



NASA Procedural Requirements

NPR 8705.2A
Effective Date: February 07,
2005
Expiration Date: February 07,
2010

COMPLIANCE IS MANDATORY

Human-Rating Requirements for Space Systems

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents
- P.5 Cancellation

Concurrences

Chapter 1. Institutional and Programmatic Requirements

- 1.1 Roles and Responsibilities
- 1.2 Overview of the Human-Rating Certification Process
- 1.3 General Requirements
- 1.4 Human-Rating Independent Review Team
 - 1.4.1 Human-Rating Independent Review Team Purpose
 - 1.4.2 Human-Rating Independent Review Team Membership
 - 1.4.3 Human-Rating Independent Review Team Membership Concurrences
- 1.5 Human-Rating Plan
 - 1.5.1 Human-Rating Plan Development
 - 1.5.2 Human-Rating Plan Content
 - 1.5.3 Tailoring and Exceptions to Human-Rating Requirements Documented in Plan
 - 1.5.4 Tailoring Process and Approvals
 - 1.5.5 Exceptions Process and Approvals
 - 1.5.6 Human-Rating Plan - Preliminary Review
 - 1.5.7 Human-Rating Plan - Final Review
 - 1.5.8 Human-Rating Plan Approval and Concurrences
 - 1.5.9 Human-Rating Requirements Plan Compliance
 - 1.5.10 Deviation Process and Approval

- 1.5.11 Waiver Process and Approval
- 1.6 Programmatic Requirements
 - 1.6.1 Critical Functions
 - 1.6.2 Cumulative Risk Goals
 - 1.6.3 System Safety and Mission Assurance
 - 1.6.4 Human Factors Engineering
 - 1.6.5 General Testing and Verification
 - 1.6.6 Human-In-The-Loop Testing
 - 1.6.7 Software Testing
 - 1.6.8 Flight Testing
- 1.7 Human-Rating Certification
 - 1.7.1 Human-Rating Certification Request
 - 1.7.2 Human-Rating Certification Recommendation
 - 1.7.3 Human-Rating Certification
 - 1.7.4 Human-Rating Certification Concurrences
 - 1.7.5 Sustaining Human-Rating Certification
 - 1.7.6 Suspension of Human-Rating Certification
 - 1.7.7 Human-Rating Certification Reinstatement

Chapter 2. Standards

Chapter 3. System Design Requirements

- 3.1 Two-Failure Tolerance
- 3.2 Human-System Interactions (Crew)
- 3.3 Human-System Interactions (Ground Control)
- 3.4 Crew Workload
- 3.5 Fault Detection, Isolation, and Recovery
- 3.6 Health and Status Data
- 3.7 Autonomous Operation
- 3.8 Crew and Passenger Survival for Generic System
- 3.9 Crew and Passenger Survival
- 3.10 Flight Control Systems
- 3.11 Proximity Operations
- 3.12 Flight Termination

APPENDICES

Appendix A. Additional Related References

Appendix B. Definitions

Appendix C. History and Rationale

Preface

P.1 Purpose

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. NASA will fulfill all requirements of this NPR (NPR 8705.2) for all space systems involving humans or interfacing with human space systems prior to becoming operational and throughout the system's use. A program is eligible for human-rating certification only if it meets engineering requirements, health requirements, and safety requirements contained in this NPR (NPR 8705.2). Human-rating certification provides the maximum reasonable assurance that a failure will not result in a crew or passenger fatality or permanent disability.

P.2 Applicability

- a. The requirements in this NPR (NPR 8705.2) shall apply to all space systems (hardware and software), developed and/or operated by or for NASA, that support human activity in space and that interact with crewed NASA human-rated space systems. This includes, but is not limited to, space systems, space suits, planetary bases, planetary rovers, and surface vehicles (Requirement 34241).

Note: If an expendable launch vehicle is used as part of a system that carries humans, then NPR 8705.2 applies to the system, including the expendable launch vehicle portion. Ground support subsystems such as the launch facility and mission control are included as part of the total system when the system is being human-rated.

- b. The Agency Program Management Committee shall determine the applicability of the requirements in this NPR (NPR 8705.2) to programs in existence (e.g., Space Shuttle and International Space Station) and to major modifications of those programs in the future (Requirement 34243).
- c. The requirements in this NPR (NPR 8705.2) shall apply to internationally provided space systems as documented in distinct separate agreements, such as joint or multilateral agreements (Requirement 34244).
- d. The requirements in this NPR (NPR 8705.2) shall be made applicable to contractors only through contract clauses, specifications, or statements of work in conformance with the NASA Federal Acquisition Regulation (FAR) supplement and not as direct instructions to contractors (Requirement 34245).
- e. The requirements in this NPR (NPR 8705.2) shall supersede any conflicting requirements imposed by other NASA procedural requirements and standards (Requirement 34246).
- f. The requirements in this NPR (NPR 8705.2) shall supplement more stringent requirements imposed by other Federal Government agencies (Requirement 34247).
- g. In this NPR (NPR 8705.2), a requirement is identified by "shall" and descriptive material by

"is."

P.3 Authority

- a. 42 U.S.C. 2473 (c)(1), Section 203 (c)(1) of the National Aeronautics and Space Act of 1958, as amended.
- b. NPD 7120.4, Program/Project Management.
- c. NPD 8700.1, NASA Policy for Safety and Mission Success.

P.4 Applicable Documents

- a. NASA Standard 3000 Volume I - II, Man-Systems Integration Standards.
- b. NASA Standard 5001, Structural Design and Test Factors of Safety for Spaceflight Hardware.
- c. NASA Standard 5007, General Fracture Control Requirements for Manned Spaceflight Systems.
- d. NASA-STD-8719.13, Software Safety Standard.
- e. JPG 8080.5, JSC Design and Procedural Standards Manual.
- f. JSC 26882, NASA Space Flight Health Requirements.
- g. MIL-STD-1472, Department of Defense Design Criteria Standard - Human Engineering.
- h. Additional related reference documents are listed in Appendix A.

P.5 Cancellation

NPR 8705.2, dated June 19, 2003.

/S/

Bryan O'Connor
Chief Safety and Mission Assurance Officer

Concurrences:

/S/

Dr. Richard S. Williams
Chief Health and Medical Officer

/S/

William F. Readdy
Associate Administrator for
Space Operations

/S/

Craig E. Steidle
Associate Administrator for Exploration Systems

/S/

Rex Geveden

Chief Engineer

Chapter 1. Institutional and Programmatic Requirements

1.1 Roles and Responsibilities

Figure 1 provides a summary of roles and responsibilities for human-rating certification.

Figure 1. Summary of Roles and Responsibilities

(Note: Chief Health and Medical Officer serves as the Independent Technical Authority for all health and medical technical requirements, standards, and matters.)

Due Date When Using Sole Source Acquisition Approach Where Procurement is At or Shortly After Acquisition Strategy Meeting	Due Date When Using Phased Acquisition Approach Where Procurement is After SRR	Key: P = Primary Responsibility C = Concur R = Review SRR = System Requirements Review PDR = Preliminary Design Review CDR = Critical Design Review FRR = Flight Readiness Review Tasks	Chief Safety and Mission Assurance Officer	Chief Engineer (Independent Technical Authority)	Chief Health and Medical Officer (Independent Technical Authority)	Associate Administrator for Exploration Systems	Associate Administrator for Space Operations	Program Manager	Human-Rating Independent Review Team
		Provide leadership, policy direction, assessment, and coordination of the technical requirements and process compliance verification for NPR 8705.2	P						
		Provide executive level functions for the Human-Rating Process	R	R	R	R	R		
Human Rating Independent Review Team Charter									
		Charter (Select membership and tasks) for the Human-Rating Independent Review Team	C	C	C	P	P		
		Co-Chair the Human-Rating Independent Review Team				P	P		
Human-Rating Plan Volume I									
		Develop Volume I: Human-Rating Plan						P	
30 workdays before Acquisition Strategy Meeting	60 workdays before SRR	Request ITA approve Tailoring and Exceptions						P	
15 workdays before Acquisition Strategy Meeting	45 workdays before SRR	Approve Tailoring and Exceptions		P	P				
45 workdays before SRR	45 workdays before SRR	Provide Volume I: Human-Rating Plan to the Human-Rating Independent Review Team for Preliminary Review						P	
30 workdays before SRR	30 workdays before SRR	Conduct Preliminary Review of Volume I: Human-Rating Plan and Provide Evaluation to Program							P
15 workdays before SRR	15 workdays before SRR	Provide Volume I: Human-Rating Plan to the Human-Rating Independent Review Team for Final Review						P	
Complete 5 workdays before SRR	Complete 5 workdays before SRR	Conduct Final Review of Volume I: Human-Rating Plan and Provide Evaluation to Human-Rating Board							P
Before SRR	Before SRR	Approve Volume I: Human-Rating Plan	C	P	P	P	P		
Human-Rating Plan Volume II									
		Develop Volume II: Human-Rating Plan						P	
45 workdays before PDR	45 workdays before PDR	Provide Volume II: Human-Rating Plan to the Human-Rating Independent Review Team for Preliminary Review						P	
30 workdays prior to PDR	30 workdays prior to PDR	Conduct Preliminary Review of Volume II: Human-Rating Plan and Provide Evaluation to Program							P
15 workdays before PDR	15 workdays before PDR	Provide Volume II: Human-Rating Plan to the Human-Rating Independent Review Team for Final Review						P	
5 workdays before PDR	5 workdays before PDR	Conduct Final Review of Volume II: Human-Rating Plan and Provide Evaluation to Human-Rating Board							P
Before PDR	Before PDR	Approve Volume II: Human-Rating Plan	C	P	P	P	P		
Human-Rating Plan Volume III									
		Develop Volume III: Human-Rating Plan						P	
45 workdays before CDR	45 workdays before CDR	Provide Volume III: Human-Rating Plan to the Human-Rating Independent Review Team for Preliminary Review						P	
30 workdays prior to CDR	30 workdays prior to CDR	Conduct Preliminary Review of Volume III: Human-Rating Plan and Provide Evaluation to Program							P
15 workdays before CDR	15 workdays before CDR	Provide Volume III: Human-Rating Plan to the Human-Rating Independent Review Team for Final Review						P	
5 workdays before CDR	5 workdays before CDR	Conduct Final Review of Volume III: Human-Rating Plan and Provide Evaluation to Human-Rating Board							P
Before CDR	Before CDR	Approve Volume III: Human-Rating Plan	C	P	P	P	P		
Plan Implementation									

Upon Approval	Upon Approval	Implement Human-Rating Plan							P	
		Approve Waivers and Deviations to the Requirements in the Approved Human-Rating Plan		P	P					
Obtaining Human-Rating Certification										
		Request Human-Rating Certification							P	
Prior to Human-Rating Certification Decision	Prior to Human-Rating Certification Decision	Review Program Documentation and Provide Recommendation Concerning Human-Rating Certification to Human-Rating Board								P
Prior to FRR	Prior to FRR	Approve/Disapprove Human-Rating Certification	C	C	C	C	P			
Continued Certification										
Upon Certification	Upon Certification	Sustain Human-Rating Certification							P	
		Suspend Human-Rating Certification					P			
		Reinstate Human-Rating Certification	C	C	C	C	P			

1.2 Overview of the Human-Rating Certification Process

1.2.1 The objective of the human-rating certification process is to document that the critical engineering requirements, health requirements, and safety requirements have been met for a space system that provides maximum reasonable assurance that the system's failure will not result in a crew or passenger fatality or permanent disability.

1.2.2 The Program Manager is responsible for ensuring that his/her program complies with the requirements set forth in this NPR (NPR 8705.2) and that the space system is qualified for human-rating certification.

1.2.3 The Chief Safety and Mission Assurance Officer serves as the Office of Primary Responsibility for the human-rating requirements. The Human-Rating Board performs executive level activities for the Human-Rating Requirements. The Associate Administrator for Space Operations and the Associate Administrator for Exploration Systems co-chair the Human-Rating Independent Review Team. The Human-Rating Independent Review Team supports the Human-Rating Board by providing insight of the Human-Rating Plan development, implementation, and the system's human-rating certification. The Chief Engineer (Independent Technical Authority) and the Chief Health and Medical Office (Independent Technical Authority for medical and human health requirements) ensure that tailoring, exceptions, deviations, and waivers are technically correct and have adequate justification. The Associate Administrator for Space Operations, Associate Administrator for Exploration Systems, Chief Engineer, and Chief Health and Medical Officer approve the Human-Rating Plan with concurrence from the Chief Safety and Mission Assurance Officer. The Chief Safety and Mission Assurance Officer provides verification that objective quality evidence has been assessed demonstrating compliance with human-rating requirements. The Associate Administrator for Space Operations provides the human-rating certification for each space system. See Figure 2 for a summary of the human-rating certification process. See Appendix B for definition of Human-Rating Board.

1.3 General Requirements

1.3.1 The Chief Safety and Mission Assurance Officer shall serve as the Office of Primary Responsibility providing leadership, policy direction, assessment, and coordination of the technical requirements and process compliance verification for NPR 8705.2 throughout the life cycle of the system ([Requirement 34259](#)).

