NASA Procedures and Guidelines

NPG: 8705.2

Effective Date: June 19, 2003
Expiration Date: June 19, 2008

Human-Rating Requirements and Guidelines for Space Flight Systems

Responsible Office: **Q/Office of Safety and Mission Assurance**

TABLE OF CONTENTS

Preface

P.1 PURPOSE

NASA's policy is to protect the health and safety of humans involved in and exposed to space flight activities, specifically the public, the crew, passengers, and ground processing personnel. This document aids in the implementation of that policy by establishing human-rating requirements for Agency space flight systems that carry humans or whose function or malfunction may pose a hazard to NASA space systems that carry humans. This document provides the requirements, procedures, and guidelines to design and certify as human-rated all space flight systems involving humans or interfacing with human space flight systems prior to and after becoming operational. The intent of this certification is to provide the maximum reasonable assurance that a failure will not imperil the flight crew or occupants and that personnel may be recovered without a disabling injury if there is a mishap. Certification ensures that conditions that could adversely affect the safety of personnel are mitigated. The human-rating process is used to maximize the safety of the crew and passengers. Other requirements for safety and mission assurance are documented in NASA Headquarters Office of Safety and Mission Assurance (OSMA) policy and program-specific requirements documents. (For space suits and human maneuvering units, human rating implies flight certified.)

P.2 APPLICABILITY

a. The requirements in this document apply to all space flight systems (hardware, software, ground, and flight) developed and/or operated by or for NASA, to support human activity in space and that interact with NASA human space flight systems. Space flight system design and associated risks to humans shall be evaluated over the program's life cycle, including design, development, fabrication, processing, maintenance, launch, recovery, and final disposal. The Governing Program Management Council (GPMC) will determine the applicability of this document to programs and projects in existence (e.g., heritage expendable and reusable launch vehicles and evolved expendable launch vehicles), at or beyond implementation, at the time of the issuance of this document. Program managers of existing and new systems will have the option of tailoring the human-rating requirements set forth in this document, with approval from the CHMO, AA for OSF, and AA for SMA. (See section 3.4, which addresses the requirements tailoring submission and approval process.) Applicability to internationally provided space flight systems should be negotiated and documented in a distinct separate agreement, which can be joint or multilateral.

b. This document is not a direct instruction to NASA contractors but provides requirements, procedures, and guidelines to the responsible NASA program officials and contracting officer. It is made applicable to contractors as appropriate through contract clauses, specifications, or statements of work in conformance with the NASA Federal Acquisition Regulation (FAR) Supplement.

c. This document shall not supersede more stringent requirements imposed by individual NASA organizations and other Federal Government agencies. NASA program and project management requirements are contained in NASA Procedures and Guidelines (NPG) 7120.5, NASA Program and Project Management Processes and Requirements. A requirement is identified by "shall," a good practice by "should," permission by "may" or "can," expectation by "will," and descriptive material by "is."

d. Human-Rating Plan Development Guidance:

(1) All program managers shall submit a human-rating plan for initial review and final approval in accordance with the requirements of this document and within the timeframe requirements in Appendix C. The human-rating plan should describe the system design, reference missions, system safety engineering, safety and risk management, and maintenance necessary to reduce risks to an acceptable level throughout the system's life cycle. The plan need not be a stand-alone plan, provided it meets the requirements set forth in this document. The human-rating plan may be incorporated into the program plan developed via NPG 7120.5, latest revision.

(2) At a minimum, all human-rating plans shall address all "shall" requirement statements in this document. All "shall" statements in this document are boldfaced. All human-rating plans should follow the format of chapter 2 of this document. All human-rating plans shall document compliance and clear traceability with all functional and performance design requirements established in this document.

(3) Human-rating plan content can be a subcategory of the risk management and verification process and deliverables. Human-rating requirements can be included in the requirements flow down from higher level requirements documents. In addition, the verification plan required for human rating can be a part of the overall program verification plan.

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 8700.1A, NASA Policy for Safety and Mission Success.

c. NPD 7120.4B, Program/Project Management.

P.4 REFERENCES

a. MIL-STD-1472, Department of Defense Design Criteria Standard - Human Engineering, latest revision.

b. NASA/TM-2002-210785, Guidelines and Capabilities for Designing Human Missions, latest revision, or equivalent NASA Standard.

c. IEEE/EIA 12207 – Information Technology, Software Life-cycle Process, latest revision.

d. JSCM 8080.5, JSC Design and Procedural Standards Manual, latest revision.

e. JSC 26882, NASA Space Flight Health Requirements, latest revision.

f. NASA Standard 8719.13, Software Safety NASA Technical Standard, latest revision.

g. NASA-STD-3000 Volume I – IV, Man-Systems Integration Standards, latest revision.

h. NASA TND-5153, The Use of Pilot Rating in the Evaluation of Aircraft Handling Qualities, latest revision.

i. NPD 8730.4, Software Independent Verification and Validation (IV&V) Policy, latest revision.

j. NPG 7120.5, NASA Program and Project Management Processes and Requirements, latest revision.

k. NPG 8715.3, NASA Safety Manual, latest revision.

l. Additional references are available in Appendix A.

P.5 CANCELLATION

None.

Original signed by

_____

/s/ Bryan D. O'Connor
Associate Administrator
for Safety and Mission Assurance

Concurrence:

/s/ Dr. Richard S. Williams Chief Health and Medical Officer	/s/ William F. Readdy Associate Administrator for Space Flight	/s/ Dr. Jeremiah F. Creedon Associate Administrator for Aerospace Technology

Chapter 1: Responsibilities

1.1 The NASA Associate Administrator for Space Flight (AA for OSF) shall:

a. Act as the Human-Rating Authority for all human space flight systems and shall certify each space flight system as human-rated.

b. Charter and direct a Human-Rating Independent Review Team (HRIRT) for human space flight systems, such as Earth-to-Orbit (ETO) vehicles, space stations, or vehicle level programs. The review team shall be composed of nonadvocate members who perform all functions independent of the program manager's control.

c. Ensure that the human-rating plan, developed by the programs/projects, is provided to the AA for SMA and the CHMO for review and concurrence.

d. With the recommendation of the AA for SMA, CHMO, and the HRIRT, review and approve the human-rating plan for all proposed space flight systems, including changes and implementation. This includes any tailoring or deviations.

e. Oversee the proper development and execution of the human-rating plan for OSF-managed programs.

f. Verify continued compliance with human-rating certification requirements.

