

[| NODIS Library](#) | [Program Management\(8000s\)](#) | [Search](#) |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY**NPR 8705.2B**

Effective Date: May 06, 2008

Expiration Date: July 06,
2016[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Human-Rating Requirements for Space Systems (w/change 4 dated 8/21/2012)

Responsible Office: Office of Safety and Mission Assurance[| TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixF](#) | [AppendixE](#) | [ALL](#) |

Chapter 2 Human-Rating Certification Requirements

2.1 Overview

2.1.1 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. 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 ([Requirement 58373](#)).

Rationale: 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.

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 and Exceptions. The Program Manager shall summarize, in the HRCP, all requests for waivers and exceptions to the certification and technical requirements in this NPR and provide access to the program documentation that contains the waivers and exceptions ([Requirement 58376](#)).

Rationale: Requests for exceptions and waivers are submitted in accordance with the requirements contained within NPR 1400.1, NASA Directives and Charters Procedural Requirements, and NPR 8715.3, NASA General Safety Program Requirements. The Safety and Mission Assurance Technical Authority dispositions requests for waivers and exceptions to the requirements of this NPR. The HRCP documents all requests for exceptions 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 and

waivers and support documentation within the HRCP. Individual waivers and exceptions to the applicable standards are not to be included in the HRCP.

2.2.3 Safety Analysis Processes. Prior to SRR, the Program Manager shall document, 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 or deficiencies as appropriate ([Requirement 58378](#)).

Rationale: 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 paragraph 2.3.6.1 of NPR 8715.3, NASA General Safety Program Requirements) 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/or 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 is also essential. 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), 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. 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. 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 paragraph 2.5.1 of NPR 8715.3, NASA General Safety Program Requirements. 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. 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 paragraph 1.5.2 of NPR 8715.3, NASA General Safety Program Requirements. (This is updated at SDR, PDR, CDR, ORR.) ([Requirement 58380](#)).

Rationale: 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. 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.

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.
- d. MIL-STD-1472, Department of Defense Design Criteria Standard - Human Engineering ([Requirement 58389](#)).

Rationale: 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, adjustments (changes that still meet the intent of the requirement or exceed the requirement), and waivers to the applicable standards require the approval of the Technical Authorities (see paragraph 2.2.2, Human-Rating Waivers 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 NASA Policy Directive (NPD) 8070.6, Technical Standards.

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 ([Requirement 58390](#)).

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 8070.6, Technical Standards.

2.2.7 Summarizing Exceptions, Adjustments, and Waivers to Applicable Standards. At SRR, the Program Manager shall summarize, in the HRCP, the exceptions, adjustments, and waivers to the applicable standards listed in paragraph 2.2.5 and provide access to the program documentation that contains the exceptions, adjustments, and waivers. (This is updated at SDR, PDR, CDR, and ORR.) ([Requirement 58392](#)).

Rationale: The intent of this requirement is to have the program collectively evaluate the impact of the waivers and exceptions to the applicable standards. It will be left to the program and the Technical Authorities to determine which waivers and exceptions are significant enough to be included in the summary.

2.2.8 Summarizing Waivers and Exceptions to other Standards Mandated by the Technical Authorities. At SRR, the Program Manager shall summarize, in the HRCP, the waivers and exceptions to the standards from the requirement in paragraph 2.2.6 that are significant to human-rating and provide access to the program documentation that contains the waivers and exceptions. (This is updated at SDR, PDR, CDR, and ORR.) ([Requirement 58394](#)).

Rationale: The intent of this requirement is to have the program collectively evaluate the impact to human-rating of the waivers 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 and exceptions are significant and relevant to human-rating. The individual waivers and exceptions are not documented in the HRCP, but the program provides the location of and access to the actual waivers 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 ([Requirement 58397](#)).

Rationale: This may be accomplished using reference missions (for spacecraft) or the equivalent (for surface habitats and mobility systems). 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.) ([Requirement 58399](#)).

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 ([Requirement 58401](#)).

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.

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.) (Requirement 58403).

Rationale: 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.) (Requirement 58405).

Rationale: 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) (Requirement).

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: 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. As noted in the rationale for 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 and simulation modeling techniques (e.g., physics-based abort effectiveness and trigger analyses). 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. 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. 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 flight 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 (Requirement).

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 (Requirement 58413).

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. 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 (Requirement).

Rationale: 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 (Requirement). *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, as appropriate, to identify significant risk contributors and 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 HRCF, 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).

Rationale: Rationale: 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 present 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/or 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. 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/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, NASA General Safety Program Requirements, and NPR 8705.5, Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects. 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/challenge design options is of greater significance than a final number that results from the analysis. 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 also expected. This information can be documented as a part of the safety analysis report described in paragraph 2.8.2 of NPR 8715.3 "NASA General Safety Program Requirements."

2.3.8 Human-System Integration Team. No later than SRR, the Program Manager shall establish a human-system integration team, consisting of astronauts, mission operations personnel, training personnel, ground processing personnel, human factors personnel, and human engineering experts, with clearly defined authority, responsibility, and accountability to lead the human-system integration (hardware and software) for the crewed space system (Requirement 58419).