1.4 Human-Rating Independent Review Team

1.4.1 Human-Rating Independent Review Team Purpose

1.4.1.1 The Human-Rating Independent Review Team shall provide the Human-Rating Board with insight of

the Human-Rating Plan development, implementation, and the system's human-rating certification process beginning in system formulation and continuing throughout the life of the program ([\(Requirement 34262\)](#)).

Note: In the context of human-rating requirements, the Human-Rating Independent Review Team provides insight that includes the review of the Human-Rating Plan, test plan, and verification compliance, and participation in meetings such as requirements development, requirements verification and closeout reviews, design certification reviews, and acceptance reviews.

1.4.2 Human-Rating Independent Review Team Membership

1.4.2.1 The Associate Administrator for Space Operations and the Associate Administrator for Exploration Systems shall charter (select membership and tasks of) the Human-Rating Independent Review Team that performs all functions independent of the Program Manager's funding and control ([\(Requirement 34265\)](#)).

1.4.2.2 The Associate Administrator for Space Operations and the Associate Administrator for Exploration Systems shall co-chair the Human-Rating Independent Review Team for each human space system ([\(Requirement 34266\)](#)).

1.4.3 Human-Rating Independent Review Team Membership Concurrences

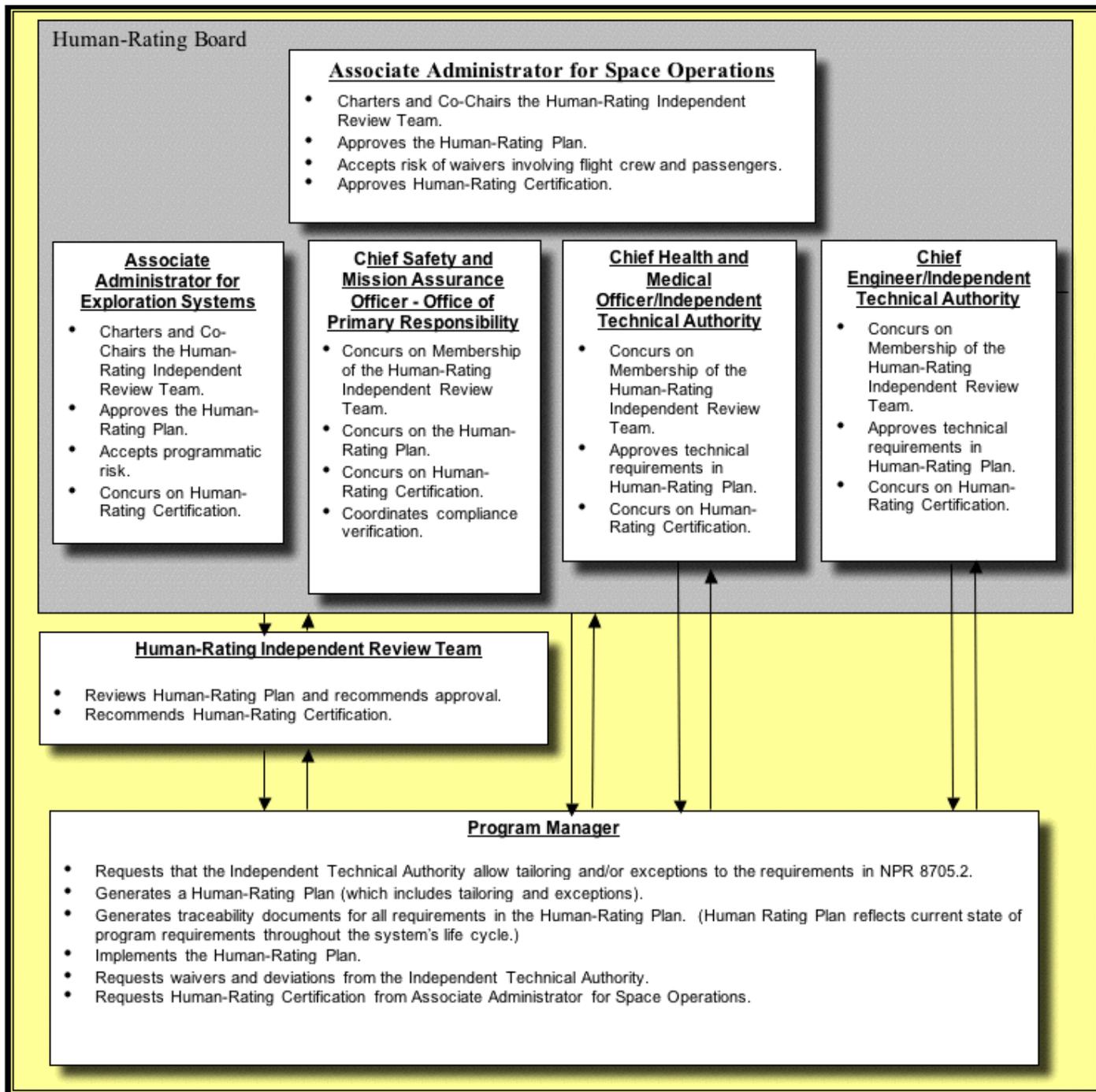
1.4.3.1 The Chief Safety and Mission Assurance Officer shall concur (or nonconcur) on the membership of the Human-Rating Independent Review Team ([\(Requirement 34268\)](#)).

1.4.3.2 The Chief Health and Medical Officer shall concur (or nonconcur) on the membership of the Human-Rating Independent Review Team ([\(Requirement 34269\)](#)).

1.4.3.3 The Chief Engineer shall concur (or nonconcur) on the membership of the Human-Rating Independent Review Team ([\(Requirement 34270\)](#)).

Note: The Charter is not complete until all members of the Human-Rating Board concur on the membership.

Figure 2. Human-Rating Certification Process Summary (Arrows indicate information flow)



1.5 Human-Rating Plan

1.5.1 Human-Rating Plan Development

1.5.1.1 The Program Manager shall develop a Human-Rating Plan for the human space system ([Requirement 34274](#)).

Note: The plan need not be a stand-alone plan provided it meets the requirements set forth in this document. One possible method is to incorporate the Human-Rating Plan into the program plan developed per NPR 7120.5.

Three volumes of the Human-Rating Plan are described within this document (NPR 8705.2). Figure 1 indicates due dates for the completion of these volumes.

1.5.2 Human-Rating Plan Content

1.5.2.1 In Volume I of the Human-Rating Plan, the Program Manager shall provide clear traceability for each requirement stated in this NPR (NPR 8705.2) by including a tracking matrix that describes how the program plans to comply with each requirement assigned to its responsibility and shows where each requirement will be incorporated into program documentation or levied onto the contractor ([\(Requirement 34278\)](#)).

Note: Requirements in this NPR (NPR 8705.2) that are the responsibility of other Agency professionals (e.g., Human-Rating Independent Review Team, Chief Safety and Mission Assurance Officer, and others) do not have to be included in the Human-Rating Plan.

1.5.2.2 The Program Manager shall document in Volume I of the Human-Rating Plan all tailoring and exceptions with the corresponding justification ([\(Requirement 34280\)](#)).

Note: Deviations and waivers are not documented in the plan because these are generated after the plan has been approved (see Figure 3).

1.5.2.3 In Volume I of the Human-Rating Plan, the Program Manager shall include a set of applicable standards approved by the Independent Technical Authority ([\(Requirement 34282\)](#)).

1.5.2.4 In Volume I of the Human-Rating Plan, the Program Manager shall document the duration of the program's human-rating certification ([\(Requirement 34283\)](#)).

Note: The duration of the human-rating certification identifies how long the certification exists before recertification is required.

1.5.2.5 In Volume II of the Human-Rating Plan, the Program Manager shall provide a description of the objective quality evidence that will be used to demonstrate that each human-rating requirement has been met ([\(Requirement 34285\)](#)).

1.5.2.6 In Volume II of the Human-Rating Plan, the Program Manager shall describe the space system(s) critical functions ([\(Requirement 34286\)](#)).

1.5.2.7 In Volume III of the Human-Rating Plan, the Program Manager shall describe each critical function's performance criteria and how the function of each will be ensured through analysis, test, inspection, and demonstration ([\(Requirement 34287\)](#)).

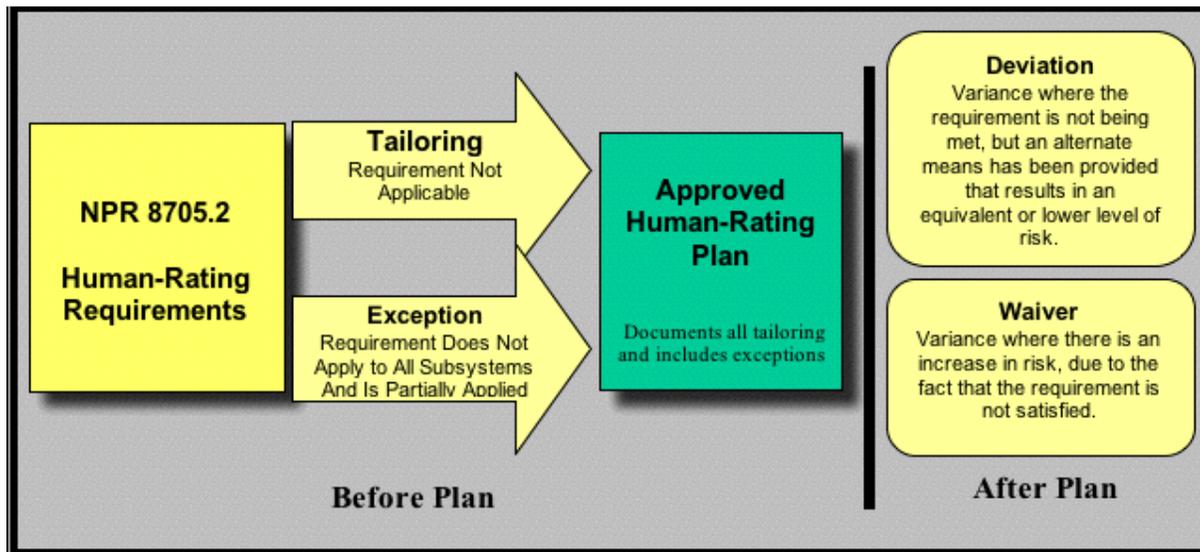
1.5.2.8 In Volume III of the Human-Rating Plan, the Program Manager shall document in the maintenance plan the processes that the program will use to ensure that the space system will be maintained in the as-certified condition ([\(Requirement 34288\)](#)).

Note: These processes may include (but are not limited to) raw material selection criteria and control, fabrication, inspection, tests, audits, and maintenance processes.

1.5.3 Tailoring and Exceptions to Human-Rating Requirements Documented in Plan

1.5.3.1 Introduction: Since space systems, missions, and environments vary significantly, all of the human-rating requirements and standards may not be applicable to each system. A summary of when tailoring, exceptions, waivers, and deviations occur is illustrated in Figure 3.

Figure 3: Overview of When Tailoring, Exceptions, Deviations, and Waivers Occur



1.5.4 Tailoring Process and Approvals

1.5.4.1 For a program using a phased acquisition approach, 60 workdays prior to the System Requirements Review (or for a program using the acquisition strategy meeting for down-select to a single contractor, 30 workdays prior to the acquisition strategy meeting), the Program Manager shall submit a request with supporting justification to the Independent Technical Authority to approve tailoring-out each requirement that does not apply to the space system ([\(Requirement 34293\)](#)).

Note: If tailoring is approved, the Program Manager does not have to meet the requirement that has been tailored out.

Note: Tailoring is for requirements that are not applicable (e.g., ascent escape requirements do not apply to a surface rover). Tailoring is not for requirements that are considered programmatically undesirable, expensive, or technically complicated.

1.5.4.2 For a program using a phased acquisition approach, 45 workdays prior to the System Requirements Review (or for a program using the acquisition strategy meeting for down-select to a single contractor, 15 workdays prior to the acquisition strategy meeting), the Independent Technical Authority shall approve (or disapprove) tailoring of the requirements in this NPR (NPR 8705.2) ([\(Requirement 34296\)](#)).

1.5.5 Exceptions Process and Approvals

1.5.5.1 For a program using a phased acquisition approach, 60 workdays prior to the System Requirements Review (or for a program using the acquisition strategy meeting for down-select to a single contractor, 30 workdays prior to the acquisition strategy meeting), the Program Manager shall submit a request with supporting justification to the Independent Technical Authority to approve an exception to a requirement if that requirement does not apply to all the subsystems ([\(Requirement 34298\)](#)).

Note: This occurs prior to System Requirements Review when the program is using a phased acquisition approach. If the program is using the acquisition strategy meeting for down-select to a single source contractor, this should be completed 30 workdays prior to the acquisition strategy meeting.

1.5.5.2 For a program using a phased acquisition approach, 45 workdays prior to the System Requirements Review (or for a program using the acquisition strategy meeting for down-select to a single contractor, 15 workdays prior to the acquisition strategy meeting), the Independent Technical Authority shall conditionally approve (or disapprove) exceptions to the requirements in this NPR (NPR 8705.2) ([\(Requirement 34300\)](#)).