1.2 The NASA Associate Administrator for Safety and Mission Assurance (AA for SMA) shall:

a. Review the human-rating plan for all proposed space flight systems, including changes and implementation, and concur or nonconcur on the plan.

b. Concur or nonconcur on all human-rating requirements tailoring and deviations to the human-rating plan.

c. Provide input to the HRIRT charter.

d. Review the HRIRT assessments and provide concurrence or nonconcurrence to the GPMC and to the NASA Administrator.

e. Concur or nonconcur on the NASA AA for OSF certification of any space flight system to be human-inhabited during any phase of flight.

f. Maintain and update the "Human-Rating Requirements and Guidelines for Space Flight Systems" NPG and verify that processes are in place to ensure compliance with the document.

1.3 The NASA Chief Health and Medical Officer (CHMO) shall:

a. Review the human-rating plan for all proposed space flight systems, including changes and implementation, and concur or nonconcur on the plan.

b. Concur or nonconcur on all human-rating requirements tailoring and deviations to the human-rating plan.

c. Provide input to the HRIRT charter and membership.

d. Review the HRIRT assessments and provide concurrence or nonconcurrence to the GPMC and to the NASA Administrator.

1.4 The NASA Associate Administrator for Aerospace Technology (AA for OAT) shall:

a. Oversee the proper development and execution of the human-rating plan for OAT-managed programs.

b. Ensure the human-rating plan, developed by programs/projects, is provided to the AA for SMA and the CHMO for review and concurrence.

c. Ensure all space flight systems design, development, testing, and evaluation are performed to meet customer requirements prior to transfer to the OSF for space flight system operations.

1.5 The Program Manager shall:

a. Develop the human-rating plan for all human space flight program activities, based upon the unique mission goals, technical and operational risk, other risk-management plan requirements, and other specific characteristics of the program.

b. Integrate the human-rating plan into overall program management planning and execution and decisionmaking processes, including cost, schedule, performance, and other programmatic risks consistent with NPG 7120.5, latest revision.

c. Obtain approval of the program's human-rating plan by the AA for OSF, the AA for SMA, and the CHMO during the program approval process.

d. Justify proposed tailoring and deviations from these requirements. Tailoring and deviations may be implemented by the program manager where sound technical rationale provides justification and it is demonstrated that the tailoring and deviations do not significantly increase risk to human occupants. The tailoring and deviations shall be documented in the program human-rating plan, approved by the AA for OSF and are subject to the concurrence from the AA for SMA and CHMO.

e. Ensure that all deviations and waivers generated after the program human-rating plan approval from NASA Headquarters are presented at all program major milestone reviews.

f. Ensure that compliance and verification processes have clear traceability with all functional and performance design requirements established in this document.

g. Ensure that issues, problems, and decisions regarding the specification and achievement of human rating are elevated to appropriate management levels using a formal management review process, with an emphasis on risk management.

h. Establish and utilize a continuous tracking method for documenting and sustaining compliance with all human-rating requirements after initial human-rating certification.

i. Use systems engineering, safety, health, and management approaches in which all aspects of design, development, fabrication, operations, maintenance, and disposal are considered in the human-rating process. This should be accomplished by utilization of tools such as failure modes and effects analyses, fault trees, hazard analyses, maintainability analyses, reliability predictions, human error analysis, and probabilistic risk assessments to identify, quantify, mitigate, and manage hazards.

j. Demonstrate program compliance with the approved human-rating and verification plans to ensure the flight system certification is achieved and maintained.

k. Ensure that all records generated in the process of complying with this document are managed and dispositioned in accordance with NPG 1441.1, NASA Records Retention Schedules, latest revision.

l. Ensure that all performance data are archived to be available for recertification of program human rating.

1.6 The Human-Rating Independent Review Team (HRIRT) shall:

a. Review critical aspects of a program's human-rating process beginning in formulation and continuing through the Flight Readiness Review (FRR) of the first flight. (This may include the review of verification results/content, verification compliance and closeout review, or any participation in design certification reviews/acceptance reviews.)

b. Review each program's proposed human-rating plan, including design criteria, system designs, test requirements and procedures, software design, test and verification requirements, safety and reliability requirements, human factors engineering requirements, health requirements, and other program elements required to achieve human rating.

c. Review program verification plan in relation to human-rating requirements.

d. Review all human-rating requirements tailoring and deviations to the human-rating plan.

e. Transmit a recommendation to the AA for OSF or his/her designee, to accept, modify, or reject the proposed human-rating plan. If the recommendation is to reject or modify the plan for human-rating, the independent review team shall provide appropriate recommendations on changes required.

f. Provide recommendation regarding adequacy of compliance of any crewed system or system that interacts with a crewed vehicle prior to certification.

g. Provide a recommendation to the AA for OSF regarding certification of any human space flight system prior to first operational flight.

Chapter 2: Technical Requirements

2.1 Introduction

2.1.1 The technical requirements specified in this document are based on a history of successful space flight experience. Spacecraft 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 of success.

2.1.2 The following technical requirements shall be followed for the human rating of all space flight systems (hardware and software, ground and flight) which are developed and/or operated by, or for NASA to support human activity in space or which interact with NASA human space flight systems. Since these space missions vary significantly from one mission to another, not all of the human-rating requirements are applicable to each. Example systems that are covered by these requirements include:

a. Earth-to-Orbit (ETO) systems, including launch vehicles and entry vehicles, reusable launch vehicles, or any vehicle operating in the launch and/or landing phase;

b. Space Station (SS) systems, including space flight systems operating exclusively in a low Earth orbit environment;

c. Beyond Earth Orbit (BEO) systems, including space flight systems that operate away from the Earth and beyond easy access for on-demand logistics resupply or crew escape;

d. Crew Rescue Systems, including space flight systems planned for emergency or other nonroutine entry;

e. Crew Transfer Systems, including space flight systems used to transfer crews, passengers, and/or hardware between any of the other listed space flight systems;

f. Planetary Surface Systems (PSS) and Surface Transportation Systems including habitats, Extravehicular Activity (EVA) suits, and other support systems;

g. Extravehicular Mobility Units (EMU), space suits, and other stand-alone systems critical to human survival in space; and

h. Planetary Landing and Ascent Vehicles (PLAV) and other space flight systems used to land and ascend from planetary surfaces, including minor planets.

