error Analysis, simulation modeling techniques (e.g., physics-based abort effectiveness and trigger analyses), and accident precursor analysis. The inter-relationship of these analysis techniques provides a comprehensive risk assessment in which these analytical techniques support and feed each other. Risk assessments should utilize the most current NASA-accepted data and environmental models within any hazard analysis or safety assessment. This requirement explicitly refers to the loss of crew which is the primary emphasis of this NPR; requirements related to hazards associated with the loss of a mission are covered within the content of other 8000 series NASA directives.

Note 3: The process does not need to be documented in a stand-alone document; it may be incorporated in other program documentation such as the integrated Safety and Mission Assurance Plan described in paragraph 2.2.4 of this NPR or in the System Safety Technical Plan described in NPR 8715.3. This requirement will be considered satisfied when the Technical Authorities verify the process has been implemented and documented.

2.2.4 Safety and Mission Assurance Program. Prior to SRR, the Program Manager shall summarize,

in the HRCP, the safety and mission assurance program established in accordance with NPR 8715.3. (This is updated at SDR, PDR, CDR, and ORR.)

Note 1: The program may document the safety and mission assurance program in a stand-alone Safety and Mission Assurance Plan or in a combined form with another program level plan. This plan may be separate from the HRCP. Verification by the Technical Authorities that the program is in place, properly documented, and referenced in the HRCP, satisfies this requirement.

Note 2: The Human-Rating Certification effort focuses on key elements of the overall safety and mission assurance, health, and systems engineering efforts. The effectiveness of implementation of these key elements depends upon the framework and integration of the activities encompassed in the overall safety and mission assurance program. Implementation and subsequent maintenance of all of the elements of the safety and mission assurance program are essential to establish a basis for Human-Rating Certification.

Note 3: Documentation of the safety and mission assurance program is a major element to allow the program team to understand and implement the program. It allows the program team to understand the elements of the safety and mission assurance program, their role(s) in the program, and the interrelationship of the safety and mission assurance program to the overall program elements.

2.2.5 Applicable Standards. The Program Manager shall comply with the following standards:

a. NASA-Standard-3001 Volume 1, Space Flight Human-System Standard: Crew Health.

b. NASA-Standard-3001 Volume 2, Space Flight Human-System Standard: Human Factors, Habitability, and Environmental Health.

c. FAA HFDS - Human Factors Design Standard.

Note: The standards listed are levied onto the program as applicable standards. These standards consist of human-system integration standards, which are unique to human space systems and other standards deemed mandatory by the Technical Authorities. Exceptions, deviations, and waivers to the applicable standards require the approval of the Technical Authorities (see paragraph 2.2.2, Human-Rating Waivers, Deviations, and Exceptions). In all cases, the application of standards remains under the control of the Technical Authorities (see paragraph 2.2.6, Other Standards Mandated by the Technical Authorities). Refer to NPR 7120.10.

2.2.6 Other Standards Mandated by the Technical Authorities. At SRR, the Program Manager shall document, in the HRCP, the list of additional program-level standards mandated by the Technical Authorities as relevant to human-rating, per paragraph 1.4 of this NPR.

Rationale: The intent of this requirement is to ensure that the program has identified and applied the necessary standards early in the system development. The Technical Authorities may mandate standards or topic areas which require standards through other NASA directives or by written direction to the program. In all cases, the standards established by

the program are approved by the Technical Authorities, and the application of the standards remains under the control of the Technical Authorities. Refer to NPD 7120.4.

2.2.7 Summarizing Exceptions Deviations and Waivers to the Applicable Standards. At SRR, the Program Manager shall summarize, in the HRCP, the exceptions, deviations, and waivers to the applicable standards listed in paragraphs 2.2.5 and 2.2.6 and provide access to the program documentation that contains the exceptions, deviations, and waivers. (This is updated at SDR, PDR, CDR, and ORR.)

Rationale: The intent of this requirement is to have the program collectively evaluate the impact to human-rating of the waivers, deviations, and exceptions to the standards mandated by the Technical Authorities for the particular system to be human-rated. It will be left to the program and the Technical Authorities to determine which waivers, deviations, and exceptions are significant and relevant to human-rating. The individual waivers, deviations, and exceptions are not documented in the HRCP, but the program provides the location of and access to the actual waivers, deviations, and exceptions for review.

2.3 Designing the System

2.3.1 Reference Missions. At SRR, the Program Manager shall document, in the HRCP, a description of the crewed space system, its functional interfaces to other systems, and the reference missions that will be certified for human-rating.

Rationale: Defining reference missions establishes the scope of the program to be human-rated and also provides a framework that supports, among other things, identification of crew survival strategies and establishment of scenarios to be used for hazard analysis and risk assessments. The reference missions also define the interfaces with other systems, such as mission control centers, that functionally interact with the crewed space systems.

2.3.2 Identifying System Capabilities for Crew Survival. At SDR, the Program Manager shall document, in the HRCP, a description of the crew survival strategy for all phases of the reference missions and the system capabilities required to execute the strategy. (This is updated at PDR, CDR, and ORR.)

Rationale: The reference missions establish a basis and framework that the program can use to establish the operational scenarios and document the strategies that will be used to enhance crew survival. Incorporating and preserving the capability for the crew to safely return from the mission is a fundamental tenet of human-rating. The scenarios should include system failures and emergencies (such as fire, collision, toxic atmosphere, decreasing atmospheric pressure, and medical emergencies) with specific capabilities (such as abort, safe haven, rescue, emergency egress, emergency systems, and emergency medical equipment or access to emergency medical care) identified to protect the crew. Some specific capabilities, such as abort, are mandated by the technical requirements in Chapter 3 of this NPR. The intent of this requirement is to have the program identify additional capabilities for their specific design that enhance crew survival. Additionally,

the program describes how the survival capabilities will be maintained during the scenarios. The broad strategies and the process used to develop both the reference missions and the strategies that respond to the scenarios help to establish a focus within the program of making crew survival an integral element of the design process. Continued challenges to (and deliberations concerning) the scenarios themselves and the assumptions, analyses, and design decisions that flow from these scenarios are essential to successfully obtaining Human-Rating Certification.

2.3.3 Documenting the Design Philosophy for Utilization of the Crew. At SRR, the Program Manager shall document, in the HRCP, a description of the design philosophy which will be followed to develop a system that utilizes the crew's capabilities to execute the reference missions, prevent aborts, and prevent catastrophic events.

Rationale: The integration of the crew with the space system and utilization of the crew's capabilities to improve safety and mission success comprise the second tenet in the human-rating definition. Establishing and documenting a design philosophy for utilization of the crew are important steps in actually producing such a system. When unexpected conditions or failures occur, the capability of the crew to control the system can be used to prevent catastrophic events and aborts. These capabilities are determined via task analysis for those tasks where there is a crew interface and documented in operation concepts and, later, referenced in the design of crew interfaces and the development of flight procedures.

2.3.4 Incorporating Capabilities into the System Design. At SDR, the Program Manager shall document, in the HRCP, a description of the implementation of the survival capabilities identified in the requirement in paragraph 2.3.2 and provide clear traceability to the highest level program documentation. (This is updated and reviewed at PDR and CDR.).