Note: Approval is on the condition that the Associate Administrator for Exploration Systems accepts the risk posed by the exception.

1.5.6 Human-Rating Plan - Preliminary Review

1.5.6.1 Forty-five workdays prior to the specified program review, as illustrated in Figure 1, the Program Manager shall submit the specified volume of the Human-Rating Plan to the Human-Rating Independent Review Team for preliminary review ([\(Requirement 34303\)](#)).

1.5.6.2 Thirty workdays prior to the specified program review, as illustrated in Figure 1, the Human-Rating Independent Review Team shall provide the Program Manager with feedback concerning the adequacy of the Human-Rating Plan ([\(Requirement 34304\)](#)).

1.5.7 Human-Rating Plan - Final Review

1.5.7.1 Fifteen workdays prior to the specified program review, as illustrated in Figure 1, the Program Manager shall submit the specified volume of the Human-Rating Plan and supporting documentation to the Human-Rating Independent Review Team and the Human-Rating Board for final review ([\(Requirement 34306\)](#)).

1.5.7.2 Five workdays prior to the specified program review, the Human-Rating Independent Review Team shall provide the Human-Rating Board with an evaluation of the adequacy of the Human-Rating Plan that includes a recommendation as to whether to accept, modify, or reject the proposed Human-Rating Plan ([\(Requirement 34307\)](#)).

1.5.7.3 If the Human-Rating Independent Review Team recommends that the Human-Rating Plan be modified or rejected, the team shall provide the Human-Rating Board with a list of the items that must be corrected to achieve compliance ([\(Requirement 34308\)](#)).

1.5.8 Human-Rating Plan Approval and Concurrences

1.5.8.1 Prior to the specified program review, as illustrated in Figure 1, the Chief Engineer (Independent Technical Authority) and Chief Health and Medical Officer (Independent Technical Authority) shall approve (or disapprove) the specified volume of the Human-Rating Plan, including all tailoring and exceptions for the space system, indicating that the plan is technically acceptable ([\(Requirement 34310\)](#)).

1.5.8.2 Prior to the specified program review, as illustrated in Figure 1, the Associate Administrator for Space Operations and the Associate Administrator for Exploration Systems shall approve (or disapprove) the specified volume of the Human-Rating Plan ([\(Requirement 34311\)](#)).

1.5.8.3 Prior to the specified program review, as illustrated in Figure 1, the Chief Safety and Mission Assurance Officer shall concur (or nonconcur) on the specified volume of the Human-Rating Plan ([\(Requirement 34312\)](#)).

Note: If the Human-Rating Plan is not approved by the Chief Engineer, Chief Health and Medical Officer, the Associate Administrator for Space Operations, and the Associate Administrator for Exploration Systems and concurred on by the Chief Safety and Mission Assurance Officer, then the program is not authorized to implement the Human-Rating Requirements and will not be eligible for Human-Rating Certification.

1.5.8.4 At any time in the program's life, when the Independent Technical Authority approves exceptions to human-rating requirements, the Program Manager shall simultaneously have the Human-Rating Plan updated and approved ([\(Requirement 34314\)](#)).

1.5.9 Human-Rating Requirements Plan Compliance

1.5.9.1 Prior to certification, the Program Manager shall demonstrate compliance with the program's human-rating requirements as allocated through program documentation per the approved Human-Rating Plan ([\(Requirement 34316\)](#)).

1.5.10 Deviation Process and Approval

1.5.10.1 When a program's human-rating requirement will not be met, but through an alternate means, the system will have an equivalent or lower level of risk, the Program Manager shall request a deviation from the human-rating requirements ([\(Requirement 34318\)](#)).

1.5.10.2 The Independent Technical Authority shall approve (or disapprove) all deviations from the human-rating requirements ([Requirement 34319](#)).

1.5.10.3 The Associate Administrator for Exploration Systems or designee shall present the status of all new deviations at the Agency Quarterly Program Management Committee Meeting ([Requirement 34320](#)).

1.5.10.4 The Program Manager shall track all deviations from the human-rating requirements ([Requirement 34321](#)).

1.5.10.5 The Chief Safety and Mission Assurance Officer shall independently verify compliance with all deviations from the human-rating requirements ([Requirement 34322](#)).

1.5.11 Waiver Process and Approval

1.5.11.1 When a program does not meet a requirement in its approved Human-Rating Plan and there is an increase in risk, due to the fact that the requirement is not satisfied, and the risk and justification for the waiver have been documented, the Program Manager shall request a waiver to the requirement ([Requirement 34324](#)).

1.5.11.2 The Associate Administrator for Exploration Systems shall accept (or not accept) the programmatic risk for waivers ([Requirement 34325](#)).

1.5.11.3 The Associate Administrator for Space Operations shall accept (or not accept) the risk for waivers involving risk to flight crew and passengers ([Requirement 34326](#)).

1.5.11.4 Upon request for a waiver to a technical requirement, the Independent Technical Authority shall provide the program manager with technically acceptable alternatives including their corresponding risk and value assessments ([Requirement 34327](#)).

1.5.11.5 The Independent Technical Authority shall approve (or disapprove) waivers as technically acceptable ([Requirement 34328](#)). Note: Without an approval from the Independent Technical Authority stating that the waiver is technically acceptable and a statement of acceptance of the risk from the both Associate Administrator for Space Operations and the Associate Administrator for Exploration Systems, the program cannot proceed with implementation of the waiver.

1.5.11.6 The Associate Administrator for Exploration Systems or designee shall present the status of all new waivers at the Agency Quarterly Program Management Committee Meeting ([Requirement 34330](#)).

1.5.11.7 The Program Manager shall track the status of compliance with the provisions of all waivers ([Requirement 34331](#)).

1.6 Programmatic Requirements

1.6.1 Critical Functions

1.6.1.1 The Program Manager shall verify that all critical functions in the approved Human-Rating Plan have been allocated into the system design at the Critical Design Review ([Requirement 34334](#)).

1.6.2 Cumulative Risk Goals

1.6.2.1 Prior to System Requirements Review and throughout the development process, the Program Manager shall analyze the probability of fatality from catastrophic events and use the analysis for related design and operational trade studies ([Requirement 34336](#)).

1.6.2.2 When the Agency has established a relative risk goal or a relative risk requirement for a system, the Program Manager shall use probabilistic risk assessment to show compliance with the goal or requirement ([Requirement 34337](#)). Note: The objective of this assessment is to evaluate the cumulative mission risk for comparison with the mission risk goal. This can be accomplished by complying with NPR 8705.5, Probabilistic Risk Assessment Procedures for NASA Programs and Projects.

1.6.2.3 The Program Manager shall develop systems engineering models that are compatible with the risk model developed as part of the probabilistic risk assessment to estimate and allocate component, subsystem, and human reliability values throughout the development and operation of the system ([\(Requirement 34339\)](#)).

Note: Systems engineering modes can be created by using the NASA Probabilistic Risk Assessment Procedures Guide for Managers and Practitioners.

1.6.3 System Safety and Mission Assurance

1.6.3.1 The Program Manager shall implement established Agency processes (documented in NASA procedural requirements for safety and quality) relative to human health and safety that identify, analyze, track, and eliminate or mitigate hazards and risks throughout the life of the program ([\(Requirement 34342\)](#)).

1.6.3.2 The Program Manager shall prepare an integrated safety and mission assurance plan that maintains safety and mission assurance throughout the system life cycle and implements all of functions listed in Figure 4 ([\(Requirement 34343\)](#)).

Figure 4. Functions to be Included in the Integrated Safety and Mission Assurance Plan

Functions to be Included in the Integrated Safety and Mission Assurance Plan	
• Design and development controls	• Quality assurance
• Electrical, electronic and electro-mechanical (EEE) parts	• Reliability
• Emergency preparedness	• Risk management
• Fabrication controls	• Safety
• Flight test/ground operations	• Sampling plans/statistical planning and analysis
• Handling and shipping for flight hardware and software	• Software assurance
• Human error management	• Software engineering
• Identification and data retrieval	• Software formal inspection
• Maintainability	• Software independent verification and validation documentation
• Metrology	• Stamp controls
• Nonconforming articles and materials	• Systems engineering
• Probabilistic risk assessment	• Testing/inspection/evaluations
• Procurement	

1.6.3.3 The Program Manager shall ensure that the space system is designed to mitigate hazards using the following order of precedence ([\(Requirement 34344\)](#)):

- a. First, to eliminate hazards.
- b. Second, to reduce the likelihood of the occurrence of hazards.
- c. Third, to incorporate safety devices.
- d. Fourth, to provide caution and warning devices.
- e. Fifth, to develop administrative procedures and training.

1.6.4 Human Factors Engineering

1.6.4.1 The Program Manager shall apply human factors engineering beginning in early concept development and continuing throughout the life cycle of the space system ([\(Requirement 34346\)](#)).

1.6.4.2 The Program Manager shall involve human factors engineering and users, such as the Astronaut Office, mission operations personnel, and ground support personnel, in the development of human system interfaces ([\(Requirement 34347\)](#)).

1.6.4.3 The Program Manager shall establish human performance criteria and system usability requirements to ensure crew and passenger safety ([Requirement 34348](#)).

1.6.5 General Testing and Verification

1.6.5.1 The Program Manager shall perform demonstration, test, and analyses of critical functions at the integrated system level to ensure that the system design will not cause loss of life or permanent disability ([Requirement 34350](#)).

Note: Testing is used to verify the integrated performance of the space system hardware and software in the operational configuration. It is acceptable for the program to test elements in logical groupings with appropriate fidelity emulations of interfaces. It is preferred that integrated testing be performed on actual hardware rather than simulated or emulated interfaces.

1.6.6 Human-In-The-Loop Testing

1.6.6.1 The Program Manager shall perform usability testing of human-system interfaces for the critical functions using support from the user community including the Astronaut Office, ground processing crew, and mission control crew to verify that the system design meets the human performance requirements during system operation and in-flight maintenance consistent with the anticipated mission operations concept and anticipated mission duration ([Requirement 34353](#)).

1.6.6.2 The Program Manager shall use an iterative design process, where the results of the usability testing are incorporated into the design ([Requirement 34354](#)).

1.6.7 Software Testing

1.6.7.1 The Program Manager shall perform testing to verify and validate the performance, security, and reliability of all critical software across the entire performance envelope (or flight envelope) including mission functions, modes, and transitions ([Requirement 34356](#)).

1.6.7.2 Flight software shall, at a minimum, be tested using a flight-equivalent avionics test-bed operating in a real-time, closed-loop test environment ([Requirement 34357](#)).

1.6.7.3 The Program Manager shall test ground-control software on the computer platforms that will be used to support flights (space missions) ([Requirement 34358](#)).

1.6.8 Flight Testing

1.6.8.1 In Volume III of the Human-Rating Plan, the Program Manager shall document the type and number of flight tests that will be performed across the mission profile under actual and simulated conditions to achieve human-rating certification ([Requirement 34360](#)).

Notes

- i. The type and number of flight tests will be approved as part of the Human-Rating Plan approval process.
- ii. The flight test program provides two objectives. First, the flight test program uses testing to validate the integrated performance of the space system hardware and software in the operational flight environment. Second, the flight test program uses testing to validate the analytical math models that are the foundation of all other analyses, including those used to define operating boundaries not expected to be approached during normal flight.
- iii. Flight and ground tests are needed to ensure that the data for the analytical models can be interpolated 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.
- iv. 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 at all for some systems (e.g., rovers).

1.7 Human-Rating Certification

Note: Human-rating certification is the documented authorization granted by the Associate Administrator for Space Operations that validates that the system will perform its mission in the expected environment and verifies with objective quality evidence that the requirements were met allowing 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).

Note: The human-rating certification process is accomplished prior to a program's flight readiness review process, and the human-rating certification is presented at the flight readiness review.

1.7.1 Human-Rating Certification Request

1.7.1.1 The Program Manager shall submit a request to the Associate Administrator for Space Operations for human-rating certification for a space system ([\(Requirement 34366\)](#)).

Note: This applies to both initial certification and recertification after the approved certification period has ended.

1.7.1.2 At the time that the Program Manager submits a request for human-rating certification, the Program Manager shall provide the Associate Administrator for Space Operations, Chief Safety and Mission Assurance Officer, Associate Administrator for Exploration Systems, Chief Health and Medical Officer, Chief Engineer, and the Human-Rating Independent Review Team with a submission package that includes the following documents: the verification matrix that tracks status of each requirement in the approved Human-Rating Plan, the objective quality evidence that coincides with the matrix and demonstrates compliance with the requirements, the design reference missions, the system specification, and the documentation for all deviations and waivers ([\(Requirement 34368\)](#)).

Note: This data may be provided in hard copy, electronically, or via the web.