2.2 Design for Human Space Flight

2.2.1 The space flight system shall be designed, built, inspected, tested, and certified specifically addressing the requirements for human rating as defined in this document.

In addition to system and subsystem testing to ensure that design requirements are achieved, components should be qualification 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, as applicable. Military Standard 1540, Test Requirements for Launch, Upper-Stage and Space Vehicles, dated September 1994, or equivalent component qualification and acceptance testing standards should be used as guidelines. The use of dedicated qualification components is recommended. Flight components should be 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 should be developed by the program. This reference to component qualification and acceptance testing is necessary to emphasize crew and passenger safety requirements, but the discussion is also applicable to other requirements for safety and mission assurance/objectives. Systems requiring incremental assembly in or BEO should 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. Testing should be carried out with software possessing flight functionality and flight hardware in flight configuration. Priority should be 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 should be accomplished.

2.2.2 The design of the space flight system shall address the aspects of human rating beginning in the formulation phase.

Spacecraft and other space flight systems intended to support humans have significantly different characteristics from other aerospace vehicles such as aircraft, and it is essential that the design of a human-rated space flight system fully account for these differences. While space flight systems design is built upon decades of aircraft experience, the unique operations and environments of the space flight systems missions lead to a different and even more stringent set of design requirements. Historically, human rating was accomplished through the use of aircraft safety factors instead of the lower safety factors typical of unmanned military launch vehicles, eliminating single failure points, and providing escape systems to rescue the crew 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 should ensure the integrity of the system design to meet human-rating requirements.

2.2.3 The space flight system design shall incorporate NASA Standard 3000, Manned Systems Integration Standards, for all microgravity and zero-G human system interfaces, including those required for on-orbit maintenance.

NASA has developed life-support systems requirements that encompass all habitable space environments inclusive of the preflight, in-flight, and postflight 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 required for optimal human performance. 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 (ISS), and multiple extravehicular suited programs. Long-duration space flight requirements are derived from NASA's Lunar, Skylab, Extended Duration Orbiter, ISS, and Phase One MIR life sciences programs.

2.2.4 The space flight system shall incorporate MIL STD 1472, DOD Design Criteria Standard - Human Engineering, and NASA/TM-2002-210785, Guidelines and Capabilities for Designing Human Missions, for all human flight system interfaces utilized during ground processing, maintenance, and operations as tailored for a specific program.

2.2.5 Crew habitability and life support systems shall comply with JSC 26882, NASA Space Flight Health Requirements.

2.3 Aerospace Design Standards

2.3.1 The space flight system design, manufacture, and test shall comply with JSCM 8080.5, "JSC Design and Procedural Standards Manual."

Emphasis is placed on using established aerospace design standards, since these standards are based on lessons learned regarding the design and operation of space flight systems. The detailed design requirements and practices specified in JSCM 8080.5 shall be incorporated in the design of human-rated space flight systems. Programmatic use of alternative approaches to these practices will have to demonstrate to the CHMO, AA for OSF, and AA for SMA that they are as effective as the accepted methods.

2.3.2 The space flight system design, manufacture, and test should comply with applicable military and aerospace design standards.

Program and project managers should encourage the access to and use of the NASA Headquarters Office of the Chief Engineer Web site (http://www.hq.nasa.gov/office/codea/codeae/tech_stan.html), 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 should be incorporated in the design of human-rated space flight systems. Programmatic use of alternative approaches to these practices will have to demonstrate that they are as effective as the accepted methods.

2.4 Flight Test

2.4.1 A comprehensive flight test program shall be completed to validate predicted flight environments, flight control characteristics, critical design parameters, preflight analysis, and analytical math models, to verify the safe flight envelope and to provide a performance database prior to the first operational flight.

No space flight system can be certified on the basis of analysis alone. 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. Therefore, a flight test program must be performed to provide two critical functions. First, the flight test program is used to verify the integrated performance of the space flight system hardware and software in the operational flight environment. Second, the flight test program is used 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.

2.4.2 A comprehensive flight test program shall be defined as either a flight test program conducted across the entire mission profile and/or a series of tests encompassing all elements of the mission profile under actual or high-fidelity simulated conditions.

Whenever possible, the flight test program should be conducted across the entire mission profile. A sufficient number of flights should be flown such that the flight test data for the analytical math models can be extrapolated to predict the performance of the space flight systems at the edges of the operational envelopes and to predict the margins of the critical design parameters. This is generally possible for systems with discrete mission profiles of manageable duration such as ETO and crew rescue space flight systems. These systems can usually be operated through several complete ascents, orbital transfers, and/or descent profiles and should give good confidence in the suitability of the design for the planned mission. 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 required. For an SS or BEO space flight systems, flight test across the entire mission profile is not feasible. Limited testing, backed with extensive analyses and simulation, may be used in these cases to verify space flight systems performance across the integrated mission profile. EMU's or other systems, including those that have a self-contained propulsion system, should also be flight tested throughout the expected flight envelope.

2.5 System Safety and Reliability

2.5.1 System Safety

2.5.1.1 In accordance with NPG 8715.3, NASA Safety Manual, latest revision, a systematic program for system safety and human health shall be established to identify, analyze, track, and eliminate or mitigate hazards throughout the lifetime of the program.

2.5.1.2 If a hazard cannot be eliminated, the space flight system shall be designed to preclude the occurrence of a hazard or to negate or reduce the likelihood and effect of the hazard.

2.5.1.3 The program shall establish a rigorous health, safety, and reliability process using qualitative and quantitative tools (such as Hazards Analysis, Fault Tree Analysis, Probabilistic Risk Assessment, Human Error Analysis, and Failure Modes and Effects Analysis) for risk identification and control including a formal review process.

2.5.2 Software Safety

2.5.2.1 Software safety shall be an integral part of the overall system safety and software development efforts associated with human-rated space flight systems.

2.5.2.2 The requirements in NASA Standard 8719.13A, Software Safety NASA Technical Standard, or equivalent, shall be followed to implement a systematic approach to software safety as an integral part of the overall system safety program.

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 should be developed and address the following: computer-based control system software requirements that should be applied regardless of function; requirements that must be met in 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, ISS program.