Note: At SDR, if the design is not determined, describing the implementation consists of identifying the trade studies and analysis to be used to determine implementation. At PDR and CDR, the design that implements the capability is described in increasing detail with traceability to the highest level requirements in program documentation.

2.3.5 Implementing the Technical Requirements. At SRR, the Program Manager shall document, in the HRCP, a description of the implementation of the applicable requirements of Chapter 3 of this NPR and provide clear traceability to the highest level program documentation. (This is updated and reviewed at SDR, PDR, and CDR.).

Note: At SRR, if the design is not determined, describing the implementation consists of identifying the trade studies and analysis to be used to determine implementation. At SDR, PDR, and CDR, the design that implements the requirement is described in increasing detail with traceability to the highest level requirements in program documentation. The description of the implementation of the failure tolerance requirements includes rationale for the level and type of redundancy for critical systems and subsystems.

2.3.6 Allocation of Safety Goals and Thresholds. At SRR, the Program Manager shall document, in the HRCP, probabilistic safety requirements derived from the Agency-level safety goals and safety

thresholds, including any allocations to mission phases and system elements (to be updated at PDR and CDR) .

Rationale: Top-level allocations of probabilistic safety requirements are documented in the HRCP to allow for comparison with the risk estimates produced as part of the design and safety analyses. Allocations established during the earlier phases of the program are treated as preliminary and may be updated as the design matures.

2.3.7 Integration of Design and Safety Analyses

2.3.7.1 The Program Manager shall integrate design and safety analyses to determine the following:

Note 1: This NPR places the responsibility on the program to determine the appropriate implementation of risk reduction measures such as failure tolerance. The program integrates the design and safety analyses to make such determinations based on an understanding of individual risk contributions as well as the total level of risk to the crew.

Note 2: As explained in the note to the requirement in paragraph 2.2.3, safety analyses, as defined by this NPR, combine existing techniques such as Hazard Analysis, Fault Tree Analysis, Failure Modes and Effects Analysis, Damage Modes and Effects Analysis, Critical Items Lists, as well as scenario-based probabilistic risk analyses including human error analysis and simulation modeling techniques (e.g., physics-based abort effectiveness and trigger analyses).

Note 3: The integration of design and safety analysis consists of the active and iterative application of these techniques and the use of the collective results from these analyses to inform design decisions. The integrated analysis is done in a consistent manner throughout the program and at the overall system level. This implies that techniques such as Hazard Analysis, Failure Modes and Effects Analysis, and probabilistic risk analyses cannot be performed in isolation and that such analyses should be internally consistent.

Note 4: The resulting assessments and rankings, along with probabilistic safety requirements, serve to inform decisions regarding safety enhancing measures such as necessary failure tolerance levels, margins, abort triggers, and crew survival capabilities.

Note 5: While the results of the design and safety analysis processes are formally submitted for endorsement by stakeholders such as the Technical Authorities and representatives of the crew at major review milestones, it is intended that these stakeholders are an ongoing part of the analysis and design deliberations, enabling them to challenge the rationale for design decisions and help identify hazards and safer alternatives.

a. A list of the significant risk contributors that together constitute the majority of the total risk to which the crew is subjected. Rationale: A ranking of risk contributors such as accident scenarios or classes of accident scenarios enables the identification of the significant risk contributors that collectively represent the majority of risk to the crew. Ranking is done based on the estimated risk to the crew, accounting for hazard controls, crew survival capabilities, and other risk reduction

measures.

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

Rationale: This requirement is tied to paragraphs 3.2.3 and 3.2.4, which require the crewed space system to be failure tolerant.

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

Rationale: The intent of these requirements is to ensure that the program has analyzed and considered the benefits of dissimilar redundancy and backup systems. Where possible, the crewed space system should provide a backup capability for entry to protect for loss of the primary attitude control and guidance system. Specific focus is placed on dynamic flight phases that do not have an abort option, such as Earth reentry and lunar ascent (other than potentially an abort to lunar orbit), because they can be very unforgiving when multiple or common cause failures occur. There is very limited time for system troubleshooting or reconfiguration and the "time to effect" for loss of a critical capability is often short.

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.

Note: An evaluation of crew survival design and operational capabilities and limitations (functionality, performance, reliability, availability, autonomy, response, activation features, and whether the design requires human interaction) will be used to determine their effectiveness given anticipated conditions and time constraints following the defeat of preventative controls, as well as their impact on the risk to the crew. Evaluations may be qualitative or quantitative and are prioritized based on the risk associated with the accident condition. At a minimum, quantitative (probabilistic) evaluations are performed for crew survival capabilities that are credited with significant reductions of 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.

Rationale: This requirement is tied to paragraph 3.2.2, which requires satisfaction of probabilistic safety requirements with a high degree of certainty. At a minimum, the determination of risk is performed for the system and any phase or system element for which an allocation is established. Other risk contributions are determined in order to decide on risk reduction measures such as failure tolerance.

Note: Types of evidence to support risk estimates commonly include design information and functional allocations, performance analyses, success criteria, other safety and reliability analyses and ground test, flight test, and operational reliability performance data.

2.3.7.2 At SDR, the Program Manager shall summarize, in the HRCP, and present the current understanding of risks and uncertainties and related decisions regarding the system design and application of testing, based on the results of the design and safety analyses performed in accordance with paragraph 2.3.7.1 (this is updated and reviewed at PDR, CDR, and ORR).

Note 1: The Technical Authorities determine compliance with this requirement during the milestone reviews indicated. A formally scheduled discussion, as part of the review milestone with the Technical Authorities and the review board, satisfies the presentation aspect of this requirement. The intent is for the program to show that safety analyses are iteratively used to make design decisions to eliminate hazards, control initiating events, or enabling conditions related to hazards and mitigate the resulting effects related to the hazard. The intent is not to track all decisions and provide a linkage to the assessment that influenced those decisions; rather, the intent is to summarize how the analyses were used.

Note 2: The effectiveness of tools such as Hazard Analyses, Failure Modes and Effects Analysis, Damage Modes and Effects Analysis, Critical Items List, Fault Trees, and PRA is dependent on their integrated use in design activities and the information and data on which they are based. Specific implementation requirements concerning the models and assessment techniques and processes (including the hazard reduction precedence) to be used in relation to this requirement are defined in NPR 8715.3 and NPR 8705.5. The demonstration here shows how these tools were used in the deliberations that: examined design alternatives, identified key uncertainties (e.g., uncertainty in system performance, uncertainty in human performance, or in understanding phenomena) related to the design options, established confidence in the analyses and the resulting design, identified focus areas for testing, and the subsequent decisions that resulted from the deliberations. Since any modeling or analysis process is an abstraction of the design (since it uses assumptions, limits scenarios modeled, and uses both program specific and generic data) the rigorous use of deliberation to identify the thresholds as well as to defend and challenge design options is of greater significance than a final number that results from the analysis.

Note 3: SDR, PDR, and CDR are the key milestones where the requirements, architectures, and design are developed and solidified. These are also the milestones where demonstration and discussion of the use of the techniques and their results are expected. This information can be documented as a part of the safety analysis report described in NPR 8715.3. A ranking of the safety risks to which the crew is subjected, and an assessment of the achievement of probabilistic safety requirements derived from the Agency-level safety goals and thresholds should be provided.