1.7.1.3 As a part of the human-rating certification process, the Program Manager shall demonstrate that appropriate process controls are in place for maintaining critical aspects of the human-rating certification throughout the life cycle of the program, including but not limited to ([\(Requirement 34370\)](#)):

- a. Production, procurement, and traceability of materials and components ([\(Requirement 34371\)](#)).
- b. Fabrication, maintenance, and inspection quality ([\(Requirement 34372\)](#)).
- c. System configuration control (Requirement 34373).
- d. Sustaining engineering (Requirement 34374).
- e. Maintenance and control of certification documentation ([\(Requirement 34375\)](#)).

1.7.2 Human-Rating Certification Recommendation

1.7.2.1 The Human-Rating Independent Review Team shall evaluate the adequacy of the program's compliance with the human-rating requirements as documented in the approved Human-Rating Plan and recommend whether the system should be certified as human-rated ([\(Requirement 34377\)](#)).

1.7.3 Human-Rating Certification

1.7.3.1 Prior to the flight readiness review, the Associate Administrator for Space Operations shall certify (or not certify) each space system as human-rated (Requirement 34379).

Note: If one of the Human-Rating Board members listed in 1.7.4 does not concur with the certification, the system cannot receive a human-rating certification.

1.7.4 Human-Rating Certification Concurrences

1.7.4.1 The Chief Safety and Mission Assurance Officer shall concur (or nonconcur) on the human-rating certification of any space system to be crewed during any phase of flight (Requirement 34382).

1.7.4.2 The Chief Health and Medical Officer shall concur (or nonconcur) on the human-rating certification of any space system to be crewed during any phase of flight (Requirement 34383).

1.7.4.3 The Chief Engineer shall concur (or nonconcur) on the human-rating certification of any space system to be crewed during any phase of flight (Requirement 34384).

1.7.4.4 The Associate Administrator for Exploration Systems shall concur (or nonconcur) on the human-rating certification of any space system to be crewed during any phase of flight (Requirement 34385).

1.7.5 Sustaining Human-Rating Certification

1.7.5.1 To sustain certification, the Program Manager shall provide sustaining and preventative maintenance to the space system to ensure it stays in the "as-certified condition" (Requirement 34387).

Note: This requirement exists because if the program manager stopped performing sustaining and preventative maintenance to the certified space system, its condition could degrade until it no longer had adequate safety and reliability.

1.7.5.2 The Program Manager shall implement a process that sustains the human-rating certification throughout the system's life cycle (Requirement 34389).

1.7.5.3 The Program Manager shall maintain the integrated safety and mission assurance plan throughout the system life cycle (Requirement 34390).

1.7.5.4 The Program Manager shall update analytical models throughout the life of the program by including design changes and actual operational and flight performance data (Requirement 34391).

1.7.5.5 The Program Manager shall maintain the risk assessment model throughout the system life cycle (Requirement 34392).

1.7.5.6 The Program Manager shall maintain the systems engineering model throughout the system life cycle (Requirement 34393).

1.7.5.7 The Program Manager shall keep all documentation related to the human-rating certification up-to-date throughout the system life cycle, including, but not limited to: the Human-Rating Plan, deviations, waivers, risk acceptance rationale, system drawings, compliance verification documentation, system maintenance plan, and safety and mission assurance plan (Requirement 34394).

1.7.6 Suspension of Human-Rating Certification

1.7.6.1 The Program Manager shall obtain Associate Administrator for Space Operations concurrence for any design changes or proposed alterations of equipment that affect the human-rating certification of the space system (Requirement 34396).

1.7.6.2 If the space system undergoes modifications or any changes to mission or environment that impact the human-rating certification as determined by the Associate Administrator for Space Operations, the Program Manager shall submit for approval the Human-Rating Plan with identified changes, any risk mitigations taken, and any increases to system risk (Requirement 34397).

1.7.6.3 If, during independent assessments and/or audits or after failures, deficiencies are identified in the "as-certified" design, operation, and/or maintenance of the space system, the Associate Administrator for Space Operations shall suspend the space system human-rating certification, thereby prohibiting use of the system for crews and passengers until compliance is reached and/or prohibition has been resolved (Requirement 34398).

1.7.7 Human-Rating Certification Reinstatement

1.7.7.1 The Associate Administrator for Space Operations shall reinstate human-rating certification only after the cause of the suspension has been thoroughly investigated and satisfactorily corrected and after he/she has obtained concurrences from the other Human-Rating Board members (Requirement 34400).

1.7.7.2 The Chief Safety and Mission Assurance Officer shall concur (or nonconcur) on the reinstatement of the human-rating certification (Requirement 34401).

1.7.7.3 The Chief Health and Medical Officer shall concur (or nonconcur) on the reinstatement of the human-rating certification (Requirement 34402).

1.7.7.4 The Chief Engineer shall concur (or nonconcur) on the reinstatement of the human-rating certification (Requirement 34403).

1.7.7.5 The Associate Administrator for Exploration Systems shall concur (or nonconcur) on the reinstatement of the human-rating certification (Requirement 34404).

CHAPTER 2. Standards

- 2.1 The Program Manager shall ensure that the system's design complies with NASA-STD-3000 Volume I - II, Man-Systems Integration Standards ([\(Requirement 34406\)](#)).
- 2.2 The Program Manager shall ensure that the system's design complies with MIL-STD-1472, Department of Defense Design Criteria Standard - Human Engineering ([\(Requirement 34407\)](#)).
- 2.3 The Program Manager shall ensure that the system's design complies with JSC 26882, NASA Space Flight Health Requirements ([\(Requirement 34408\)](#)).
- 2.4 The Program Manager shall ensure that the system's design complies with JPG 8080.5, JSC Design and Procedural Standards Manual ([\(Requirement 34409\)](#)).
- 2.5 The Program Manager shall ensure that the system's software development complies with the requirements in NASA-STD-8719.13, Software Safety Standard ([\(Requirement 34410\)](#)).
- 2.6 The Program Manager shall ensure that the system's design complies with the requirements in NASA Standard 5001, Structural Design and Test Factors of Safety for Spaceflight Hardware ([\(Requirement 34411\)](#)).
- 2.7 The Program Manager shall ensure that the system's design complies with the requirements in NASA Standard 5007, General Fracture Control Requirements for Manned Space Flight Systems ([\(Requirement 34412\)](#)).
- 2.8 The Program Manager shall ensure that the system's design complies with the additional set of applicable design and operational standards specified by the Independent Technical Authority ([\(Requirement 34413\)](#)).
- Note: The Independent Technical Authority selects standards (such as but not limited to: fabrication, flight operations, general navigation and control, ground processing, health, human factors, life support, medical, safety and mission assurance, structures, workmanship) that are to be applied to the system's Request for Proposal and subsequent contract. These standards will constitute requirements on the contractor or implementing authority as specified in the contract.*
- 2.9 Any tailoring or exceptions to these standards shall be approved by the Independent Technical Authority ([\(Requirement 34415\)](#)).
- 2.10 The Independent Technical Authority shall resolve any conflicts between technical standards and/or military specification and determine the appropriate standards for the program ([\(Requirement 34416\)](#)).

CHAPTER 3. System Design Requirements

3.1 Two-Failure Tolerance

3.1.1 Space systems shall be designed so that no two failures result in crew or passenger fatality or permanent disability ([\(Requirement 34419\)](#)).

Note: System design for reliability is a definitive element of space systems. While hardware is designed for inherent reliability at the component level, it is preferred that the architecture of the system also provides protection against random failures and minimizes the probability of loss of mission, space system, crew, or passengers. In systems with relatively short periods of operation, or where dynamic flight modes (such as powered ascent) are involved, installed redundancy is the principal means of ensuring the system's reliability. In space systems with longer missions and/or more time for recovery from failures, maintenance, designed-in-supportability, and logistics resupply are critical.

3.1.2 The Program Manager shall provide evidence and rationale that one or more of the following are met when requesting an exception, deviation, or waiver from the two-failure tolerance requirement ([\(Requirement 34421\)](#)).

- a. Two-failure tolerance is technically not feasible.
- b. The program manager demonstrates through analysis that redundancy does not reduce the critical system contribution to cumulative risk or the contribution of common cause failures to that critical system's failure.
- c. The system or subsystem, such as but not limited to, structures, pressure vessels, and thermal protection systems, that is unable to meet the two-failure tolerance requirement will be designed and certified in accordance with approved standards.

3.1.3 The system shall be designed and operated so that neither two inadvertent actions during operation or in-flight maintenance nor a combination of one inadvertent action and one failure result in crew or passenger fatality or permanent disability ([\(Requirement 34422\)](#)).

Note:

- i. *Inadvertent action includes, but is not limited to, out-of-sequence actions, wrong keystrokes, or inadvertent switch throws.*
- ii. *Design is the preferred method to produce an error-tolerant system. If the system cannot be designed to prevent inadvertent actions, then the system must provide the user with a method to detect and correct the inadvertent actions. An operational control is the last resort to manage this. Training is not considered an operational control to manage error because training alone does not ensure that errors are prevented or that the results of the error can be detected and corrected unless the system provides feedback and controls that allow error correction or hazard mitigation.*

3.1.4 The Program Manager shall provide evidence and rationale that one or more of the following are met when requesting an exception, deviation, or waiver to the two-inadvertent action requirement ([\(Requirement 34424\)](#)).

- a. Meeting the two-inadvertent action requirement is technically not feasible.
- b. The program manager demonstrates through analysis that redundancy does not reduce the critical system contribution to cumulative risk, or the contribution of common cause failures to that critical system's failure.
- c. The Program Manager has demonstrated by test data and comprehensive risk analyses that the system shall provide personnel with the capability to detect and recover from the inadvertent actions in time to prevent crew or passenger fatality or permanent disability.

Note: This requirement may be implemented through a top-down approach, a bottoms-up approach, or an accident scenario analysis approach. Error tolerance may be implemented in the design, such as "ready-arm-fire" for the initiation of potentially hazardous sequences, or in the operation, through the use of multiple crewmembers required to perform hazardous tasks.

3.1.5 The space system shall provide human error management in the following order of precedence ([\(Requirement 34426\)](#)):

- a. The system design prevents human error.
- b. The system reduces the likelihood of human error and provides the capability for the human to detect and correct the error through the incorporation of systems, controls, and associated monitoring.
- c. The system provides a method to limit the negative effects of errors so that the error does not result in a fatality or permanent disability.

Note: The intent of this requirement is to first avoid errors and when that is not possible, to avoid the catastrophic consequences that the errors may produce. This can be accomplished by describing the system goals and functions, describing the situation, describing the task and jobs, analyzing where errors are likely to occur, estimating the probability of each error, estimating the probability that the error is not corrected, determining the worst case effects of the error, determining where error has the potential to cause fatality or permanent disability, and providing error management.

Error management uses the following principles of design:

- i. Prevent error (see Figure 5 for details).
- ii. Provide redundancy to enable continued function after a failure.
- iii. Isolate elements so that the failure does not cause another failure.
- iv. Provide error detection, design failure limits, including the capability to sustain damage when the error occurs.
- v. Limit the negative consequences of the error.
- vi. Design a failure path to control and direct the effects of the error.
- vii. Allow for undefined unforeseen errors.
- viii. Consider adverse affects of foreseeable errors in the design, operation, and maintenance of the system.

Figure 5: Possible Methods to Prevent Error Possible Methods to Prevent Error

- Automatic sequencer (prevents human's mis-sequencing)
- Automation (prevents human's calculation errors)
- Automation (prevents human's monitoring errors)

- Boundary/Barrier to Entry (prevents entry into area)
- Breakaway (prevents system overload errors)
- Button/Switch Cover (prevents inadvertent activation)
- Constraint (limits movement)
- Control Limit (prevents exceeding boundaries)
- Dead Man Switch (prevents use)
- Dissimilar Shape Connectors (prevents incorrect connection)
- Dissimilar Size Connectors (prevents incorrect connection)
- Exclusion Design (design makes it impossible to make error)
- Guards (prevents entering into an area)
- Guides (prevents going out of boundary)
- In-process Feedback (feedback embedded in task step)
- In-process Verification (self-check embedded in task step)
- Interlock (prevents action out of sequence)
- Keyed Connector (prevents incompatible connections)
- Limiters (limits human action)
- Load Limiting Fuses (prevents overloads)
- Lock-in (prevents premature stopping of process)
- Lockout (prevents access)
- Machine Guards (prevents entering into area)
- Rate Limiter (prevents excess rate)
- Safeguards (prevents use, will not operate under unexpected conditions)
- Selection Limits (prevent incorrect selection)
- Shields (prevents access)
- Speed Restrictor/Governor (prevents going excess speed)
- Timer Lockouts (prevents activation of equipment at wrong time)
- Torque Limiter (prevents excess torque)

3.1.6 Space systems shall not use emergency systems or contingency and emergency operations (such as fire suppression or crew escape) to satisfy the two-failure tolerance requirement or two-inadvertent action requirement (([Requirement 34429](#))).