2.5.3 Failure Tolerance and Reliability

2.5.3.1 All human-rated space flight systems shall be designed so that no two failures shall result in permanent disability or loss of life.

a. Failure tolerance is a term frequently used to describe minimum acceptable redundancy, but it may also be used to describe two similar 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. Where necessary, system design should incorporate cross strapping, failure tolerance, failure detection, and failure recovery capabilities to minimize the negative consequences of failures.

b. System design for reliability is a definitive element of space flight system design. Space flight system hardware is designed for inherent reliability at the component level, but the architecture of the system must also protect against random failures and minimize the probability of loss of mission, space flight 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 flight systems with longer missions and/or more time for recovery from failures, maintenance and logistics resupply are critical.

c. For ascent and descent space flight systems, the time constraints of the dynamic flight modes may preclude the opportunity to use in-flight maintenance and system reconfiguration to recover from failures. Therefore, two-failure tolerance is a critical element in ensuring adequate space flight systems reliability. Elements that are designed for minimum risk (such as primary structure, and pressure vessels) are excluded from failure tolerance requirements.

d. In the case of BEO space flight systems, it is unlikely that resupply space flight systems can supplement the resources aboard the space flight systems unless that capability was planned for in advance through pre-positioned spares. Therefore, safe operation of the space flight systems requires that sufficient reliability be achieved through a combination of reliable hardware design, installed redundancy (both similar and dissimilar), and logistics capability to support maintenance.

e. For long-duration missions, maintenance and system reconfiguration may be used to restore redundancy to the failed functions. For long-duration missions such as on a SS or a BEO space flight system, failure tolerance and functional redundancy are not sufficient since NASA cannot fully predict failure rates, causes, or environments. For these missions, multiple failures are expected, and the response must include maintenance and system reconfiguration to restore the failed functions. In the case of an SS, the maintenance capability and associated logistics inventory need only support critical systems until the arrival of the next resupply vessel. This is likely to be a period of a few

weeks to several months. Maintenance may be considered as an additional level of redundancy beyond two-failure tolerance when mission operations, time criticality, and logistics allow it.

2.5.3.2 All human-rated space flight systems shall be designed so that neither two human errors during operation or in-flight maintenance nor a combination of one human error and one failure shall result in permanent disability or loss of life.

2.5.3.3 The program shall consider tailoring requirement 2.5.3.1 if:

a. **It can demonstrate that two-failure tolerance is either impractical or negatively impacts overall system reliability, and**
b. **Test data, hazard analyses, and comprehensive risk analyses together provide certainty that the system will have a very high reliability without two-failure tolerance.**

Impractical refers to cost prohibitive. Certainty that a system will have a high reliability refers to demonstration of high confidence. Very high reliability is reliability consistent with the accepted crewed aerospace industry standard at the time of each program's initiation.

2.5.3.4 The program shall consider tailoring requirement 2.5.3.2 when:

a. **Error prevention has been demonstrated either to be impractical or negatively impact overall system reliability, and**
b. **Test data and comprehensive risk analyses demonstrate that the system will provide personnel with the capability to detect and recover from errors prior to significant injury or death.**

2.5.3.5 All human-rated space flight systems shall be designed so that the interaction of the components operating as specified (including software) does not result in a permanent disability or loss of life.

2.5.3.6 Emergency systems (such as fire suppression and crew escape) shall not be considered to satisfy failure tolerance requirements; however, these systems may be utilized in evaluation of failure mitigation and in reducing probability of loss of life.

2.5.3.7 As a defense against common cause failure, use of dissimilar redundancy shall be assessed in the design of critical functions.

2.5.4 Crew survival

2.5.4.1 As part of the design process, program management (with approval from the CHMO, AA for OSF, and AA for SMA) shall establish, assess, and document the program requirements for an acceptable life cycle cumulative probability of safe crew and passenger return. This probability requirement can be satisfied through

the use of all available mechanisms including nominal mission completion, abort, safe haven, or crew escape.

2.5.4.2 The cumulative probability of safe crew and passenger return shall address all missions planned for the life of the program, not just a single space flight system for a single mission.

The overall probability of crew and passenger survival must meet the minimum program requirements (as defined in section 2.5.4.1) for the stated life of a space flight systems program (the predeclared time period or number of missions over which the system is expected to operate without major redesign or redefinition). This approach is required to reflect the different technical challenges and levels of operational risk exposure between the various missions. For example, the large number of expected launch operations in the ETO mission represent fundamentally different risks than conducting the first BEO mission to Mars. Single mission risk on the order of 0.99 for a BEO mission may be acceptable, while considerably better performance, on the order of 0.9999, is expected for a reusable ETO design that will fly 100 or more flights.

2.5.4.3 A systems engineering model to estimate and allocate component, subsystem, and human reliability factors shall be developed, maintained, and used throughout the development of the system.

The allocation process should begin early in order to guide the program management and engineer in design trades throughout the design phase. Inclusion of reliability estimation and allocation during system definition facilitates timely and effective decisionmaking before critical design solutions are precluded. Reliability allocation should be used to assign the reliability requirement for complex systems to lower levels and provide insight into fundamental design and architectural requirements to meet system goals.

2.5.4.4 All critical flight systems shall be designed to provide an indication of a failure of a critical system/component, including fault detection and isolation, and the means to preclude a catastrophic safety risk to the flight crew.

The failure, detection, isolation, recovery, and prognostics approach should be used to maximize the potential to identify component failures that endanger the flight crew and allow for the isolation and recovery of the system, if possible.

2.5.4.5 All space flight systems shall be designed to ensure accessibility to vital equipment involved in immediate and followup action to effect emergency recovery of the space flight system, such as, but not limited to, spacecraft compartment pressurization, life support, and emergency systems.

2.6 Abort and Crew Escape

2.6.1 The capability for rapid crew and occupant egress shall be provided during all prelaunch activities.

2.6.2 The capability for crew and occupant survival and recovery shall be provided on ascent using a combination of abort and escape.

2.6.3 The capability for crew and occupant survival and recovery shall be provided during all other phases of flight (including on-orbit, reentry, and landing) using a combination of abort and escape, unless comprehensive safety and reliability analyses indicate that abort and escape capability is not required to meet crew survival requirements.