2.3.8 Human-Systems Integration Team. At SRR, the Program Manager shall establish a Human-Systems Integration (HSI) team comprising representation from the system's user community (e.g., astronauts, mission operations personnel, training personnel, ground processing personnel, human factors and human-systems SMEs, etc.), with defined authority, responsibility, and accountability in support of the program's HSI Plan for the crewed space system.

Rationale: Past experience with development of spacecraft and military aircraft has shown that, when a correctly staffed human-system integration team is given the authority, responsibility, and accountability for human-system design and integration, the best possible system is achieved within the schedule and budget constraints. This team focuses

on all human-system interfaces (e.g., crew, launch control, and applicable ground processing operations) and ensures an acceptable crew health and performance environment in the space systems. See NPR 7123.1, NASA/SP-2016-6105 Rev 2, and NASA/SP-2015-3709 for more guidance.

Note: NPR 7123.1 requires that a Human-Systems Integration (HSI) Plan be created and updated throughout the development cycle of a human-rated system. The plan defines how human-system considerations are integrated into the full systems engineering design, verification, and validation life cycle. Updates are required to document the implementation of an HSI design approach to the system and its mission and to demonstrate how the design accommodates human capabilities and limitations. This requirement is consistent with NASA-STD-3001 and other standards for human-centered design and with Federal Agency HSI best practices for development of systems that involve humans and further builds on standards such as NASA-STD-5005. The intent is to ensure that, through developing and executing the HSI Plan, the PM expends the effort to integrate HSI expertise, capture HSI approach, and track HSI metrics throughout the life cycle of the program to increase safety, human performance, and mission success. HSI domains include safety; human factors engineering; operational resources management; training; maintainability and supportability; and habitability and environment. Lessons learned from previous programs and projects have shown that by including stakeholders with expertise in relevant HSI domains, the best possible outcome is achieved for operations and mission success. HSI focuses on all human-system interaction (crew, ground control, and ground processing) that can cause or prevent a catastrophic failure.

2.3.9 Evaluating Crew Workload. At SRR, the Program Manager shall document, in the HRCP, a description of how the crew and ground control workload for the reference mission(s) will be evaluated. (This is updated and reviewed at PDR and CDR.)

Rationale: The design of the system can have a significant impact on crew and ground control workload and productivity. Integration of the human into the system is a fundamental tenet of human-rating. Understanding how the system design affects workload is part of the integration process. Additionally, if the resultant workload during a mission is too high, crew fatigue can affect safety. The expectation is that the evaluation of workload would be tasked to the human-systems integration team. Evaluation of the workload requires the program to establish criteria for the evaluation.

2.3.10 Human-in-the-Loop Integration Evaluation.

2.3.10.1 The Program Manager shall conduct human-in-the-loop usability evaluation for the human-system interfaces and integrated human-system performance testing, with human performance criteria, for critical system and subsystem operations involving crew and ground control performance during crewed operations.

2.3.10.2 At PDR, the Program Manager shall summarize, in the HRCP, and present how the human-in-the-loop usability evaluations for human-system interfaces and integrated human-system performance evaluation results (to date) were used to influence the system design and provide access to the detailed evaluation plans and results. (This is updated at CDR.)

2.3.10.3 At ORR, the Program Manager shall summarize, in the HRCP, how the integrated

human-system performance test results were used to validate the system design and provide access to the detailed test plans and results.

Rationale: The expectation is that human-in-the-loop testing is conducted during the development life cycle and is intended to ensure the integrated system requirements and operational concepts are progressively met. Tests and analyses are the standards utilized to demonstrate the operational concepts and human-system interface design requirements are met. Test and analysis data are used to verify and validate the integrated performance of the space system hardware, software, and human operators in simulated vehicle and mission operations environments. Testing can include quantitative and objective human-in-the-loop testing and simulations of flight-critical systems, vehicle, and mission-level operations in ground-based simulators. In addition, integrated test data should be complemented by usability evaluation data and analysis of human-system interfaces. This data can also be used to inform and validate human error analysis.

2.3.11 Human Error Analysis.

2.3.11.1 The Program Manager shall conduct a human error analysis for all mission phases to include operations planned for response to system failures.

2.3.11.2 At PDR, the Program Manager shall summarize, in the HRCP, and present how the human error analysis (to date) was used to: (This is updated at CDR and ORR.)

a. Understand and manage potential catastrophic hazards which could be caused by human errors.

b. Understand the relative risks and uncertainties within the system design.

c. Influence decisions related to the system design, operational use, and application of testing.

Rationale: Personnel trained in human error analysis (HEA) need to be part of the human-system integration team to perform this analysis. The intent is to show that the HEA (which includes hazard identification, analysis [including process failure modes and effects analysis], and modeling of human behavior) is iteratively used to make design decisions. The effectiveness of HEA tools is dependent on their integrated use in design activities, upgrades, enhancements, and operation-risk trades.

Note: The human error analysis includes all mission operations while the crew is interacting with the space system - including crew and ground control operations, and ground processing operations with flight crew interfaces. This analysis covers response to system failures and abort scenarios. While the potential errors of ground processing personnel are to be considered, their personal safety is not addressed by this NPR. A formally scheduled discussion as part of the review milestone with the Technical Authorities and the review board is necessary to satisfy the presentation aspect of this requirement. The intent of this human error analysis requirement is to have the program:

1) Identify inadvertent operator actions and failure to act which would cause a catastrophic event and determine the appropriate level of tolerance.

2) Identify other types of human error that would result in a catastrophic event.

3) Apply the appropriate error management (per paragraph 2.3.12).

2.3.12 The Program Manager shall design the system 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.

2.4 Verifying and Validating the System Capabilities and Performance

2.4.1 Verifying and Validating Implementation of the Technical Requirements. At SRR, the Program Manager shall document, as part of the HRCP, how the implementation of the technical requirements in Chapter 3 will be verified and validated (with rationale). (This is updated at SDR, PDR, and CDR.)

Rationale: This is linked to the certification requirement in paragraph 2.3.5. From a human-rating perspective, it is important to understand how the implementation of the requirements in Chapter 3 will be validated, which may not be demonstrated by requirements verification alone.

2.4.2 Verifying and Validating Survival Capabilities. At CDR, the Program Manager shall document, as part of the HRCP, how the implementation of survival capabilities from the requirement contained in paragraph 2.3.4 will be verified and validated (with rationale).

Note: This is linked to certification requirement in paragraph 2.3.4. These are the capabilities identified by the program that are unique to the reference mission and the system.

2.4.3 Verifying and Validating Critical System and Subsystem Performance. At CDR, the Program Manager shall document, as part of the HRCP, how the critical system and subsystem performance will be verified and validated (with rationale).