3.1.7 Space systems shall not use abort as the first leg of failure tolerance (([Requirement 34430](#))).

3.1.8 If the Program Manager has been granted an exception, deviation, or waiver to the two-failure tolerance requirement or the two-inadvertent action requirement, the justification and documentation shall include the level of fault tolerance achieved, the quantitative evidence of reliability with applicable data, the design process used to achieve minimum risk, and evidence that the exception, deviation, or waiver has been documented in the program's critical items list including acceptance rationale (([Requirement 34431](#))).

Note: Applicable data is specific to the system or component being evaluated, using similar components under similar conditions.

3.2 Human-System Interactions (Crew)

3.2.1 The space system shall provide a crew station, or equivalent interface, to provide the crew the capability to monitor, at a minimum, the health and status of critical functions (([Requirement 34434](#))).

Note: Within the context of this requirement, NASA defines "monitoring" as 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.

3.2.2 The space system shall include a crew station or equivalent interface that provides the crew the capability to operate, at a minimum, the critical functions of the system ([\(Requirement 34436\)](#)).

Note: Operate is equivalent to control. 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 crewmember 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).

3.2.3 The space system shall provide the crew feedback for all human commands for critical functions. ([\(Requirement 34438\)](#)).

Note: Feedback for human commands is a system communication that directly results from the user's input to the system and provides the user with information that allows him/her to determine if the input was received and what has been accomplished.

3.2.4 The space system shall provide the crew with the capability to reverse or correct inputs to critical functions from ground-control or flight crew that are physically reversible ([\(Requirement 34440\)](#)).

Note: Some inputs are not physically possible to reverse, such as pyrotechnic firing or activation of booster separation, and are not covered under this requirement.

3.2.5 The space system shall provide the crew accessibility to equipment involved in immediate and follow-up action that effects emergency recovery of the space system, such as, but not limited to, spacecraft compartment pressurization, life support, and emergency systems ([\(Requirement 34442\)](#)).

3.2.6 The space system shall provide the crew control over those systems that directly affect the performance of the crew (including, but not limited to, cabin temperature, cabin exterior/interior lighting, and radio volume) ([\(Requirement 34443\)](#)).

Note: This control will increase the probability of correct crew performance. Consequently, the crew will be less likely to make errors that cause loss of a critical function.

3.2.7 The space system shall provide the crew with the capability for manual override of higher-level software and automation (such as configuration change and mode change) when the transition from software/automation to manual control will not cause loss of critical functions ([\(Requirement 34445\)](#)).

3.3 Human-System Interactions (Ground Control)

3.3.1 The space system shall provide the ground control with the capability to monitor, at a minimum, the health and status of critical functions ([\(Requirement 34447\)](#)).

3.3.2 The space system shall provide the ground control the capability to operate, at a minimum, the critical functions of the system ([\(Requirement 34448\)](#)).

3.3.3 The space system shall provide the ground control feedback for all human commands for critical functions. ([\(Requirement 34449\)](#)).

3.3.4 The space system shall provide the ground control with the capability to reverse or correct inputs to critical functions from ground-control or flight crew ([\(Requirement 34450\)](#)).

3.3.5 The space system shall provide the ground control with the capability for manual override of higher-level software and automation (such as configuration change and mode change) when the transition from software/automation to manual control will not cause loss of critical functions ([\(Requirement 34451\)](#)).

3.4 Crew Workload

3.4.1 The space system shall be designed so mission design, including task design, procedures, and scheduling, does not affect the ability of the crew to successfully operate the spacecraft ([\(Requirement 34453\)](#)).

Note: This requirement is intended to provide a spacecraft system where mission training and operations can be accomplished with reasonable workloads for the flight and ground control crews. The system accomplishes this through system architecture being developed in parallel with, and with consideration to, the operations concept of the vehicle including the specific mission and task design.

3.4.2 The space system shall provide the flight crew with human-interfaces such that all tasks required of the flight crew meet a workload rating of 3 or better on the Bedford Workload Scale or the Modified Cooper-Harper Scale when tested by trained operators under simulated and actual flight conditions ([\(Requirement 34455\)](#)).

Note: One can measure the performance of the crew-system interface in terms of workload, performance, and errors. The Bedford Workload Scale (Roscoe, 1984) or the Modified Cooper-Harper Scale (Casali & Wierwille, 1983) measure workload and provide an estimate of how much workload margin is left over to perform additional tasks.

3.4.3 During periods of human-in-the-loop flight/ground path and attitude and directional control, the space system shall exhibit Level I handling qualities as defined by the Cooper-Harper Rating Scale when operated/flown by trained professionals under simulated and actual operational (flight) conditions ([\(Requirement 34457\)](#)).

Note: Systems such as a rover, space suit, or lunar base/processing system need Level I handling qualities for operations, whereas a flight system needs these for both flight and operations.

3.5 Fault Detection, Isolation, and Recovery

3.5.1 The system shall provide a fault detection, isolation, and recovery (FDIR) system for faults that affect critical functions ([\(Requirement 34460\)](#)).

3.6 Health and Status Data

3.6.1 The space system shall provide the capability to record health and status data of critical systems ([\(Requirement 34462\)](#)).

3.7 Autonomous Operation

3.7.1 The space system shall provide the capability for autonomous operation of critical functions ([\(Requirement 34464\)](#)).

Note: Autonomy from ground control is achieved through the ability of the crew to make decisions when input from the ground is unavailable or incomplete or when the situation is time-critical. Decisionmaking aids and/or expert systems that provide detailed information concerning potential system failure and recovery modes are methods that can be used when the ground support cannot be reached.

3.8 Crew and Passenger Survival for Generic System

3.8.1 The space system, such as a rover, lunar base, or other system, shall provide crew and passengers survival modes throughout the mission profile in the event of loss of a critical function ([\(Requirement 34467\)](#)).

3.9 Crew and Passenger Survival

3.9.1 The space system shall provide the crew and passengers with the capability for emergency egress to a safe haven during prelaunch activities ([\(Requirement 34469\)](#)).

3.9.2 The space system shall provide emergency egress, safe haven, and rescue post touchdown ([\(Requirement 34470\)](#)).

3.9.3 The space system shall provide crew and passenger survival modes throughout the ascent and on-orbit profile (from hatch closure until atmosphere entry interface) in the following order of precedence ([\(Requirement 34471\)](#)):

- a. Abort.
- b. Escape by retaining the crew and passengers encapsulated in a portion of the vehicle that can reenter without crew or passenger fatality or permanent disability.
- c. Escape by removing the crew and passengers from the vehicle.

Note: The requirement is for survival modes to cover 100 percent of the ascent trajectory. The preferred method is for abort to cover 100 percent of the trajectory, thus returning the crew to the Earth in the spacecraft. Some architecture options that do not lend themselves to the 100 percent abort coverage will need to use the other methods to meet the intent of this requirement.

3.9.4 The program shall ensure that ascent survival modes can be successfully accomplished during any ascent failure mode including, but not limited to, complete loss of thrust, complete loss of control, and catastrophic booster failure at any point during ascent ([\(Requirement 34473\)](#)).

3.9.5 The space system shall provide crew and passenger survival modes throughout the descent profile (from entry interface through landing) in the following order of precedence ([\(Requirement 34474\)](#)):

- a. Design features that increase tolerance to loss of critical functions such that landing can still be accomplished.
- b. Escape.

Note: A design feature such as a passive reentry mode is the preferred method of ensuring crew survival during reentry. Use of escape methods will be necessary for reentry vehicle designs that do not lend themselves to tolerance of loss of function.

3.9.6 The program shall ensure that the descent survival modes can be successfully accomplished for

loss of critical functions including, but not limited to, loss of active attitude control and loss of primary power ([\(Requirement 34476\)](#)).

3.9.7 The space system shall provide the crew with the capability to select abort modes ([\(Requirement 34477\)](#)).

3.9.8 The space system shall provide the crew with the capability to initiate the abort sequence ([\(Requirement 34478\)](#)).

Note: This requirement does not preclude automatic initiation of an abort system as long as an override capability is provided.

3.9.9 The space system shall provide the crew with the capability to inhibit the abort system ([\(Requirement 34480\)](#)).

3.9.10 The space system shall provide the crew with the capability to initiate the crew escape system ([\(Requirement 34481\)](#)).

Note: This does not preclude automatic initiation of an abort or crew escape system. It is desirable for the flight crew to be able to override the initiation sequence, recognizing the fact that there are some failure modes, particularly on ascent, where the initiation of escape occurs rapidly to save the flight crew, and the crew does not have time to override the initiation.

3.9.11 The space system shall provide the crew with the capability to override automatic initiation sequences ([\(Requirement 34483\)](#)).

Note: This includes automatic initiation of the crew escape system and ground control initiation of the escape system.

3.9.12 The space system shall provide ground control with the capability to select abort modes ([\(Requirement 34485\)](#)).

3.9.13 The space system shall provide ground control with the capability to initiate the abort sequence ([\(Requirement 34486\)](#)).

3.9.14 The space system shall provide ground control with the capability to initiate the crew escape system ([\(Requirement 34487\)](#)).

3.9.15 The space system shall provide the capability to automatically initiate abort(s) during dynamic phases of flight ([\(Requirement 34488\)](#)).

Note: Automatic aborts may be required during dynamic phases of flight where the crew may be unable to activate the system quickly enough to ensure crew survival.

3.9.16 While on the ground or in space, the space system shall provide the capability to disable the crew escape system by mechanical means (such as a pin, handle, or lever lock) ([\(Requirement 34490\)](#)).

Note: This provides the capability to ensure that the crew escape system is not activated during egress and ingress.

3.10 Flight Control Systems

3.10.1 The system design shall prevent or mitigate the effects of common cause failures in time-critical software (e.g., flight control software during dynamic phases of flight such as ascent) ([\(Requirement 34493\)](#)).

Note: Specific implementation of this requirement can take different forms. The following methods have been used in human-rated systems and meet the intent of this requirement:

- i. Redundant independent software running on a redundant identical flight computer.
- ii. Use of an alternate guidance platform, computer and software (e.g., using the space craft guidance to control a booster).
- iii. Use of nearly identical source code uniquely compiled for different dissimilar processors.
- iv. Regardless of the method to mitigate the effects of common cause failures, there is no substitute for software quality and exhaustive and thorough testing. An appropriate testing and verification process includes Independent Verification and Validation (IV&V) with manual code checks such as unit testing, path testing, stress testing, requirements verification, and code inspections.

3.10.2 During all phases of flight, the system shall provide the capability for manual control of flight path and attitude, when the human can operate the system within the structural, thermal, and performance margins without causing crew or passenger fatality or permanent disability ([\(Requirement 34495\)](#)).

3.11 Proximity Operations

3.11.1 Two crewed space systems conducting proximity operations shall have the capability to transmit and receive voice communications between each other ([\(Requirement 34497\)](#)).

3.11.2 When crewed and uncrewed space systems are performing proximity operations, the crewed space system shall have the capability to monitor the status of those systems on the uncrewed vehicle that are critical to the prevention of crew or passenger fatality or permanent disability ([\(Requirement 34498\)](#)).

3.11.3 When crewed and uncrewed space systems are performing proximity operations, the crewed space system shall have the capability to command those systems on the uncrewed space system that are critical to the prevention of crew or passenger fatality or permanent disability ([\(Requirement 34499\)](#)).

3.11.4 When crewed and uncrewed space systems are performing proximity operations, the ground control shall have the capability to monitor the status of those systems on the uncrewed vehicle that are critical to the prevention of crew or passenger fatality or permanent disability ([\(Requirement 34500\)](#)).

3.11.5 The crewed system shall provide the capability to confirm the environmental conditions of an unoccupied crew compartment prior to opening the hatch of that compartment ([\(Requirement 34501\)](#)).

Note: Environmental conditions include, but are not limited to, pressure, temperature, toxics, and oxygen.

3.11.6 The crewed space system shall provide the capability for manual flight control during proximity operations ([\(Requirement 34503\)](#)).

3.12 Flight Termination

3.12.1 Flight termination shall include features that allow sufficient time for abort or escape prior to

activation of the destruct system ([Requirement 34505](#)).

Note: The Range is responsible for safety of the public and ultimately will determine if and when the need for flight termination exists. Design features on the space system will be required to ensure adequate time to engage crew survival modes (abort or escape) prior to initiating the flight termination function.