2.6.4 Determinations regarding escape and abort shall be made based upon comprehensive safety and reliability analyses across all mission profiles.

a. Crew escape systems are required on ascent, regardless of analytical risk assessments, due to the highly dynamic nature of the ascent flight regime and the increased likelihood of catastrophic, uncontainable failures. Crew escape is also required to offset the uncertainty associated with verification of high probabilities of safe crew and passenger return.

b. An intact abort provides for the recovery of the space flight system and its crew and occupants to a suitable site without exceeding stability and control, structural or thermal limits of the system, or cognitive or physiological limits of the crew. Intact abort is the preferred alternative when a successful mission is not possible because it permits the safe recovery of the crew, passengers, and space flight hardware for various levels of system malfunction that do not require crew escape. A contingency abort provides for the recovery of the space flight system and its crew and passengers while potentially exceeding certified limits of the system. The design of intact and contingency abort modes should remain within the performance envelope of the crew escape system, if applicable, to address additional system failures or other problems during the abort trajectory.

c. The reliability, abort, and escape requirements, as defined in this document, may result in different design solutions for the different mission scenarios, levels of risk exposure during a mission, and system architectures. See Appendix D for mission-specific implementation guidance.

2.7 Flight Termination

Any flight termination system (such as range safety system) for human-rated launch vehicles shall include design features (such as thrust termination), which allow sufficient time for safe human escape prior to activation of the destruct system.

A flight termination system will most likely be required for ETO space flight systems (including BEO space flight systems launched intact) that cannot demonstrate sufficiently low hazard to the public throughout the launch phase. Range safety and flight termination requirements are dictated by the Eastern and Western Range Safety

Regulation, EWR 127-1, for Government launch complexes, and the Federal Aviation Administration for commercially licensed facilities. Flight termination systems that do not require the destruction of the space flight systems are preferred for space flight systems that carry humans to space. However, regardless of system requirements, the flight termination system should be designed to work in concert with the human escape system to maximize the capability for the safe return of the humans on board without endangering people on the ground.

2.8 Proximity Operations

2.8.1 Space flight systems operations in proximity to, or docking with, a human space flight system shall comply with joint system requirements (both space flight and operational).

Space flight systems operations in proximity to another space flight system constitute a significant hazard to both vehicles. Therefore, the design and operation of both space flight systems must be compatible with and responsive to the unique requirements of proximity operations.

2.8.2 The autonomous approaching vehicle shall permit safety-critical commanding from the human space flight system, including the abilities to station-keep, separate, and breakout from the proximity operations at any time, without violating the design and operational requirements of the human space flight system.

Specific requirements are unique to space flight systems and missions but should address the following: human Situational Awareness (SA) and ability to monitor and control; docking mechanisms and mating hardware; interspace flight systems communications; power; software; command and telemetry; trajectory monitoring, and attitude control; remote station-keeping, separation, and breakout commanding for uninhabited space flight systems and external environments including pluming, contamination, induced structural loads, electromagnetic interference, and thermal. Example references for these requirements include the Interface Definition Document for ISS Visiting Vehicles, SSP 50235, January 1998, and the Rendezvous and Proximity Operations Design Reference for the ISS, JSC 27240, May 1999.

2.8.3 Designs shall provide a manual capability to monitor and conduct proximity operations, docking, and undocking.

This requirement does not preclude autonomous operations.

2.9 Analysis and Assurance of Critical Functions

2.9.1 The program shall identify and document, in the Human-Rating Plan, a specific set of critical functions to ensure human safety during each phase of the mission.

A specific set of critical functions is required to ensure human safety and mission success during each phase of the mission. Priority should be given to those functions required to provide a safe return of the crew and passengers and protect ground processing personnel and the public. The set of critical functions will vary with the mission (such as ETO, BEO, and the phase of the mission). For example, a different set of functions is required for an Earth-Orbiting SS than for a planetary surface mission. Likewise, a different set is required to safely return a crew from the cruise portion of a mission to Mars than that required during the descent to landing phase. The human-rating plan must describe critical functions required to meet system and program safety requirements by mission phase and design features to ensure their availability.

2.9.2 The program shall incorporate critical functions, defined in the human-rating plan, into the design documentation prior to the Preliminary Design Review (PDR).

This set of critical functions should be specifically identified early in the system design phase to ensure all potential mission scenarios have been identified. For example, in the case of an Earth Orbiting SS, human return and/or safe haven functions provide for the safety of the crew and passengers, while attitude control and reboost, which prevent unplanned reentry, are required to ensure the safety of the vehicle and the public. Additional core vehicle functions are required to ensure the safety of the crew and passengers if human return capability is not provided or employed. Thus, the provision of robust human return capability shifts the minimum critical functionality required of the SS to that required for vehicle and public safety. A matrix of these functions and how they will be ensured should be provided in design documentation early in the system design phase such as a program PDR. The matrix should include function performance criteria that demonstrate the ability of the function to meet the system performance requirements through analysis, test, and inspection.

2.10 Human-in-the-Loop Requirements

2.10.1 A crew station, or equivalent capability, shall be provided to allow the crew to monitor and operate the vehicle appropriate to the flight phase system and function.

Final crew station configuration will be dependent upon specific mission objectives and requirements. While the majority of space missions should 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.

2.10.2 The space flight system shall provide the flight crew and ground crew with insight into vehicle performance and the capability for flight crew and ground crew intervention appropriate to the flight phase, system, and function.

Within the context of this requirement, "insight" is defined as the ability to determine where the vehicle is, its condition, and what it is doing. Insight helps to build SA. Good SA improves the performance of the human operator and enhances the mission.

2.10.3 The space flight system shall provide feedback for all human commands to the flight crew and, where applicable, ground crew.

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.

2.10.4 The space flight system shall provide the flight crew with the capability to reverse or correct inputs where feasible.

The technology of displays and controls design has made tremendous progress in recent years, and the state of the art should be applied to the human interface to minimize crew workload and errors. The number of successful autonomous vehicles designed to perform complex space missions is small. 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 flight 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 flight 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. Military aircraft experience has demonstrated that these capabilities provided to flight crews have made a difference in aircraft recovery during emergency situations. Flight crew contribution is increased as capabilities are provided.

2.10.5 Minimum Crew Intervention Requirements

2.10.5.1 Flight Path and Attitude

2.10.5.1.a The control of vehicle flight path and attitude, during dynamic phases of flight such as ascent and entry, shall be provided by independently developed and redundant software systems.

2.10.5.1.b The crew shall have the capability to select between two independently developed versions of flight control software systems during flight.

During automated and manual control of the vehicle flight path and attitude during dynamic phases of flight such as ascent and entry, the crew shall have the ability to select between two independently developed and tested versions of the flight control software. In addition, selecting the backup version of the flight control software should not corrupt

the primary version. The crew shall have the ability to select either version at any time during dynamic flight.