Rationale: The intent of this requirement is to have the program prove that the critical (sub)system actually performs its functions properly, which may or may not be demonstrated by requirements verification alone. Testing provides the last line of defense and opportunity to discover unexpected interactions and the ability to validate and verify models used during design. The axiom is "Test Like You Fly." The "Test Like You Fly" approach, covering nominal and off-nominal scenarios, assures the system can, in fact, accomplish the mission with the intended safety controls and robustness to mission success. It is acknowledged that testing is not possible for all types of systems and that testing is combined with analysis and other methods. Therefore, the second intent of this requirement is have the program justify the cases where a "Test Like You Fly" approach cannot or should not be used and to describe how validation is accomplished assuring sufficient coverage of the expected flight environments and operational sequences demonstrating critical (sub)system functions, performance, and margins. A detailed summarization of the

plans and procedures for performing the verification and validation with respect to the critical system and subsystem performance is sufficient to meet this requirement, provided complete references are provided to the detailed plans and procedures that document the verification and validation activities.

2.4.4 Integrated Verification and Validation of Critical Systems and Subsystems. At CDR, the Program Manager shall document, as part of the HRCP, how critical system and subsystem performance will be verified and validated at the integrated system level to ensure that (sub)system interactions will not cause a catastrophic hazard (with rationale).

Rationale: The intent of this requirement is to have the program prove that the critical (sub)systems actually perform their functions properly in an integrated environment and to demonstrate that (sub)system interactions do not cause a catastrophic hazard. Testing provides an opportunity to discover unexpected interactions and allows the program to validate and verify models used during design. The axiom is "Test Like You Fly." The "Test Like You Fly" approach, covering nominal and off-nominal scenarios, assures the system can, in fact, accomplish the mission with the intended safety controls and robustness to mission success. It is acknowledged that testing is not possible for all types of systems and that testing is combined with analysis and other methods. Therefore, the second intent of this requirement is to have the program justify the cases where a "Test Like You Fly" approach cannot or should not be used and to describe how validation is accomplished assuring sufficient coverage of the expected flight environments and operational sequences demonstrating critical (sub)system functions, performance, and margins.

2.4.5 Verifying and Validating Critical Software Performance.

2.4.5.1 At CDR, the Program Manager shall document, as part of the HRCP, how testing will be used to verify and validate the performance, security, and safety of all critical software across the entire performance envelope (or flight envelope) including mission functions, modes, and transitions (with rationale).

2.4.5.2 At CDR, the Program Manager shall also document, as part of the HRCP, how testing will be used to verify and validate the performance, security, and safety of all critical software under additional off-nominal, contingency, and stress testing (with faults injected) (with rationale).

Rationale: The intent of these requirements is to have the program fully describe the verification and validation approach that will be used, including fidelity of test environment and extent of stress testing to be performed. Critical mission software, which may include both flight and ground software, should be tested using the highest fidelity closed-loop test environment possible; for example, when a flight-equivalent avionics test bed is not used, the program needs to provide the rationale and strategy for the alternate approach.

2.4.6 System Design Verification and Validation Results. At ORR, the Program Manager shall summarize, as part of the HRCP, the results of the verification and validation performed per requirements 2.4.1 and 2.4.2, along with access to the detailed results.

2.4.7 Critical System and Subsystem Performance Verification and Validation. At ORR, the Program Manager shall summarize, as part of the HRCP, the results of the critical system and subsystem verification and validation performed per requirements 2.4.3 and 2.4.4, along with access

to the detailed results.

2.4.8 Software Verification and Validation Results. At ORR, the Program Manager shall summarize, as part of the HRCP, the results of the critical software testing performed per requirement 2.4.5, along with access to the detailed results.

2.4.9 Validating Crew Workload. At ORR, the Program Manager shall document, in the HRCP, how the crew and ground control workload was validated for the reference mission(s) and how the Program identified and implemented necessary mitigations to significant findings.

2.4.10 Updating Safety Models to Support System Validation. At the ORR, the Program Manager shall describe, in the HRCP, how the safety analysis documented in paragraph 2.2.3 related to loss of crew was 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.

Rationale: This requirement is verified by the Technical Authorities at ORR. A formally scheduled discussion with the Technical Authorities and the review board is a satisfactory method for the delivery of the information. When a program prepares for system acceptance, it is essential to examine the system in a comprehensive manner. The system capabilities need to be examined in relationship to the overall safety and mission assurance framework that is documented in the overall safety analyses defined in paragraphs 2.2.3 and 2.3.7. Only in looking at these in a collective sense can uncertainties related to uncontrolled or unidentified hazards be reduced and confidence in the results be established to the point necessary to obtain Human-Rating Certification.

Rationale: Also, while testing is the preferred approach to validate and verify the design, there will be situations where testing will not be performed. The intent here is to show where these tools and analyses are used to support validation and verification when testing is not performed.

2.5 Flight Testing the System

2.5.1 Establishing the Flight Test Program. At SDR, the Program Manager shall document, as part of the HRCP, the flight test program, including the type and number of test flights that will be performed.

Rationale: 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. The program may elect to bring forward the flight test program at an earlier milestone for concurrence.

2.5.2 At PDR, the Program Manager shall update the flight test program documented in the HRCP to include the flight test objectives with linkage to specific program requirements that are validated by flight test. (This is updated and reviewed at CDR.)

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 unmanned flight test be conducted prior to a manned flight test. It is acknowledged that this may not be feasible for all phases of flight and may not be necessary for some systems.

2.5.3 Flight Test Results. At ORR, the Program Manager shall summarize, as part of the HRCP, the results of the flight test program to date and each test objective, along with access to the detailed test results.

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.

2.6 Certifying and Operating the Human-Rated System

2.6.1 Maintaining the System and System Configuration Control. At ORR, the Program Manager shall provide, as part of the HRCP, a configuration management and maintenance plan that documents the processes that the program will use to ensure that the space system remains in the "as-certified" condition through the end of the life cycle to include system disposal.

Rationale: The plan is used to define how the human-rating for the system remains current in the face of configuration or operational changes that may require re-evaluation. The processes documented may include (but are not limited to) raw material selection criteria and control, fabrication, inspection, acceptance tests, audits, and maintenance processes.

2.6.2 Data Collection, Management, and Analysis. At ORR, the Program Manager shall provide, as part of the HRCP, a data collection, management, and analysis plan that documents the processes that the program will use to ensure that the appropriate 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.

Note: These data and processes may include (but are not limited to) time to failure of critical components, operating histories (operating times and demands), thermal and structural-related data used to verify design parameters, test data, updated environment models, repair times, acceptance tests, and maintenance processes.

2.6.3 System Certification. Prior to the first crewed flight, the Program Manager shall obtain from the NASA Administrator, as the authority for human-rating, a Human-Rating Certification for the

crewed space system based on the reference (or test) missions.

Note: The specific administrative process is detailed in Chapter 1 of this NPR. The certification request will specify the duration of the certification. See Appendix F for the request form.

2.6.4 Evaluating Changes to the System.

2.6.4.1 After Human-Rating Certification, the Program Manager, the Technical Authorities, and the Director, JSC, shall collectively evaluate design changes, manufacturing (or refurbishment) process changes, testing changes to the space system, and temporary exemptions to the failure tolerance requirement.

2.6.4.2 If the Program Manager, any of the Technical Authorities, or the Director, JSC determine that a re-rating is required, the Program Manager shall submit a request for Human-Rating Recertification, with a revised HRCP, to the NASA Administrator, as the authority for human rating.