Appendix A. Additional Related References

- A.1** Advanced Avionics Architecture & Technology Review - Phases 1 & 2, Joint Aeronautical Commanders Group, AAATR811, 21 January 1997.
- A.2** AFSPCMAN 91-1710, Range Safety User Requirements Manual, Volumes 1-7.
- A.3** Introduction to Software Verification and Validation, J. S. Collofello, SEI Curriculum Module SEI-CM-13-1.1, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, December 1988.
- A.4** JSC 13956, NASA Medical Operations Requirements Document for Space Shuttle.
- A.5** JSD SSP50260, International Space Station Medical Operations Requirements Document.
- A.6** JSC 23211, Proposed Standards for Human-Rating Space Systems, by Mary Cerimele, et al., October 1992.
- A.7** JSC 26895, Guidelines for Assessing the Toxic Hazard of Space Systems Chemicals and Test Materials, October 1997.
- A.8** JSC 27240, Rendezvous and Proximity Operations Design Reference for the ISS.
- A.9** JSC 27735, Space Medicine Monitoring and Countermeasures Project Plan, February 1997.
- A.10** MIL-HDBK-1797, Flying Qualities of Piloted Aircraft.
- A.11** NASA TND-5153, The Use of Pilot Rating in the Evaluation of Aircraft Handling.
- A.12** NASA/TM-2002-210785, Guidelines and Capabilities for Designing Human Missions.
- A.13** NASA-TMX-65284, Safety Requirements for Man-Rating Space Systems, 8 November 1968.
- A.14** NPR 7120.5, NASA Program and Project Management Processes and Requirements.
- A.15** NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects.
- A.16** Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, August 2002, <http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf>.
- A.17** NSTS 08080-1, Space Shuttle Manned Space Systems Criteria and Standards, 30 June 1992.
- A.18** NSTS-12820, NASA Mission Operations Directorate Operational Flight Rules, Volumes A, B, C, & D.
- A.19** QS-22A-LSK, Flight Crew Emergency Egress, Escape and Rescue.
- A.20** A Perspective on the Human-Rating Process of U.S. Space Systems: Both Past and Present,

George Zupp, ed. NASA Special Publication 6104, February 1995.

A.21 A Review of Man-Rating in Past and Current Manned Space Flight Programs, Aleck C. Bond, Eagle Engineering/LEMSCO Report Number 88-193, Contract Number NAS 17900, 20 May 1988.

A.22 SSP 50005, ISS Flight Crew Integration Standard.

A.23 JSSG-2010, Department of Defense, Joint Service Specification Guide: Crew Systems.

A.24 SSP 50038, Computer-Based Control System Safety Requirements - International Space Station Program.

A.25 SSP 50235, Interface Definition Document for ISS Visiting Vehicles.

Appendix B. Definitions

B.1 Abort: Termination of the nominal mission that allows the crew and passengers to be returned to Earth in the portion of the space system used for nominal entry and touchdown.

B.2 Automated: Automatic (as opposed to human) control of a system or operation.

B.3 Autonomous: Ability of a space system to perform operations independent from ground control and other space systems. This includes no communication with, or real-time support from, the ground control or other systems.

B.4 Breakout: During proximity operations, the ability to maneuver one or more vehicles to a safe separation distance.

B.5 Certification: Certification is documentation that validates that the requirements were correct, the system will perform its mission in the expected environment, and verifies that the requirements were met.

B.6 Crew: Any human on board the space system while in flight that has been trained to interact with the space system; same as flight crew.

B.7 Crew and Passengers: Every human on the space flight vehicle.

B.8 Crew Escape: See definition for escape.

B.9 Crew Survival: Capability and ability to preclude crew fatality or permanent disability.

B.10 Critical Functions: Capabilities or functions that are essential to the safety of the crew and passengers, that if lost would cause loss of life or permanent disability.

B.11 Critical Software: Any software component whose failure or unanticipated performance could lead to the loss of the flight crew and passengers or space system. This includes the flight software as well as ground-control software that can affect flight safety.

B.12 Critical System: A system is assessed as critical if loss of overall system function, or improper performance of a system function, could result in loss of life, loss of vehicle, or damage to the system.

B.13 Design for Minimum Risk: A process in which risks are reduced through specified margins of safety, factors of safety, material properties, or any other properties inherent to the design of the part, component, subassembly, or assembly. The process includes design implementation and verification provisions to enhance the safety critical reliability of space systems to the maximum extent practical.

B.14 Deviation: A written authorization for a variance where the requirement will not be met, but through an alternate means, the system will have an equivalent or lower level of risk.

B.15 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).

B.16 Exception: A written authorization given to the program, allowing the program relief from, or an alternative to, a requirement, because that requirement does not apply to any of the subsystems.

B.17 Fail-Safe: Ability to sustain a failure and retain the capability to safely terminate or control the operation.

B.18 Fault: A defect, imperfection, mistake, or flaw of varying severity that occurs within some hardware or software component or system. "Fault" is a general term and can range from a minor defect to a failure.

B.19 Flight Crew: Any human on board the space system while in flight that has been trained to interact with the space system; same as crew.

B.20 Hazard: Existing or potential condition that can result in or contribute to a mishap.

B.21 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.

B.22 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.

B.23 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.

B.24 Human-Rated Space System: A space system that incorporates those design features, operational procedures, and requirements necessary to accommodate human participants such that:

- a. Risks have been evaluated and either eliminated or reduced to acceptable levels;
- b. Human performance and health management and care have been appropriately addressed such that the system has been certified to safely support human activities; and
- c. The capability to safely conduct human-tended operations has been provided, including safe recovery from any credible emergency situation.

B.25 Human-Rating Board: The following group of NASA senior management that performs executive level activities for the Human-Rating Requirements: Chief Engineer, Chief Health and Medical Officer, Chief Safety and Mission Assurance Officer, Associate Administrator for Space Operations, and Associate Administrator for Exploration Systems.

B.26 Human-Rating Certification: Human-rating certification is the documented authorization granted by the Associate Administrator for Space Operations that validates that the system will perform its mission in the expected environment, and verifies with objective quality evidence that the requirements were met allowing 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).

B.27 Human-Rating Independent Review Team: An independent group of technical experts who reviews program products during the human-rating certification process and provides recommendations to NASA Headquarters senior management.

B.28 Human-Rating Plan: A formal document detailing the human-rating requirements that will be applied to a specific space system from System Requirements Review to system disposal at end of life. The Human-Rating Plan provides traceability from NPR 8705.2, Human-Rating Requirements for Space Systems, and includes rationale for all tailoring and exceptions. The Human-Rating Plan includes a verification matrix for all human-rating requirements that indicates how the requirements in the plan will be met, and the specific objective quality evidence that will be used to verify or demonstrate compliance with each requirement.

B.29 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.

B.30 Intervention Capability: The ability of the crew to assert control over all space system functions in nominal and off-nominal situations.

B.31 Manual Control: The crew's ability to bypass automation in order to exert direct control over a space system or operation.

B.32 Objective Quality Evidence: Any statement of fact, either quantitative or qualitative, pertaining to the quality of a product or service based on observations, measurements, or tests which can be verified. (Evidence will be expressed in terms of specific quality requirements or characteristics. These characteristics are identified in drawings, specifications, and other documents which describe the item, process, or procedure.)

B.33 Office of Primary Responsibility: The Office that is designated as "Responsible Office" for the requirements document.

B.34 Override: To take precedence over system control functions.

B.35 Passenger: Any human on board the space system while in flight that has no functional responsibility to perform any mission task for that system.

B.36 Permanent Disability: Any occupational injury or illness that does not result in a fatality or permanent total disability, but, in the opinion of competent medical authority, results in permanent impairment through loss of or compromised use of any part of the body, with the following exceptions: loss of fingernails or toenails, loss of tip of fingers or tip of toe without bone involvement, inguinal hernia (if it is repaired), or sprains or strains that do not cause permanent limitation of motion. Any nonfatal injury or occupational illness that, in the opinion of competent medical authority, permanently and totally incapacitates a person to the extent that he or she cannot follow any gainful occupation and results in a medical discharge or civilian equivalent.

B.37 Proximity Operations: Two or more vehicles operating 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).

B.38 Public: All humans not participating in the space flight activity who could be potentially affected by the function or malfunction of the space system.

B.39 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.

B.40 Rescue: The process of locating the crew, proceeding to their position, providing assistance, and transporting them to a location free from danger.

B.41 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, mission impacts) and associated uncertainties given that the undesired event(s) occur(s).

B.42 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.

B.43 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 or repair can be affected.

B.44 Safety: The freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

B.45 Space System: Any system developed and/or operated that supports activity in space, including, but not limited to, subsystems supporting launch, mission control, and operations.

B.46 Supportability: The degree of ease to which system design characteristics and planned logistic resources, including the logistics support elements, allow for the meeting of system availability and operational utilization requirements.

B.47 Tailoring: A process where a written authorization is given to the program from the Independent Technical Authority or designees prior to the approval of the Human-Rating Plan, allowing the program to exclude or modify a requirement in NPR 8705.2, Human-Rating Requirements for Space Systems, from the Human-Rating Plan, because the system does not have the component/subsystem described in that requirement, and consequently the requirement does not apply as written. For example, the system is not a flight vehicle; therefore it is not required to perform flight tests.

B.48 Test Flight: A flight occurring prior to certification.

B.49 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.

B.50 Validation: (1) An evaluation technique to support or corroborate requirements to ensure that necessary functions are complete and traceable; or (2) the process of evaluating software at the end of the software development process to ensure compliance with software requirements.

B.51 Variance: Documented and approved permission to perform or avoid some act or operation contrary to established requirements. A variance is an exception, deviation, or waiver.

B.52 Verification: The process of proving or demonstrating that requirements have been satisfactorily met through design and/or operational elements.

B.53 Verification Plan: A formal document listing the specific technical process to be used to show compliance with each requirement.

B.54 Waiver: A written authorization allowing a variance from a specific requirement where there is an increase in risk. The waiver includes a formal acceptance of risk by the program manager and by an official authorized to speak for the risk-takers when they do not fall under the authority of the program.

Appendix C. History and Rationale

C.1 Human-Rating Requirements

C.1.1 This appendix is included to provide a history and rationale to enhance the understanding of the human-rating requirements. This section does not negate application of requirements to a system or alter the requirements in NPR 8705.2. If it is interpreted to be in conflict with the requirements, the requirements supersede this appendix.

C.2 Introduction to Human Rating

C.2.1 The human-rating process for NASA programs has not fundamentally changed since the Mercury program. This process is meant to ensure the incorporation of design features and requirements necessary to maximize the health and safety of the human participants. This process demands that system safety be embraced at all levels of the program. It demands rigorous design, development, and testing as well as meticulous verification and process control. It dictates stringent management oversight and accountability of all participants. This process culminates in a formal certification for operational readiness and continues through the life of the program.

C.2.2. Human-rating requirements fall into two basic categories, Management and Design/Engineering/Implementation (Table C-1). Management rigor is required to ensure emphasis on crewed flight awareness, the development of a robust engineering and management review process, complete and timely problem reporting and corrective action, process controls for documentation, configuration, and certification, and finally, the utilization of appropriate and accurate risk analysis tools. Engineering requirements are aimed at the application of conservative design methods and standard practices, developing redundancy in critical systems, utilizing proven technology, and verification of design through extensive test and analysis.

C.3 Applicability of Requirements

C.3.1 Human-rating requirements are applicable to any system which transports or houses humans or interfaces with other systems which transport or house humans. Therefore, many uncrewed elements may also be subject to these requirements. For example, currently the expendable launch vehicle is not used in concert with a human-rated system, and so these requirements do not apply. However, if an expendable launch vehicle is used as part of a crewed launch system, human-rating requirements apply.

C.3.2 Human-rating requirements are to be reviewed carefully to ensure that requirements which do not apply (e.g., ascent abort requirements do not apply to surface rovers) are culled out of the initial requirements set via the tailoring process. The tailoring process is not intended to accommodate the deletion of requirements which are costly, technically difficult, or create a longer schedule. The

process is strictly for requirements which are not applicable to a specific system.

C.3.3 Exceptions are to be utilized when a requirement is not applicable to some subsystems, such as requirements for two-failure tolerance on primary structure, but is generically applicable to other subsystems. If the program has an approved Human-Rating Plan and then determines that it cannot meet a planned human-rating requirement for a subsystem (e.g., structures), and this variance is permanent (e.g., the system will not be designed to meet the requirement), the program is able to request an exception. If the exception is approved, the program updates the Human-Rating Plan to reflect this.

C.3.4 All other variances from requirements are handled through the waiver and deviation process to ensure appropriate visibility into the inability to meet requirements.

C.4 The Human-Rating Plan

C.4.1 The Human-Rating Plan documents how the program plans to comply with the human-rating requirements throughout the system's life cycle. The plan is, by necessity, a living document, or a multiple volume set, in order to comply with the content and approval requirements of this document. The plan need not be a stand-alone plan. As a matter of fact, it may be more expedient to fold it into overall systems plans and requirements; however, it is essential that the human-rating requirements are easily identified and extractable from these systems level documents, so as to be able to meet human-rating requirement review milestones. Most important is not where the requirements reside, but that there be clear identification of specific human-rating requirements and clear traceability from requirements to demonstration of compliance.

Table C-1: Areas of Emphasis for Human Rating

<p>Fundamental Tenets of Human Rating Management:</p>	<ul style="list-style-type: none"> ● Continuous Attention to Human-Rating Throughout the Program ● Human Health and Safety Priority ● Design/Engineering/Implementation: ● Well Established and Proven Aerospace Design Standards and Analytical Approaches ● Conservative Design Factors ● State-of-the-Art Technology ● High Quality ● Comprehensive Ground Test and Flight Test Before Crewed Flight ● Crew Survival Modes ● Two-Failure Tolerance to Prevent Fatality or Permanent Disability ● Hazard Detection and Safeing ● High Reliability Parts and Components ● Well Understood and Characterized Materials
---	---

C.5 Management Requirements

C.5.1 Program management is crucial to the success of human space flight and requires active involvement in every phase of the program. Proper attention by program management begins in the early formulation of the program by applying the requirements in this document and implementing them throughout the life of the program. It is ultimately the program manager's responsibility to assure the successful implementation of all human-rating requirements.