2.10.5.1.c On orbit and during entry, manual control of vehicle flight path and attitude shall be provided, where vehicle structural, thermal, and performance margins allow.

2.10.5.1.d On ascent, manual control of the vehicle flight path and attitude shall be provided where vehicle structural, thermal, and performance margins allow.

2.10.5.2 Control of Automated Functions

The design shall allow the human operator to override higher level software and automation (such as configuration change and mode change), and the transition from software/automation to manual control will not adversely impact vehicle safety.

The design should include the critical information necessary to provide the crew with SA and the capability to safely transition from an automated state to a manual state without loss of critical function or vehicle control during the transition itself.

2.10.5.3 Control of Subsystem Configuration

2.10.5.3.a The space flight system shall be designed to provide the capability to the crew to monitor and control the vehicle functions critical for safety of flight.

Determining the level of crew control over individual functions is a decision that must be made separately for specific vehicles. At a minimum, the crew should have 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 should be offered to the crew where the crew can be a viable part of the system design and perform that function. For example, a crewmember probably should not have control of individual valves that meter the flow of propellant to the engines, but a throttle which incorporates multiple valve movements to achieve a desired end state (reduce or increase thrust) would be required. This requirement may or may not imply a need for discrete mechanical switches. A simple, intuitive software interface may satisfy this requirement.

2.10.5.3.b The space flight system shall provide the capability to the crew to monitor and control subsystems that directly interface with the crew and, therefore, could impact crew effectiveness.

The crew should have control over those systems that directly affect the performance of the crew such as cabin temperature, cabin exterior/interior lighting, and radio volume, so that, within the capabilities of the subsystem, crew performance can be optimized. The displays should 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.

2.10.5.4 Selection/Initiation of Abort

The flight crew shall be able to select and initiate abort modes.

This requirement does not preclude automatic initiation of an abort system, as long as an override capability is provided per the Control of Automated Functions requirement in section 2.10.5.2. Consideration should be given and human factors accommodations made to address the changes in the environment likely to exist when an abort situation occurs.

2.10.5.5 Selection/Initiation of Escape System

2.10.5.5.a The flight crew shall be able to initiate the escape sequence.

2.10.5.5.b The ground crew shall be able to disarm the escape system by some mechanical means (such as a pin, handle, or lever lock), which guarantees the system is safe.

2.10.5.5.c The flight crew shall be able to disable/inhibit the automated initiation of the crew escape system.

2.10.5.5.d The flight crew should be able to override automatic initiation sequences.

An escape system offers another layer of safety to the crew, much like an ejection seat in a fighter aircraft. Manually arming/disarming the system allows for ground personnel and crewmembers to be seated and work around the cabin area when crew escape is not warranted. The crew must have the ability to override automated crew escape initiation when the system is not functioning properly, or a regime is entered where the automated system may not make sense. None of these requirements is intended to preclude automatic initiation of an escape system. It is desirable for the 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 must occur rapidly to save the crew, and the crew may not have time to override the initiation. When assessing the changes in environment likely to occur in an abort situation, program managers should address human factors accommodations.

2.10.6 The safety of the flight crew shall not depend on communication with or real-time support from the ground and other space flight systems.

Autonomy from the ground is achieved through the ability of the flight crew to make decisions when input from the ground is unavailable or incomplete, or when the situation is time-critical. All mission phases must provide human insight, intervention capability, and control over spacecraft automation if there are people on board or when operating in close proximity to another spacecraft. Decisionmaking aids and/or expert systems that

provide detailed information concerning potential system failure and recovery modes should be available when the ground support cannot be reached.

2.10.7 Flight crew interactions with interfaces and all tasks required of the flight crew shall be designed to meet a workload rating of 3 or better on the Bedford Workload Scale, or the Modified Cooper-Harper Scale, or equivalent workload scales used to evaluate flight crew workload.

The performance of the crew-vehicle interface can be measured in terms of workload, performance, and errors. Crew and vehicle interfaces shall be developed following accepted methods and standard practices, including concept development, rapid prototyping, and structured usability testing with flight crew involvement (see section 2.10.9). 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 crew interface should be designed at a workload rating of 3, 2, or 1 on the Bedford Workload Scale (Figure 2.1) or the Modified Cooper-Harper Rating Scale (Appendix E), or their equivalents. The workload should meet these requirements even for off-nominal situations.

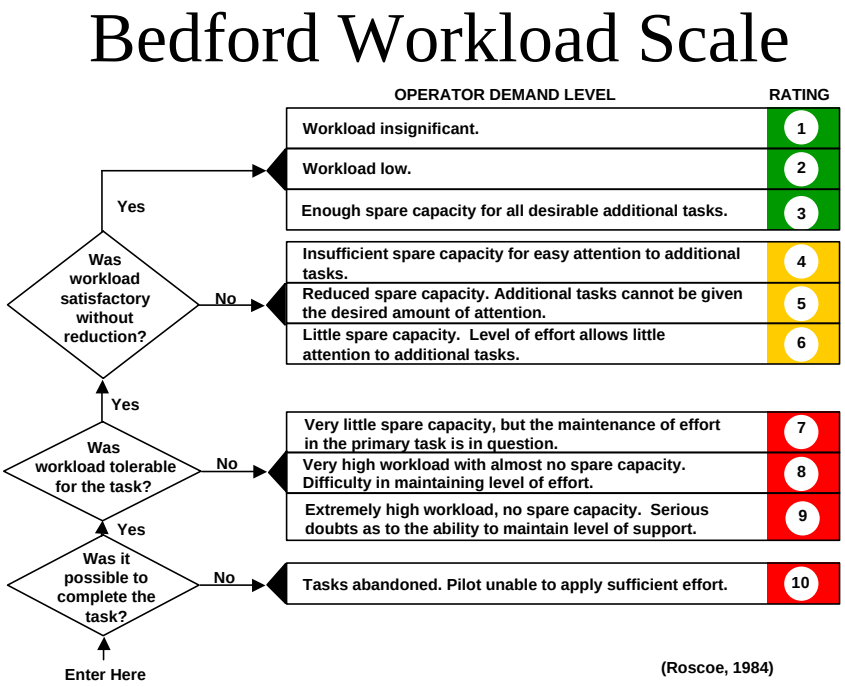


Figure 2.1 - Example of workload rating scale.