Rationale 1: When changes to the design, manufacturing or refurbishment process, or acceptance testing are made, the Human-Rating Certification is reevaluated. In some cases, the Technical Authorities and the Director, JSC may decide that the changes do not affect the certification. In this case, the change should be documented and certified for flight at the appropriate level.

Rationale 2: Major hardware and software changes in requirements, design, major upgrades, major modifications or changes to the process, or testing that affect form, fit, performance, timing, or function, or the structural integrity and structural life of the system should be evaluated through a recertification process. Recertification is completed prior to the next flight/mission readiness review process.

2.6.5 Operating the System within the Certification. 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.

Chapter 3. Technical Requirements for Human-Rating

3.1 Overview

3.1.1 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

3.1.2 As stated previously in this NPR, these requirements are not intended to be all inclusive or an absolute prescription for human-rating. Compliance with these requirements does not assure a safe system for human missions into space. These technical requirements are intended to provide the foundation of capabilities upon which the Program Manager will build by identifying and incorporating additional unique capabilities for each reference mission (see paragraph 2.3.2). Furthermore, some of these requirements were intentionally written to force the design team to bound the problem. The design team should evaluate the intent of these technical requirements and use their talents to deliver the safest practical system that accomplishes the mission within constraints, guided (directly or indirectly) by Administrator-approved safety goals and thresholds defining long-term targeted and minimum tolerable levels of safety (maximum tolerable levels of risk). Technical requirements, along with history's lessons, legacy solutions, expert opinions, and best practices, are only as good as the implementer's understanding of their origins and assumptions.

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

3.2 System Safety Requirements

3.2.1 The space system shall provide the capability to sustain a safe, habitable environment for the crew.

> *Rationale: Protection from the hazardous environment of space or the hazardous environment at the planetary surface is fundamental to crew survival. Also, the space system should be inherently safe or designed to minimize risk (e.g., no exposed sharp edges, no exposed high temperature surfaces). This requirement includes protection from known environments such as space radiation hazards and lunar dust. Providing a habitable environment is also fundamental to the integration of the human into the space system. In order for the crew to contribute to the safe conduct of the mission, their basic habitability needs to be met. Satisfying the applicable standards listed in paragraph 2.2.5 constitutes a safe, habitable environment for the purposes of this requirement.*

3.2.2 The space system shall meet probabilistic safety criteria derived from the Agency-level safety

goals and safety thresholds with a specified degree of certainty.

Note: Probabilistic safety analysis methods provide one basis for the comparison of design options with regards to safety (see paragraph 2.3.7.1). Probabilistic safety requirements defined in accordance with paragraph 1.4.7 establish criteria for safety metrics such as loss of crew probabilities that are an outcome of such analyses. The analyses must consider the uncertainty associated with calculated values and the degree of certainty that the probabilistic criteria are met. The required degree of certainty is specified as part of the probabilistic safety requirements. Even when these metrics are determined in accordance with accepted analysis protocols, it is 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 in themselves sufficient to determine that a system is safe. Consequently, compliance with probabilistic requirements can only be an element of the case to be made that a system provides an acceptable level of safety.

3.2.3 The space system shall provide at least single failure tolerance to catastrophic events, with specific levels of failure tolerance and implementation (similar or dissimilar redundancy) derived via an integration of the design and safety analysis (per the requirement in paragraph 2.3.7.1).

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. 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 Director, JSC (for crew risk acceptance) provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.

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

Rationale: First and foremost, the failure tolerance is applied at the overall system level - to include all capabilities of the system. While failure tolerance is a term frequently used to describe minimum acceptable redundancy, it may also be used to describe two similar systems, dissimilar systems, cross-strapping, or functional interrelationships that ensure minimally acceptable system performance despite failures or additional features 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. Rationale: 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 total risk for the reference mission are below acceptable levels. Note 1:

Redundancy alone does not meet the intent of this requirement. 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: There are examples of dissimilar redundancy in current systems. For Earth reentry, the Soyuz spacecraft has a dissimilar backup ballistic entry mode to protect for loss of the primary attitude control system and a backup parachute for landing. Other examples include backup batteries for critical systems that protect for loss of the primary electrical system and the use of pressure suits during reentry to protect for loss of cabin pressure. Note 4: Ultimately, the program and Technical Authorities evaluate and agree on the failure scenarios/modes and determine the appropriate level of failure tolerance and the practicality of using dissimilar redundancy or backup systems to protect for common cause failures. Note 5: 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 Technical Authorities to control hazards associated with the physical properties of the hardware and are typically controlled via application of margin to the environments experienced by the design or system properties effected by the environment. Acceptance of these approaches by the Technical Authorities avoids processing waivers for numerous hazard causes where failure tolerance is not the appropriate approach. This includes, but is not limited to, Electro-Magnetic Interference, Ionizing Radiation, Micrometeoroid Orbital Debris, structural failure, pressure vessel failure, and aerothermal shell shape for flight.

3.2.4 The space system shall provide the failure tolerance capability in 3.2.3 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 NPR and consistent with NPR 8715.3, include crew fatality and the unplanned loss of a major element of the crewed space system during the mission that could potentially lead to death or permanent disability of the crew or passengers.

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

3.2.5 The space system shall be designed to tolerate inadvertent operator action (minimum of one inadvertent action), as identified by the human error analysis (paragraph 2.3.11), without causing a catastrophic event.

Note: An operator is defined as any human that commands or interfaces with the space system during the mission, including humans in the control centers. The appropriate level of protection (i.e., one, two or more inadvertent actions) is determined by the integrated human error and hazard analysis described in 2.3.7.1 and 2.3.11.

3.2.6 The space system shall tolerate inadvertent operator action, as described in 3.2.5, 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.

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

Note: 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.

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

Rationale: It is necessary to alert the crew to faults (not just failures) that affect critical functions. A fault is defined as an undesired system state. A failure is an actual malfunction of a hardware or software item's intended function. The definition of the term "fault"

envelopes the word "failure," since faults include other undesired events such as software anomalies and operational anomalies.

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

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

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

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

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

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

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

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

3.3 System Control Requirements - General

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

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

b. The capability would prevent a catastrophic event; or

c. The capability would prevent an abort.

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

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

Rationale: This is a specific capability necessary for the crew to control the crewed space system. While this capability should be derived by the program per paragraph 3.3.1, the critical nature of software control and automation at the highest system level dictates specific mention in the NPR. Therefore, the crew has the capability to control automated configuration changes and mode changes, including automated aborts, at the system level as long as the transition to manual control is feasible and will not cause a catastrophic event. The program and Technical Authorities will determine the appropriate implementation of this requirement - which is documented in the HRCP.

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

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

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

c. The remote capability would prevent an abort.

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

d. 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.

e. 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.

3.4 System Control Requirements - Human-Rated Spacecraft

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

Rationale: The capability for the crew to control the spacecraft's flight path is a fundamental element of crew survival. The most robust satisfaction of this requirement is provided by direct manual control of the vehicle flight path, through an independent flight control system (bypassing the affected vehicle guidance, navigation, and flight control system failures). A minimum implementation of manual control allows for the crew to bypass the automated guidance of the vehicle by interfacing directly with the flight control system to effect any possible flight path within the capability of the flight control system. Limiting the crew to choices presented by the automated guidance function is not a valid implementation of manual control.