C.5.2 An endeavor as complex as human space flight requires that continuous attention be paid to all aspects of human rating throughout the life cycle of the program. Systems engineering, safety processes, risk management, certification, and sustaining engineering all require direct management involvement to assure the safety of the space flight system and its crew.

C.6 Technical Requirements

C.6.1 The technical requirements specified in this document are based on a history of successful space flight experience, as well as some difficult lessons learned. Space systems operate in an inherently high-risk environment, especially during the ascent and descent phases, and only the best practices of the aerospace industry are sufficient to give reasonable assurance that a failure does not result in a crew or passenger fatality or permanent disability.

C.6.2 Design and Test

C.6.2.1 Emphasis during design is on using established aerospace design standards, since these standards are based on lessons learned regarding the design and operation of space flight systems. While space flight systems design is built upon decades of aircraft experience, the unique operations and environments of the space flight missions lead to a different and even more stringent set of design requirements. It is essential that the design of a human-rated space flight system fully account for these differences. Historically, human rating was accomplished through the use of aircraft safety factors instead of the lower safety factors typical of uncrewed military launch vehicles, eliminating single failure points, and providing crew and passenger survival systems in case of a catastrophic vehicle failure. Incorporating historical and evolving lessons learned is critical to ensuring the highest level of design safety. As the design evolves, all system trades are focused on ensuring the integrity of the system design to meet human-rating requirements. The detailed design requirements and practices specified in JSCM 8080.5 represent significant crewed spacecraft design and operational knowledge applicable to a wide range of crewed space flight activities, and are to be utilized in all spacecraft and ground systems design.

C.6.2.2 The human-rated space flight system is designed, built, inspected, tested, and certified specifically addressing the requirements for human rating from the early formulation of the program. In addition to system and subsystem testing to ensure that design requirements are achieved, components are qualification and acceptance tested to ensure that adequate design margin exists at the component level for vibration, acoustic, thermal, shock (including pyrotechnic shock), and pressure/aerodynamic/structural loads, and to ensure the production hardware meets the quality of the certification hardware. Military Standard 1540, Test Requirements for Launch, Upper-Stage and Space Vehicles, dated September 1994, or equivalent component qualification and acceptance testing standards are good guidelines for the development of testing requirements. The use of dedicated qualification components is recommended. Flight components are acceptance tested in the previously noted environments, as applicable, to ensure that each individual component has adequate performance margin for its intended use. Policies for required margins for each environment for

qualification and acceptance are developed by the program. The performance margins are based on NASA and Military Standards, as well as successful similar programs.

C.6.2.3 For systems requiring incremental assembly where elements involve distributed end-to-end subsystems in low Earth orbit or beyond Earth orbit, it is prudent to conduct multiple-element integrated testing prior to launch. Use of approaches such as testing elements in logical groupings with appropriate fidelity emulations of interfaces is acceptable. The use of emulators is, however, less desirable than testing the actual hardware, and additional care needs to be exercised in the development of interface controls to ensure the emulators reflect the true "as built" configuration of the system. Testing is carried out with software possessing flight functionality and flight hardware in flight configuration. Priority is given to interface validations of hardware and hardware/software interaction. If applicable, end-to-end testing of command and telemetry links between the control center(s) and the vehicle can be accomplished.

C.6.3 Flight Test

C.6.3.1 No space flight system can be certified on the basis of analysis alone; therefore, comprehensive flight test is a very important part of the certification process. These flight tests can be done with humans providing all practical testing and analysis is completed and the vehicle is "Certified." Flight experience has shown that many critical performance parameters are highly design-specific and require thorough operational test and checkout to verify. Virtually all flight programs have shown important areas where flight and operational experience did not match the predictions. The design process for space flight systems is based on analyses and simulations that are highly dependent upon the analytical math models of the flight environment and the space flight systems hardware. Current and expected technologies require that many of these math models be based on estimates, approximations, and simplifications of the real world.

C.6.3.2 Whenever possible, it is good practice to conduct the flight test program across the entire mission profile. A sufficient number of flights are needed so that the flight test data validates the analytical math models in order to predict the performance of the space flight systems at the edges of the operational envelopes. This is generally possible for systems with discrete mission profiles of manageable duration such as Earth-to-orbit and crew rescue space flight systems. These systems can usually be operated through several complete ascents, orbital transfers, and/or descent profiles and can give good confidence in the suitability of the design for the planned mission. For some systems, a flight test across the entire mission profile may not be feasible, either due to the excessive amount of time required to cover the planned mission duration, or the lack of suitable conditions to test, as in the case of planetary landing space flight systems. In these cases, a series of tests encompassing all elements of the mission profile under actual or high-fidelity simulated conditions is the best method for demonstrating capability. Limited testing backed with extensive analysis and simulation may be an acceptable substitute for well-understood environments. Flight testing requirements apply to extravehicular mobility units or other systems, including those that have a self-contained propulsion system.

C.6.4 Human Engineering and Life Support

C.6.4.1 NASA has developed life support systems requirements that encompass all habitable space environments inclusive of the preflight, in-flight, and post-flight phases. An environment suitable for human habitation has been defined for pressurized elements according to the specifications and standards in NASA STD 3000. Human-factor-compliant designs and monitoring of critical environmental health parameters are necessary for optimal human performance. JSC 26882, NASA Space Flight Health Requirements, also discuss crew habitability and life support systems. These standards also apply to uninhabited space flight systems volumes that may require ingress and egress by a crewmember or passenger in flight such as a pressurized logistics mission cargo carrier. These

requirements have evolved from NASA's Mercury, Gemini, Apollo, Skylab, Shuttle Transportation System, the International Space Station, and multiple extravehicular suited programs. Long-duration space flight requirements are derived from NASA's Lunar, Skylab, Extended Duration Orbiter, International Space Station, and Phase One Mir life sciences programs. Other important human engineering standards to be relied upon are MIL STD 1472, DOD Design Criteria Standard - Human Engineering, and NASA/TM-2002-210785, Guidelines and Capabilities for Designing Human Missions.

C.6.5 Software

C.6.5.1 Providing effective safety of a space flight system dictates that controls be established for computer-based control systems. A computer-based control system utilizes computer hardware, software, and/or firmware to accept input information and processes that information to provide outputs to a defined task. Specific requirements for computer-based control of systems address the following: computer-based control system software requirements applied regardless of function; requirements for the control of functions that must work; and requirements for functions whose inadvertent operation would cause a hazard (such as must-not-work functions). An example reference for these technical requirements is SSP 50038, Computer-Based Control System Safety Requirements, International Space Station program.

C.6.5.2 Confirming integrity of software design and testing is essential to human space flight systems, and requires the use of independent software verification and validation to ensure that the software requirements are consistent and complete, that the scope of the test matrix covers all requirements, and that all discrepancies in the test results are resolved before flight. Software has become a key component in the safety and reliability of today's aerospace space flight systems, consequently all critical software is expected to be tested to the same levels of quality as the hardware systems. Critical software is any software component whose failure or unanticipated performance could lead to the crew or passenger fatality or permanent disability. This includes the flight software as well as ground software that can affect human health and safety.

C.6.6 General Aerospace Standards and Lessons Learned

C.6.6.1 Program and project managers are encouraged to access and use the NASA Headquarters Office of the Chief Engineer Web site which includes links to standards-developing organizations as well as links to lessons learned and best practices for aerospace design. Additional information on traditionally accepted design and verification methods and standards can be obtained through historical certification requirements documents listed in Appendix A of this document. The intent of the detailed design requirements and practices specified in these documents is to be incorporated in the design of human-rated space flight systems.

C.6.7 Two-Failure/Two-Inadvertent Action and Error Tolerant Design Requirements

C.6.7.1 As defined "fault (failure) tolerance" is the ability of a system or subsystem to perform its function(s) or (in case of a safety system) maintain control of a hazard in the presence of failures of its components.

C.6.7.2 Here, a component is defined as an individual constitutive element of the system. Components include passive hardware (such as pipes, wires, vessels, etc.), active hardware (such as pumps, valves, actuators, relays, etc), firmware (computer programs and data loaded into a class of memory that cannot be dynamically modified by the computer during processing), software (computer programs and data that can be dynamically modified during processing), and humans. All systems (and subsystems) are made up of components, whether passive or active.

C.6.7.3 The analysis of failures involves understanding the component's function and evaluating both

the context (environment, operating conditions, state of the remainder of the system) within which the component is called upon to function and its modes of failure. For example, the evaluation of passive components considers their passive functions and both their external and internal environments (microgravity, temperature, ionizing atmospheres, etc.) along with their failure modes (i.e., leaks in pipes or pressure vessels or minor bleed off shorts in wiring; catastrophic ruptures accompanied with shrapnel or complete dead shorts with sparks and heat). Analyses of active components involve the same process of considering their function, the context in which they are called upon to operate, and their failures modes.

C.6.7.4 Analysis of failures includes human failures or errors. An error, in this context, pertains to the failure of the human component. In almost all systems, the most complex component is the human. In addition, humans are considered active components where some human actions are learned rote responses to input stimulus while other actions are a result of cognitive processes. The human component also has the capacity to "fix" or "repair" its errors. Basically, a human error can be classified as an error of commission (performing the wrong action) or omission (failing to perform an action). When analyzing human errors, the same process used to analyze failures is employed. The analysis considers the action to be performed, the context (environment, performance shaping factors, operating conditions, state of the remainder of the system) within which the human is called upon to perform the action, and the modes of failure. To some degree, the analyses of software components are similar to the analyses of human components. This methodology has been used to analyze countless error in aerospace and other industries and can be performed with commercially available software.

C.6.7.5 In the perspective of the human-rating requirements, the two-failure tolerance and two-inadvertent action requirements are levied in the design of space systems only to the extent that they prevent or reduce the possibility of permanent disability or loss of life to the crew and space system passengers.

C.6.7.6 Therefore, two-failure/two-inadvertent action is the ability of the system or subsystem to perform its function(s) or (in case of a safety system) maintain control of a hazard in the presence of two failures/two inadvertent actions of its components. Said another way, it is a requirement that the space system be designed to tolerate two component failures/inadvertent actions without resulting in permanent disability or loss of life.

C.6.7.7 Appropriate failure tolerance is a fundamental aspect of human rating. Failure tolerance is a term frequently used to describe minimum acceptable redundancy, but 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. It is highly desirable that the space flight system performance degrades in a predictable fashion that allows sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures. This is true for failures involving hardware, software, and humans.

C.6.7.8 Due to the demands of a long duration mission, failures in systems will occur. Therefore, long duration mission design may use maintenance and system reconfiguration to restore failed functions and sustain two-failure tolerance and meet the two-inadvertent action requirement.

C.6.7.9 Once potential failures/errors are identified, system design trades can be made to prevent the failures or mitigate their effects. For example, system design may incorporate dissimilar systems performing the same function, cross strapping, failure tolerance, failure detection, and failure recovery capabilities to minimize the negative consequences of failures. Space flight system hardware is designed for inherent reliability at the component level, but the architecture of the system also needs to protect against random failures and minimize the probability of crew or passenger fatality or permanent disability. In systems with relatively short periods of operation, or

where dynamic flight modes (such as powered ascent) are involved, installed redundancy is the principal means of ensuring the system's reliability. In space flight systems with longer missions and more time for recovery from failures, maintenance and logistics resupply are critical. Elements that are designed for minimum risk, such as primary structure and thermal protection systems, are generally exempt from two failure tolerance requirements.

C.6.7.10 In practice, not all human errors can be identified, nor can systems be designed to prevent all human errors in operational contexts. However, many errors can be prevented, the frequency of human error can be minimized through design, and when error prevention is not possible, design features can be put in place to detect and correct the errors and mitigate the negative consequences.

C.6.7.11 When error prevention is not technically feasible or increases overall system risk, error can be managed through designs that assist the human in detection of the error and provide controls and time to recover from the error.

C.6.7.12 Human factors engineering uses these concepts along with detailed knowledge of human anthropometrics (ergonomics), cognitive reasoning in light of stimuli, rote memory, training, experience, feedback, sensory perception (sight, sound, olfactory, tactile) and the effects of environmental inputs (performance shaping factors) to design systems that interface with and are controlled by the human component. Meeting the two-failure tolerance/two-inadvertent action requirements is essential to operational safety where systems and subsystems are designed with full consideration of the actions of the human component in conjunction with potential failures of hardware, firmware, and software, the environments under which these actions are performed, and the potential human failures modes. This requirement also provides the designer a lot of flexibility establishing when a given error is impracticable or technically not feasible to eliminate.