2.10.8 During periods of human-in-the-loop flight path and attitude control, the vehicle shall exhibit Level I handling qualities as defined by the Cooper-Harper Rating Scale, or equivalent.

To maximize flight crew performance in areas where vehicle maneuvering is required, the spacecraft should exhibit Level I control qualities as measured using the Cooper-Harper Rating Scale (NASA TND-5153). Level I handling qualities should be available in all nominal phases of flight and most off-nominal situations. However, certain failures which degrade flight control surfaces or engine gimballing may result in handling characteristics which are worse than Level I. In these cases, handling qualities should be no worse than Level II to be considered a reasonable method for crew and vehicle survivability. (See Appendix E.)

2.10.9 Human factors engineering shall be applied to the flight human-system interfaces for ground personnel and flight crew to ensure the system will operate within human performance capabilities.

Attention must be applied to the human-machine 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, should comply with applicable standards such as MIL-HDBK-1797. Designing the crew and machine interface should also include iterative prototyping and usability evaluations with direct crew involvement.

2.10.10 The overall system and mission design, including task design, procedures, and scheduling, shall not adversely affect the ability of the crew to successfully operate the spacecraft.

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 crews. This is accomplished through system architecture being developed in parallel with, and with consideration to, the operations concept of the vehicle to include the specific mission and task design. Attention must be paid to the human-machine interface to minimize workload, to reduce human error, and to make the interaction with the system as user-friendly as possible. Mockups and simulators should 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 should be evaluated under realistic scenarios, nominal and off-nominal, to ensure they support the safety and reliability requirements of this document. Mission tasks cannot be scheduled at such a pace that will result in the degradation of crew performance. This requirement is not intended to discourage a high-tempo of operations, but should result in the considerations of all factors that can adversely impact crew performance.

2.10.11 Human performance criteria and system usability requirements shall be established to ensure crew safety.

2.11 Systems Test and Verification

2.11.1 The program shall verify space flight systems reliability and safety by test and analysis at the integrated system level prior to the first flight with humans on board.

Verification of the reliability performance requirement by testing in applicable environments is preferred over analysis for all critical systems and should be accomplished to the maximum extent possible.

2.11.2 The program shall develop and implement a formal process to maintain the human-rating certification for the life of the program.

This requirement may be accomplished by a combination of system health checks, inspections, and examination of the prior flight history of the components. The program's effectiveness in maintaining the certification should be continuously verifiable.

2.11.3 Structured usability testing with crew involvement shall be completed to verify that the system design meets the required human performance criteria during system operation, maintenance, and control.

2.11.4 Software Testing

2.11.4.1 The performance, security, and reliability of all critical software across the entire flight envelope, as well as mission functions, modes and transitions, shall be tested, verified, and validated.

2.11.4.2 The testing facility shall use a flight-equivalent avionics test-bed operating in a real-time, closed-loop test environment.

2.11.4.3 Ground software shall be tested on the computer platforms that will be used to support flights.

2.11.4.4 The development of all flight and ground software should comply with aerospace software development standards, such as IEEE/EIA 12207 – Information Technology, Software Life-cycle Process (12207.0 – S/W Life-cycle Processes, 1207.1 – Life-Cycle Data, and 12207.2 – Implementation Considerations).

2.11.4.5 The program shall confirm the integrity of the software design and testing process through independent verification and validation methods (NPD 8730.4, Software Independent Verification and Validation (IV&V) Policy).

This 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 reliability of today's aerospace space flight systems and, as such, all critical software must 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 loss of the space flight system or crew and passengers. This includes the flight software as well as ground software that can affect flight safety.

2.11.4.6 The program shall verify that the critical functions defined in the human-rating plan have been implemented in the design at the Critical Design Review (CDR).

Chapter 3: Compliance and Certification

3.1 Human-Rating Certification

3.1.1 Human-rating certification of space flight systems is the authorization granted by the AA for OSF to operate the space flight vehicle within its prescribed parameters for its defined missions as described in the program human-rating plan.

3.1.2 The program manager shall develop a human-rating plan for the human space flight system to include those areas outlined in paragraph P.2, Applicability, of this NPG. The human-rating plan should identify items and areas to be surveyed and provide a summary of the requirements that must be satisfied to achieve and sustain certification. The plan need not be a stand-alone plan provided it meets the requirements set forth in this document (at a minimum, all "shall" statements shall be addressed). The human-rating plan may be incorporated into the program plan developed through NPG 7120.5, latest revision.

3.1.2.1 **Initial Human-Rating Plan Submission** - The program manager should submit a request to the AA for OSF for initial certification. The submission package shall include the human-rating plan, description of the space flight system, reference missions, system safety program plan, and maintenance plan (necessary to ensure the system does not degrade through use, age, or exposure to the environment).

3.1.2.2 **Sustaining Certification** – To maintain certification, the space flight system must be operated and maintained in the "as-certified" condition. The length of a certification shall be documented in the program's Human-Rating Plan.

3.1.2.3 **Recertification** - If the space flight system undergoes major modifications or any changes to mission or environment, the program manager must update the human-rating plan and identify all the changes that impact system risk. The updated information must be submitted to the AA for OSF, and the vehicle must be recertified prior to flight.

3.1.2.4 **Suspension of Certification** – With significant failures or if during independent assessments and/or audits, deficiencies are identified in the approved design, operation, and/or maintenance of the space flight system, the AA for OSF can suspend the space flight system certification, thereby prohibiting use of the system until compliance is reached and/or prohibition has been resolved.

3.1.2.5 **Reinstatement of Certification** - The AA for OSF will reinstate human-rating certification when the cause of the suspension has been thoroughly investigated and satisfactorily corrected, and it has been established that there is maximum reasonable assurance that a failure will not imperil the flight crew or occupants and that personnel may be recovered without a disabling injury if there is an accident.

3.2 Certification Documentation Submission Requirements

Appendix C addresses program life cycle timeframe requirements for draft human-rating plan submittal, NASA Headquarters approval/disapproval, final human-rating plan approval and baseline, human-rating certified design, and certification renewal frequency.

3.3 Program Compliance

3.3.1 All NASA human space flight systems development programs shall incorporate plans for human rating beginning with the System Requirements Review (SRR).

3.3.2 All programs shall demonstrate compliance with the language and intent of this document at the PDR and at other milestones as defined in the human-rating plan.

3.3.3 All programs shall demonstrate compliance with these human-rating requirements and obtain certification from the AA for OSF prior to first operational flight and first flight with humans onboard.