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

Note 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 verified in a cockpit environment to ensure they are adequate to support manual control and operations.

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

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

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

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

b. The capability would prevent a catastrophic event; or

c. The capability would prevent an abort.

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

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

3.5.2 The crewed space system shall provide the capability for direct voice communication between crewed spacecraft (two or more) during proximity operations.

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

3.6 Crew Survival and Abort Requirements

3.6.1 Earth Ascent Systems

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

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

a. Complete loss of ascent thrust/propulsion.

b. Loss of attitude or flight path control. Rationale: Flying a spacecraft through the Earth's atmosphere to orbit entails inherent risk. Three crewed launch vehicles have suffered catastrophic failures during ascent or on the launch pad (one Space Shuttle and two Soyuz spacecraft). Both Soyuz crews survived the catastrophic failure due to a robust ascent abort system. Analysis, studies, and past experience all provide data supporting ascent abort as the best option for the crew to survive a catastrophic failure of the launch vehicle. Although not specifically stated, the ascent abort capability incorporates some type of vehicle monitoring to detect failures and, in some cases, impending failures.

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

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

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

3.6.1.4 Earth Ascent Abort

3.6.1.4.1 The space system shall provide the capability for the crew to initiate the Earth ascent abort sequence. Note: The ability to inhibit an automated abort initiation is described in paragraph 3.3.2.

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

3.6.1.5 If a range safety destruct system is incorporated into the design, the space system shall automatically initiate the Earth ascent abort sequence when range safety destruct commands are received onboard, with an adequate time delay prior to destruction of the launch vehicle to allow a successful abort. Rationale: Prior to destruction of the launch vehicle by means of a range safety destruct (flight termination) system, the abort system is initiated. An automated initiation of the abort sequence provides the best chance for crew survival while protecting the public from a range safety violation. It is left to the program to determine which range safety command (arm or fire) will result in the initiation of the abort sequence.

3.6.2 Earth Orbit Systems

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

Note: Where possible, the crewed space system should provide a backup capability for entry to protect for loss of the primary attitude control and guidance system. Paragraph 2.3.7.1 addresses scenarios where this may not be applicable.

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

3.6.4 Lunar Descent Systems

The crewed space system shall provide the capability to autonomously abort the lunar descent and execute all operations required for a safe return to Earth. Note: The extent of abort coverage is to be determined by the program. The goal is 100 percent coverage during the descent.

3.6.5 Lunar Surface Systems

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

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

3.6.6 Lunar Ascent Systems Reserved for a future version of the NPR.

3.6.7 Earth Reentry Systems

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

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

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

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

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

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

Appendix A. Definitions

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

Automated: Automatic (as opposed to human) control of a system or operation.

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

Breakout: During proximity operations, the ability to maneuver one or more vehicles to a safe separation distance.

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

Catastrophic Hazard: Any hazard that, when uncontrolled, results in a catastrophic event.

Common Cause Failure: Failure of multiple items or systems due to a single event or common failure mode.

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

Crew/Passenger Escape: See definition for escape.

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

Crewed Element (of the Space System): All system elements that are occupied by the crew/passengers during the space mission and provide life support functions for the crew/passengers. The crewed element includes all the subsystems that provide life support functions for the crew/passengers.

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

> The following examples are provided for clarification of the definition of crewed space system as it relates to the Human-Rating Certification:
>
> Application example 1: A launch vehicle for a crewed spacecraft on a NASA mission is part of the crewed space system for Earth ascent. In this example, the Human-Rating Certification applies to the launch vehicle and the spacecraft operating together as a crewed space system during the ascent phase of the reference mission.

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

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

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

Critical Action: A critical action is defined as any operator action that, if performed in error during operations with zero or one system failures, would result in a catastrophic event or an abort.

Critical Functions: Mission capabilities or system functions that, if lost, would result in a catastrophic event or an abort.

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.

Critical (sub)System: A (sub)system is assessed as critical if loss of overall (sub)system function, or improper performance of a (sub)system function, could result in a catastrophic event or abort.

Deviation: A documented authorization releasing a program or project from meeting a requirement before the requirement is put under configuration control at the level the requirement will be implemented. [NPD 7120.4 and NPR 7120.5]

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

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

Emergency Equipment and Systems: A set of components (hardware and/or software) used to mitigate or control hazards, after occurrence, which present an immediate threat to the crew or crewed spacecraft. Examples include fire suppression systems and extinguishers, emergency breathing devices, and crew escape systems.

Emergency Medical: The capability to respond to crew illness or injury in order to prevent, or mitigate, crew demise or permanent disability. This includes either an inherent capability on a vehicle, timely transfer to a place or vehicle that can provide a higher level of medical care, or both.

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

Exception: A written authorization granting relief from a specific, non-applicable requirement. NPR 7120.5 defines non-applicable requirement as "Any requirement not relevant; not capable of being applied." The term exception is generally no longer used. For the purposes of this NPR, the term "exception" is equivalent to and interchangeable with a "Determination of nonapplicability" as described in NPR 8715.3.

Exemption: A written authorization granting relief from the space system failure tolerance requirement.

Failure: Inability of a system, subsystem, component, or part to perform its required function within specified limits (Source - NPR 8715.3).

Failure Tolerance: The ability to sustain a certain number of failures and still retain capability.

Fault: An undesired system state and/or the immediate cause of failure (e.g., maladjustment, misalignment, defect, or other). The definition of the term "fault" envelopes the word "failure," since faults include other undesired events such as software anomalies and operational anomalies (Source - MIL-STD-721C). Faults at a lower level could lead to failures at the higher subsystem or system level.

Hazard: A state or a set of conditions, internal or external to a system, which has the potential to cause harm (Source - NPR 8715.3).

Hazard Analysis: The process of identifying hazards and their potential causal factors.

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

Human Health Management and Care: The set of activities, procedures, and systems that provide (1) environmental monitoring and human health assessment; (2) health maintenance and countermeasures; and (3) medical intervention for the diagnosis and treatment of injury and illness.

Human Performance: The physical and mental activity required of the crew and other participants to accomplish mission goals. This includes the interaction with equipment, computers, procedures, training material, the environment, and other humans.

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

1. Human-rating is the process of evaluating and assuring that the total system can safely conduct the required human missions.
2. Human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success.
3. Human-rating includes the incorporation of design features and capabilities to enable safe

recovery of the crew from hazardous situations.

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

Human-Rating Certification Package: See Appendix D.

Human-Rating Process: The process steps used to achieve a human-rated space system. These steps include human safety risk identification, reduction, control, visibility, and program management acceptance criteria. Acceptable methods to assess the risk to human safety include qualitative and/or quantitative methods such as hazards analysis, fault tree analysis, human error analysis, probabilistic risk assessment, and failure modes and effects analysis.

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

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

Life Cycle: The totality of a program or project extending from formulation through implementation encompassing the elements of design, development, verification, production, operation, maintenance, support and disposal.