C.6.8 Common Cause Failures

C.6.8.1 When using redundancy to meet the two-failure tolerance/two-inadvertent action requirements, it is a "best practice" to eliminate common cause failures/inadvertent actions and/or mitigate the risk. These types of failures /inadvertent action occur when both redundant systems fail because of some common reason, for example, the use identical components, exposure to common adverse environments, common incorrect maintenance operations, and components called upon to function outside their specifications. A method for reducing the potential for common cause failures would be to use dissimilar systems performing the same function.

C.7 Human Interfaces and Intervention

C.7.1 Industry experience does not support placing humans on board without the capability to intervene in the case of malfunction or other unanticipated events. History has shown that the overall contribution of the crew increases mission reliability since, in addition to being available to respond to hardware failures and unanticipated natural events, a human can overcome many latent errors in hardware and software design given the opportunity and if proper attention is paid to the human-machine interface. The contribution of the crew is maximized when it is provided with the proper insight, intervention capability, control over vehicle automation, authority to enable irreversible actions, and autonomy from the ground.

C.7.2 The intent of human interface requirements is that the system be designed to provide the operators with the required level of insight, feedback, and control appropriate to the flight phase, system and function:

- a. Feedback for human commands is a system communication that directly results from the user's input to the system and provides the user with information that allows him/her to determine if

the input was received and what has been accomplished. Determining the appropriate level of crew control over individual functions is a decision that is made separately for specific vehicles.

- b. Per the human-rating requirements, the system is designed so that the crew has control of the configuration and operation of all functions that can affect safety of flight. Specifically, if a valve or relay can be controlled by a computer, then that same control ought to be offered to the crew where the crew can be a viable part of the system design and perform that function. For example, it is not practical for a crew member to have control of individual valves that meter the flow of propellant to the engines, but a human interface capability (e.g. throttle) which incorporates multiple valve movements to achieve a desired end state (reduce or increase thrust) could be incorporated into the design to meet requirements.
- c. Per the human-rating requirements, the system is designed so that the crew has control over those systems that directly affect the performance of the crew such as cabin temperature, cabin exterior/interior lighting, and radio volume within safe operating limits, so that, within the capabilities of the subsystem, crew performance can be optimized. (Safe limits as defined by the Occupational Health and Safety Administration - for example, it is possible to adjust radio volume to a level that may cause hearing damage or impairment.)

C.8 Crew Stations and Displays

C.8.1 It is a best practice to apply attention to the human-system interface to maximize insight and minimize flight crew workload and errors. This holistic approach to designing the human-machine interface, including displays and controls, is required throughout the design process and, for each task identified, comply with applicable standards such as MIL-HDBK-1797. It is good practice in the design of the crew and machine interface to include iterative prototyping and usability evaluations with direct crew involvement.

C.8.2 The technology of displays and controls design continues to change and the state of the art can be applied to the human interface to minimize crew workload and errors. For example, the displays may be organized in a hierarchical fashion such that the highest level display provides an overview, the "big picture," with the provision for the crew to directly access additional displays for more specific details about the individual subsystems.

, ,

C.8.3 Specific designs for crew station configuration is dependent upon specific mission objectives and requirements. While the majority of space missions may be capable of being operated by a single, fully trained pilot, certain space missions may require more than one trained pilot due to increased workload. Vehicle designs that provide multiple functional crew stations can provide flexibility, improve safety, and enhance mission success. Multiple functional crew stations also provide redundancy for loss of displays or vehicle control devices.

C.8.4 Mockups and simulators can be developed to fully test the human-machine system in an operationally relevant context. A high-fidelity simulator is especially valuable for testing system performance in failure scenarios that cannot be safely tested with hardware and/or flight test. The human-in-the-loop functions ought to be evaluated under realistic scenarios, both nominal and off-nominal, to ensure they support the safety and reliability requirements of this document.

C.9 Crew Workload and System Handling Requirements

C.9.1 The performance of the crew-vehicle interface can be measured in terms of workload,

performance, and errors. It is good practice to develop crew and vehicle interfaces following accepted methods and standard practices, including concept development, rapid prototyping, and structured usability testing with flight crew involvement. The Bedford Workload Scale (Roscoe, 1984) or the Modified Cooper-Harper Scale (Casali & Wierwille, 1983) measure workload and may provide an estimate of how much workload margin is left over to perform additional tasks. The workload ought to meet the human-rating requirements even for off-nominal situations. Mission tasks cannot be scheduled at a pace that results in the degradation of crew performance. This is not intended to discourage a high-tempo of operations, but to result in the considerations of all factors that can adversely impact crew and therefore system performance.

C.9.2 To maximize flight crew performance in areas where vehicle maneuvering is required, the spacecraft is to exhibit Level I control qualities as measured using the Cooper-Harper Rating Scale (NASA TND-5153). Level I handling qualities ought to be available in all nominal phases of flight and most off-nominal situations. However, certain failures which degrade flight control surfaces or engine gimbaling may result in handling characteristics which are worse than Level I.

C.10 Crew and Passenger Survival

C.10.1 Probability of Survival Requirements

C.10.1.1 Expectations for overall probability of crew and passenger survival are to be defined early in the program. This allows for allocation of risk to specific systems at the conceptual design phase, which is essential to guide the program management and engineer in design trades. Inclusion of reliability estimation and allocation during system definition facilitates timely and effective decision making before critical design solutions are precluded. It is well understood that crew survival systems are difficult to retrofit into a mature design; however, options for robust design and crew escape systems that increase the probability of crew and passenger survival are feasible if addressed in early mass allocations.

C.10.2 Crew and Passenger Survival Modes

C.10.2.1 Crew and passenger survival modes (such as, but not limited to, abort, escape, safe haven, emergency egress and rescue) are a significant design element of space systems given the relative immaturity of human space flight. The overarching objective of a crew and passenger survival centered design is for the system to withstand critical system failure with appropriate redundancy and robust design. The need for survival modes beyond this robust design is an acknowledgement that the space system cannot always be designed to anticipate and withstand all failure modes. A robust crew survival capability is necessary for any human rated system, but the specific determination of survival modes is highly dependant on the system configuration.

C.10.3 Abort vs. Escape

C.10.3.1 For ascent, abort is always the preferred mode of operation after failure. Exposure to the environment, addition of complex extraction systems, and limited capability for system verification all add risk for a successful crew or passenger extraction. It is good design practice for abort modes to remain within the performance envelope of the crew escape system to survive additional system failures or other problems during the abort trajectory.

C.10.3.2 Recovery from catastrophic failure modes during reentry necessitates robust design to withstand the event, to allow for landing with the failure, or to withstand the event and allow for subsequent escape and crew and passenger recovery. The ability to withstand significant failure through robust design and allow for a landing is always preferred over an escape. Robust design is defined as the implementation of design characteristics which provide resistance to catastrophic

failure modes and tolerance to failure by supplying additional capability to withstand extreme off nominal circumstances and environments (e.g. structural hardening). Depending on system architecture, combinations of survival modes may be required to offset the uncertainty associated with verification of high probabilities of safe crew and passenger return.

C.10.3.3 A verified abort mode allows for crew and passenger return and crew recovery without exceeding the physiological and cognitive limits of the crew, while maintaining stability, control, structural, or thermal safety factors of the space flight system. Contingency abort modes, where stability, control, structural, or thermal safety factors are reduced, still retain positive margin and remain within physiological and cognitive limits of the crew. It is good practice to verify aborts with flight test.

C.10.3.4 Crew escape systems require extensive testing and analysis to verify the functional envelope and environment for system utilization, as well as detailed tests and assessments to ensure the system does not cause a fatality or permanent disability. Due to the dynamic and unpredictable nature warranting the use of crew escape systems, complete verification by integrated flight test is impossible. Crew escape systems may never be considered as a leg of redundancy.

C.10.4 Crew and Passenger Survival Risk Assessment

C.10.4.1 When determining the appropriate crew and passenger survival modes to employ for a given failure scenario, it is good practice to perform qualitative and quantitative risk analyses employing safety and reliability methodologies to determine the best solution for crew survival. Analyses of likelihood of success for candidate survival methods take into account the time required to successfully implement the method as compared to the time to effect of the hazardous situation. Variables such as exposure of the crew and passengers to the hazard in question (e.g., booster explosion), as might be the case for an escape, are analytically compared to the risks of attempting to execute a separation of the crewed spacecraft from the hazard. New hazards may be introduced by the employment of a given survival method (e.g., such as premature firing of an ejection seat) that are weighed against the potential risk mitigation gained from the method. Combined with detailed engineering analyses, these risk analyses provide a common yardstick to measure the potential for risk reduction or risk increase.

C.10.5 System Specific Implementation

C.10.5.1 Earth-to-Orbit

C.10.5.1.1 For some launch systems (i.e., capsule derivatives) 100 percent abort may be a viable option to meet requirements for crew and passenger survival; however, for other launch systems, escape modes may be required to achieve the desired probability of crew and passenger survival. The incorporation of survival modes on ascent is necessary, regardless of analytical risk assessments, due to the highly dynamic nature of the ascent flight regime and the increased likelihood of catastrophic, uncontrollable failures.

C.10.5.2 Beyond Earth Orbit

C.10.5.2.1 Beyond Earth orbit missions require unique survival modes. Missions designed for beyond Earth orbit require sufficient power, consumables, and trajectory design to maximize crew and passenger survival capabilities. These modes include, but are not limited to: powered return, free return, pre-positioning capabilities, safe haven, and rescue. In general, the mission profile requires the space flight systems and their propulsion system to have sufficient propellant to fly off-nominal trajectories. The design can provide time for other systems or the crew to recover from a critical system failure. As a last resort, when abort modes are not feasible, a safe haven capability may be provided to ensure that survival capability and consumables exist to return the crew to a

position from which a normal recovery or rescue can be conducted. It is good practice in long-duration mission planning to give consideration to pre-positioning consumables, spare parts, and other critical logistics and services to improve abort and safe haven capabilities.

C.10.5.2.2 Autonomy, functional redundancy, and tools to deal with the unexpected are a critical part of the design for safety. Technology will likely pace the schedule for accomplishing this.

C.10.5.3 Crew and Passenger Rescue

C.10.5.3.1 The crew and passenger rescue mission achieves its reliability through appropriate system design for availability, simplicity of hardware, and failure tolerance. Flight experience has shown that it is likely to be used at least once during the life of a Space System program, most likely due to a medical contingency. Since it may be attached to the Space System for extended periods of time and is essential to the Space System mission, operational availability on demand and high reliability throughout its on-orbit life are significant aspects of Space System design. To achieve acceptable levels of reliability and availability, on-orbit checkout and maintenance capabilities may be required.

C.10.5.3.2 Since crew rescue vehicles provide emergency escape, traditional abort and escape modes are not applicable. Consequently, the space flight system provides the capability to transport severely injured or ill crewmembers, in need of medical evacuation, safely to Earth.

C.10.5.4 Crew and Passenger Transfer

C.10.5.4.1 The main function of a crew transfer system is to ferry crewmembers and passengers to or from space flight systems. Since life support systems aboard a crew transfer vehicle may be limited, abort modes that allow for the safe recovery of crewmembers and passengers are critical.

C.10.5.4.2 When transferring crewmembers to or from space flight systems, there may be multiple options for abort modes (such as return to origin, abort to destination, and station-keeping).

C.10.5.5 Non-Crewed Systems

C.10.5.5.1 When a space flight system is used without crew or passengers aboard and in proximity operations to a crewed vehicle, an abort mode to separate a safe distance from the crewed vehicle is to be provided.

C.10.5.6 Space System

C.10.5.6.1 An extended Space System mission duration increases the probability that some emergencies will arise. This requires that the means be provided to manage these emergencies to successful resolution rather than evacuating at the first indication of system malfunction, crew or passenger illness, or injury. This can be accomplished through resilient core system design, including high degrees of failure tolerance, maintainability, skip cycle logistics stores on orbit, a robust logistics chain, and the provision of emergency medical facilities on board. However, the capability to evacuate and return to Earth is to be provided at all times. For Space Station missions, abort and crew escape requirements are functionally the same. Therefore, the program requires an escape vehicle and/or a safe haven, which provides for safe and timely crew and passenger return.

C.10.5.7 Habitable Surface Systems

C.10.5.7.1 A Habitable Surface System is similar to a Space Station in that it will typically have an extended mission duration, but it differs in that the capability for an immediate crew and passenger return will not always be feasible. Therefore, providing a means of dealing with emergencies is required. In many cases, an immediate evacuation in response to an emergency may not be practical. For these situations, emergency medical and safe haven capabilities including remote medical

treatment are significant elements in the system design.

C.10.5.8 Extravehicular Mobility Unit

C.10.5.8.1 Extravehicular Mobility Units operate in the vicinity of a larger space system. Therefore, the minimum reliability of the Extravehicular Mobility Unit provides for enough reserve capacity to allow the crewmember to safely return to the larger space flight systems. This reliability is allocated over the number of required missions of the Extravehicular Mobility Unit. Extravehicular Mobility Units ought to include crew self rescue devices worn by each Extravehicular Activity crewmember during all periods when there is no vehicle to credibly rescue an inadvertently detached Extravehicular Activity crewmember. This device could be the Simplified Aid for Extravehicular Activity Rescue or an equivalent capability.