Rationale: Past experience with cockpit development in spacecraft and military aircraft has shown that when a correctly staffed human-system integration team is given the authority, responsibility, and accountability for cockpit design and human integration, the best possible system is achieved within the schedule and budget constraints. This team focuses on all human system interfaces (crew, launch control, and ground processing) that can cause a catastrophic failure.

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

(Requirement 58421).

Rationale: The design of the system can have a significant impact on crew workload and productivity. Integration of the human into the system is a fundamental tenet of human-rating. Understanding how the system design affects crew 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 crew workload would be tasked to the human-systems integration team. Evaluation of the crew 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 human performance (Requirement 58423).

2.3.10.2 At PDR and CDR, the Program Manager shall summarize, in the HRCP, and present how the 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 (Requirement 58424).

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 (Requirement 58425).

Rationale: The expectation is that this testing would be conducted by the human-systems integration team. While not specifically stated in the requirements, conducting usability and human-system performance testing requires the establishment of test criteria. The intent of this requirement is to have the program progressively demonstrate that the operational concept meets system requirements for operational safety, efficiency, and user interface design. Test data is used to validate the integrated performance of the space system hardware, software, and human operators in simulated vehicle and mission operations environments. Test and/or analysis is the standard to demonstrate that the operational concept meets requirements. Where analysis is not available, testing consists of quantitative and objective human-in-the-loop simulations of flight-critical system, 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. A formally scheduled discussion as part of the review milestone with the Technical Authorities and the review board is necessary to satisfy the present aspect of this requirement.

2.3.11 Human Error Analysis. The Program Manager shall conduct a human error analysis for all mission phases to include operations planned for response to system failures (Requirement 58430).

2.3.11.1 At PDR, CDR, and ORR, the Program Manager shall summarize, in the HRCP, and present how the human error analysis (to date) was used to:

- a. Understand and manage potential catastrophic hazards which could be caused by human errors (Requirement 58432).
- b. Understand the relative risks and uncertainties within the system design (Requirement 48433).
- c. Influence decisions related to the system design, operational use, and application of testing (Requirement 58434).

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. The human error analysis includes all mission operations within the space system - including operations in the control centers. The intent of this human error analysis requirement is to have the program: 1) Identify inadvertent operator actions 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). The scope of this human error analysis covers response to system failures and abort scenarios. A formally scheduled discussion as part of the review milestone with the Technical Authorities and the review board is necessary to satisfy the present aspect of this requirement.

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 (Requirement 58444).

2.4 Verifying and Validating the System Capabilities and Performance

2.4.1 Verifying and Validating Implementation of the Technical Requirements. At SRR, SDR, PDR, and CDR, 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) ([Requirement 58446](#)).

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) ([Requirement 58448](#)).

Rationale: 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) ([Requirement 58450](#)).

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) ([Requirement 58452](#)).

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) ([Requirement 58455](#)).

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) ([Requirement 58456](#)).

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 ([Requirement 58458](#)).

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 ([Requirement 58459](#)).

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 ([Requirement 58460](#)).

2.4.9 Validating Crew Workload. At ORR, the Program Manager shall document, in the HRCP, how the crew workload was validated and determined acceptable for the reference mission(s) ([Requirement 58461](#)).

2.4.10 Updating Safety Models to Support System Validation. At the ORR, the Program Manager shall describe how the safety analysis documented in paragraph 2.2.3 related to loss of crew was updated based on the results of validation/verification testing and used to support validation/verification of the design in circumstances where testing was not accomplished ([Requirement 58462](#)).

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. 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 ([Requirement 58466](#)).

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.) ([Requirement 58468](#)).

Rationale: 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. 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. 3) In order to minimize risk to the flight test 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 ([Requirement 58473](#)).

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.

2.5.4 Crewed Test Flights. The Program Manager shall obtain an interim Human-Rating Certification prior to crewed test flights per paragraph 2.6.3 ([Requirement 58473](#)).

Rationale: While past experience has shown that every space mission should be treated like a 'test flight,' this requirement deals with early crewed missions that are specifically identified as test flights. For these missions, the program may have a Test Readiness Review vice a Flight or Mission Readiness Review. For the purpose of the interim Human-Rating Certification, these may be considered equivalent reviews. The contents of the HRCP, while incomplete, are reviewed prior to approving the test flight. The Reference Mission for the interim certification reflects the flight test profile (as indicated in the test plan) rather than the nominal Reference Mission.

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 ([Requirement 58478](#)).

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 ([Requirement 58480](#)).

Rationale: 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 ([Requirement 58483](#)).

Rationale: 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, along with the Technical Authorities, and the Director, JSC, shall collectively evaluate design changes, manufacturing (or refurbishment) process changes, and testing changes to the space system.

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 ([Requirement 58486](#)).

Rationale: 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. Major hardware/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 ([Requirement 58490](#)).
- b. Verification that the human-rated system will be operated within the certified envelope of the reference mission(s) ([Requirement 48491](#)).
- c. Anomalies from the previous flight/mission that affect the Human-Rating Certification and their resolution ([Requirement 58492](#)).
- 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 (Requirement).

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.

| [TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [AppendixA](#) |
[AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixF](#) | [AppendixE](#) | [ALL](#) |

| [NODIS Library](#) | [Program Management\(8000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