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

Mission Abort: Same as "Abort." The forced early return of the crew to Earth when failures or hazards prevent continuation of the mission profile and a return to Earth is required to prevent a catastrophic event. The crew is safely returned to Earth in the space system nominally used for entry and landing/touchdown.

NASA Human Spaceflight Missions: Terminology used to distinguish human spaceflight missions that require human-rated systems per this NPR. Any human spaceflight mission where NASA retains the mission decision authority and the responsibility for crew safety is considered a NASA mission.

Operator: Any human interacting with the crewed space system during the mission.

Override: To take precedence over system control functions.

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."

Permanent Disability: A non-fatal occupational injury or illness resulting in permanent impairment through loss of, or compromised use of, a critical part of the body, to include major limbs (e.g., arm, leg), critical sensory organs (e.g., eye), critical life-supporting organs (e.g., heart, lungs, brain), and/or body parts controlling major motor functions (e.g., spine, neck). Therefore, permanent disability includes a non-fatal injury or occupational illness that permanently incapacitates a person to the extent that he or she cannot be rehabilitated to achieve gainful employment in their trained occupation and results in a medical discharge from duties or civilian equivalent.

Probabilistic Safety Requirement: The specification of a criterion for a probabilistic safety metric (e.g., the probability of a loss of crew) and the degree of certainty with which such criteria must be met.

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

Public: All humans not participating in the spaceflight activity who could be potentially affected by the function or malfunction of the space system.

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.

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.

Risk Ranking: The ordering of risk contributors such as accident scenarios or classes of accident scenarios based on the extent of their contribution (accounting for hazard controls, crew survival capabilities, and other risk reduction measures) such that the significant contributors can be identified.

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

Safety: 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.

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

Safety Threshold: The minimum tolerable level of safety for a given reference mission, specified at the system level in terms of an aggregate measure of risk to the crew such as the probability of a loss of crew.

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

Subsystem: A secondary or subordinate system within a system (such as the crewed space system) that performs a specific function or functions. Examples include electrical power, guidance and navigation, attitude control, telemetry, thermal control, propulsion, structures subsystems. A subsystem may consist of several components (hardware and software) and may include

interconnection items such as cables or tubing and the support structure to which they are mounted.

Technical Authority: The individuals who provide independent oversight of programs and projects in support of safety and mission success, who have formally delegated authority traceable to the Administrator, and are funded independent of Programmatic Authority. (Source: paraphrased from NPD 1000.0)

Test Flight: A flight or mission dedicated primarily to test objectives. Flight tests can include scaled test articles, uncrewed flights, and crewed flights.

Usability Testing: Evaluation by people using the system (hardware or software) in a realistic situation to determine how well it can be used for its intended purpose (e.g., how well people can manipulate parts or controls, receive feedback, and interpret feedback) to identify potential human errors and areas for design improvement.

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 specifications. May be determined by 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 documented authorization releasing a program or project from meeting a requirement after the requirement is put under configuration control at the level the requirement will be implemented (source NPD 7120.4), where a certain level of risk has been documented and accepted.

Appendix B. Acronyms

CDR	Critical Design Review
EVA	Extravehicular Activity
FAA	Federal Aviation Administration
HEA	Human-Error Analysis
HQR	Handling Qualities Rating
HRCP	Human-Rating Certification Package
ISS	International Space Station
JSC	Johnson Space Center
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
ORR	Operational Readiness Review
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
SDR	System Definition Review
SIR	System Integration Review
SRR	Systems Requirements Review

Appendix C. References

C.1 NPD 8900.5, NASA Health and Medical Policy for Human Space Exploration.

C.2 NPR 1400.1, NASA Directives System Procedural Requirements.

C.3 NPR 7120.5D, NASA Space Flight Program and Project Management Requirements.

C.4 NPR 7120.10, Technical Standards Products for NASA Programs and Projects.

C.5 NPR 7123.1, Systems Engineering Processes and Requirements.

C.6 NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects.

C.7 NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.

C.8 NPR 8715.3, NASA General Safety Program Requirements.

C.9 NPR 8900.1, Health and Medical Requirements for Human Space Exploration.

C.10 NASA-STD-5005, Standard for The Design and Fabrication of Ground Support Equipment.

C.11 NASA/SP-2007-6105 Rev 2, NASA Systems Engineering Handbook, 2007.

C.12 NASA/SP-2011-3421, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, 2011.

C.13 NASA/SP-2015-3709, Human Systems Integration (HSI) Practitioner's Guide, 2015.

C.14 "System Safety Requirements for Manned Space Flight," NASA Manned Flight Safety Office, January 1969.

C.15 "A Review of Man Rating in Past and Current Manned Space Flight Programs," Eagle Engineering/LEMSCO, 88-193, A. Bond, 1988.

C.16 "Guidelines for Man-Rating Space Systems," JSC 23211, M. Cerimele et al., 1991.

C.17 "A Perspective on the Human Rating Process of Spacecraft: Both Past and Present," NASA Special Publication 6104, G. Zupp et al., 1995.

C.18 "Human-Rating Requirements," JSC 28354, J. Van Laak et al., 1998.

C.19 "OSP-ELV Human Flight Safety Certification Study Report," MSFC, J. Bullman et al., March 2004.

C.20 MIL-STD-721C, Definition of Terms for Reliability and Maintainability.

C.21 MIL-STD-1472, Department of Defense Design Criteria Standard - Human Engineering.

Appendix D. Human-Rating Certification Package

D.1 The form of the HRCP is a compilation of pertinent plans and documents, plus presentation material to help guide reviewers through the package. The HRCP is not intended to duplicate/repackage existing program documentation but rather provides a summarization of information the details of which can be found in referenced documents or other data sources and justification/explanation/augmentation for information that isn't available in other documentation). The HRCP must be maintained under configuration management (especially to referenced/linked material) to clearly track changes made between milestones.

D.2 Refer to the referenced paragraphs for the detailed requirement text and delivery milestones. The material provided prior to and during each milestone review will be considered draft and for review and comment. An update will be provided after all changes resulting from the review have been incorporated. The post-review HRCP will be maintained in a location and in a manner that supports review by designated Technical Authorities and JSC Center Director representatives and designated review panel members.

D.3 The final HRCP submitted for approval and granting of a Human-Rating Certification will be provided in a manner as prescribed by the Program Management Council.

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

	Requirement	HRCP Content	SRR	SDR	PDR	CDR	ORR
	2.2 Process and Standards						
1	2.2.2	A summary of all requests for waivers, deviations, and exceptions to the certification and technical requirements in this NPR, as well as any exemptions to the failure tolerance requirement, and how to access these.	I	U	U	U	U
2	2.2.3	A description of a process for identifying hazards, understanding risk implications of the hazards, modeling hazard scenarios, quantifying and ranking risks to crew safety, and mitigating risks and deficiencies.	X				
3	2.2.4	A summary of the safety and mission assurance program established in accordance with NPR 8715.3.	I	U	U	U	U
4	2.2.6	A list of program-level standards mandated by the Technical Authorities as relevant to human-rating with a status of Technical Authorities approval.	X				

5	2.2.7	A summary of the exceptions, deviations, and waivers to the applicable standards listed in paragraphs 2.2.5 and 2.2.6, and access to the program documentation that contains the exceptions, deviations, and waivers.	I	U	U	U	U
	Designing the System						
6	2.3.1	A description of the crewed space system, its functional interfaces to other systems, and the reference missions that will be certified for human-rating.	X				
7	2.3.2	A description of the crew survival strategy for all phases of the reference missions and the system capabilities required to execute the strategy.		I	U	U	U
8	2.3.3	A description of the design philosophy which will be followed to develop a system that utilizes the crew's capabilities to execute the reference missions, prevent aborts, and prevent catastrophic events.	X				
9	2.3.4	A description of the implementation of the survival capabilities and clear traceability to the highest level program documentation.		I	U	U	
10	2.3.5	A description of the implementation of the applicable requirements of Chapter 3 of this NPR and clear traceability to the highest level program documentation.	I	U	U	U	
11	2.3.6	A description of probabilistic safety requirements derived from the Agency-level safety goals and safety thresholds, including any allocations to mission phases and system elements.	I		U	U	
12	2.3.7.2	A summary of the current understanding of risks and uncertainties and related decisions regarding the system design and application of testing, based on the results of the design and safety analyses performed in accordance with paragraph 2.3.7.1.		I	U	U	U

13	2.3.9	A description of how the crew and ground control workload for the reference mission(s) will be evaluated.	I		U	U	
14	2.3.10.2	A summary of how the human-in-the-loop usability evaluations for human-system interfaces and integrated human-system performance evaluation results (to date) were used to influence the system design.			I	U	
15	2.3.10.3	A summary of how the integrated human-system performance test results were used to validate the system design and provide access to the detailed test plans and results.					X
16	2.3.11.2	A summary of how the human error analysis (to date) was used to: a. Understand and manage potential catastrophic hazards which could be caused by human errors b. Understand the relative risks and uncertainties within the system design c. Influence decisions related to the system design, operational use, and application of testing			I	U	U
	Verifying and Validating the System Capabilities and Performance						
17	2.4.1	A description of how the implementation of the technical requirements in Chapter 3 will be verified and validated (with rationale).	I	U	U	U	
18	2.4.2	A description of how the implementation of survival capabilities will be verified and validated (with rationale).				X	
19	2.4.3	A description of how the critical system and subsystem performance will be verified and validated (with rationale).				X	
20	2.4.4	A description of how critical system and subsystem performance will be verified and validated at the integrated system level to ensure that (sub)system interactions will not cause a catastrophic hazard (with rationale).				X	

21	2.4.5.1	A description of how testing will be used to verify and validate the performance, security, and safety of all critical software across the entire performance envelope (or flight envelope) including mission functions, modes, and transitions (with rationale).				X	
22	2.4.5.2	A description of how testing will be used to verify and validate the performance, security, and safety of all critical software under additional off-nominal, contingency, and stress testing (with faults injected) (with rationale).				X	
23	2.4.6	A summary of the results of the critical system and subsystem verification and validation performed per requirements 2.4.1 and 2.4.2, along with access to the detailed results.					X
24	2.4.7	A summary of the results of the critical system and subsystem verification and validation performed per requirements 2.4.3 and 2.4.4, along with access to the detailed results.					X
25	2.4.8	A summary of the results of the critical software testing performed per requirement 2.4.5, along with access to the detailed results.					X
26	2.4.9	A description of how the crew and ground control workload was validated for the reference mission(s), and how the Program identified and implemented necessary mitigations to significant findings.					X
27	2.4.10	A description of how the safety analysis documented in paragraph 2.2.3 related to loss of crew was 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						

28	2.5.1	A description of the flight test program, including the type and number of test flights that will be performed.		X			
29	2.5.2	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.			U	U	
30	2.5.3	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						
31	2.6.1	A configuration management and maintenance plan that documents the processes that the program will use to ensure that the space system remains in the "as-certified" condition through the end of the life cycle to include system disposal.					X
32	2.6.2	A data collection, management, and analysis plan that documents the processes that the program will use to ensure that the appropriate 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

Appendix E. Human-Rating Certification Package Endorsements

HUMAN-RATING CERTIFICATION PACKAGE ENDORSEMENT

Name of Program:

Scope of Certification (Systems and Reference Missions Addressed in the Human-Rating Certification Package):

Check here if Additional Scope Information is attached ☐

The Human-Rating Certification Package for ☐ SRR ☐ SDR ☐ PDR ☐ CDR ☐ ORR milestone (or equivalent) is complete and is provided for your approval.

Program Manager:_____ Date _____

Within the scope of my Authority, I concur with this Human-Rating Certification Package and indicate:

1. For the identified Milestone and pending satisfactory completion of open items identified at the ☐ SRR ☐ SDR ☐ PDR ☐ CDR ☐ ORR, the Human-Rating Certification Package is satisfactory and represents acceptable progress toward formal Human-Rating Certification in conjunction with flight readiness determination.
2. All Human-Rating Certification Package-related items identified at the previous Milestone have been satisfactorily resolved and documented.
3. All waivers and exceptions to human-rating certification requirements or technical requirements for human-rated systems have been reviewed and satisfactorily dispositioned.

Required Signatures	Signature	Date	Reservations (Y/N)
Associate Administrator, Mission Directorate			
Director, Johnson Space Center (Consent for Crew Risk)			
Chief, Safety and Mission Assurance (Technical Authority)			
Chief Engineer (Technical Authority)			
Chief Health and Medical Officer (Technical Authority)			

I endorse that this Human-Rating Certification Package represents acceptable progress toward formal Human-Rating Certification in conjunction with flight readiness determination.

Associate Administrator (at PDR) or
Associate Administrator, Mission Directorate

Appendix F. Human-Rating Certification

Human-Rating Certification

Program Name:

Scope of Certification (Systems and Reference Missions Covered in this Human-Rating Certification):

Check here if Additional Scope Information is attached ☐

Duration of Certification:

In accordance with NPR 8705.2C, the Program identified above has satisfactorily completed the Human-Rating Certification activities and has satisfied the technical requirements for human-rated systems, except as noted within the approved waivers and exceptions contained within the Human-Rating Certification Package. I request that the Program identified above be granted Human-Rating Certification within the scope described.

_____ _____
Program Manager Date

PROGRAM CONCURRENCE

I endorse and concur with the request to grant the Human-Rating Certification within the scope described.

_____ _____
Associate Administrator, Mission Directorate Date

TECHNICAL AND RISK CONCURRENCE

Within the scope of my authority, I concur with this request to grant the Human-Rating Certification within the scope described.

_____ _____
Director, Johnson Space Center (Consent for Crew Risk) Date

_____ _____
Chief, Safety and Mission Assurance (Technical Authority) Date

_____ _____
Chief Engineer (Technical Authority) Date

_____ _____
Chief Health and Medical Officer (Technical Authority) Date

ENDORSEMENT

I endorse the request to grant the Human-Rating Certification within the scope described.

_____ _____
Associate Administrator Date

CERTIFICATION

I certify the Program to be human-rated within the scope described.

_____ _____
Administrator Date