3.3.4 All programs shall develop a process to ensure compliance throughout the life of the program.

3.4 Requirements Tailoring, Deviations, and Waivers

3.4.1 Since space flight systems, missions, and environments vary significantly, all of the human-rating requirements may not be applicable to each. When a program manager for a specific human-rated space flight system believes a requirement does not apply, the program and project manager may tailor out that requirement. All proposed tailoring of requirements and justification shall be documented in the program human-rating plan that is submitted to NASA Headquarters for approval by the AA for OSF, with concurrences by the AA for SMA and the CHMO.

3.4.2 When a program manager for a specific human-rated system believes a requirement applies, but cannot be accomplished, or can be satisfied by alternate methods, the manager may request a deviation to that requirement. All proposed deviations shall be documented, with sound technical rationale, in the program human-rating plan submitted to NASA Headquarters for approval by the AA for OSF, with concurrences by the AA for SMA and the CHMO.

3.4.3 After program human-rating plan approval, all deviation and waivers may be implemented by the program manager where sound technical rationale exists, but those deviations and waivers shall be presented to the AA for OSF, the AA for SMA, and the CHMO at the major program milestone reviews (See Appendix C). At a minimum, they should be presented at the PDR, CDR, Systems Acceptance Review (SAR), Test Readiness Review (TRR), and FRR. Note: The SRR would be completed prior to final program human-rating plan approval.

Appendix A: Additional References

Advanced Avionics Architecture & Technology Review – Phases 1 & 2, Joint Aeronautical Commanders Group, AAATR811, 21 January 1997.

EWR 127-1, Range Safety Policies and Procedures, latest revision.

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.

JSC 13956, NASA Medical Operations Requirements Document for Space Shuttle, latest revision.

JSC 16785, NASA Medical Operations Readiness Review Plan.

JSC 23211, Proposed Standards for Human-Rating Space Systems, by Mary Cerimele, et al., October 1992.

JSC 26895, Guidelines for Assessing the Toxic Hazard of Space Flight Systems Chemicals and Test Materials, October 1997.

JSC 27240, Rendezvous and Proximity Operations Design Reference for the ISS, latest revision.

JSC 27735, Space Medicine Monitoring and Countermeasures Project Plan, February 1997.

MIL-HDBK-1797, Flying Qualities Of Piloted Aircraft, latest revision.

NASA-TMX-65284, Safety Requirements for Man-Rating Space Systems, 8 November 1968.

NPG 1441.1D, NASA Record Retention Schedule.

NPD 2820.1, NASA Software Policies.

NPD 7100.8D, Protection of Human Research Subjects.

NPG 8000.4, Risk Management Procedures and Guidelines.

NPD 8900.1F, Medical Operations Responsibilities in Support of Human Space Flight Programs.

NPD 8900.3F, Astronaut Medical and Dental Observation Study and Care Program.

NSTS 08080-1, Space Shuttle Manned Space Flight Systems Criteria and Standards, 30 June 1992.

NSTS-12820, NASA Mission Operations Directorate Operational Flight Rules, Volumes A, B, C, & D, latest revision.

QS-22A-LSK, Flight Crew Emergency Egress Escape and Rescue.

A Perspective on the Human-Rating Process of U.S. Space Flight Systems: Both Past and Present, George Zupp, ed. NASA Special Publication 6104, February 1995.

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.

SSP 50005, ISS Flight Crew Integration Standard.

SSP 50038, Computer-Based Control System Safety Requirements - International Space Station Program, latest revision.

SSP 50235, Interface Definition Document for ISS Visiting Vehicles, latest revision.

Appendix B: Definitions

B.1 **Abort**: The successful recovery of the space flight system and its crew and passengers in the event of an anomaly that precludes mission continuance. One type of abort (intact) allows recovery without exceeding stability, control, thermal, or physiological limits, and the other type (contingency) may result in exceeding system limits in the process.

B.2 **Breakout**: During proximity operations, the ability to maneuver one or more vehicles to a safe separation distance.

B.3 **Catastrophic Hazard:** A condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or major systems or vehicle destruction during the mission.

B.4 **Certification:** The comprehensive evaluation of the technical and nontechnical features of a system and other safeguards, made as a part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified requirements.

B.5 **Contingency Abort:** Designed to permit flight survival following severe failures when an intact abort is not possible.

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

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

B.8 **Crew Escape:** The successful recovery of the space flight system crew and passengers in the event of an anomaly that precludes mission continuance. The space flight system in this scenario is abandoned and presumably lost.

B.9 **Crew Survival:** Capability and ability to keep the crew alive.

B.10 **Critical Functions:** Capabilities or functions that are essential to the safety of the public, crew, passengers, and/or vehicle.

B.11 **Critical Software**: Any software component whose failure or unanticipated performance could lead to the loss of the crew and passengers or space flight system. This includes the flight software as well as ground 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 a vehicle system.

B.13 Design for Minimum Risk: A design process or characteristic thereof such that deliberate effort is expended to maximize crew survival. Hazards not controlled by failure tolerance should be controlled by specified margins of safety, factors of safety, material properties, or any other properties inherent to the design of the part, component, subassembly, or assembly.

B.14 Deviation: A variance that authorizes departure from a particular safety requirement where the intent of the requirement is being met through alternate means that provide an equivalent level of safety.

B.15 Fail-Safe: Ability to sustain a failure and retain the capability to safely terminate or control the operation.

B.16 Flight Crew: Any human on board the space flight system while in flight that has been trained to interact with the space flight system; same as crew.

B.17 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.18 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.19 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.20 Human-Rating: The certification that a system has been developed and is capable of being operated in a manner appropriate for use by human crews at minimal risk. Human-rated certification includes: (1) human safety; (2) human performance (both nominal and degraded states of operation); and (3) human health management and care as applicable.

B.21 **Human-Rating Plan:** A formal document outlining the elements and rationale for the human-rating process to be applied to a specific space flight system from SRR to system disposal at end of life. The human-rating plan is to incorporate both requirements and the verification of these requirements.

B.22 **Human-Rating Process:** The process steps used to achieve a human-rated system as defined in **B.19**. 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.23 **Human-Rating Independent Review Team:** An independent group of technical experts tasked with review and concurrence of the proposed requirements, test plans, verification plans, and other program elements that constitute the basis for achieving and maintaining human rating.

B.24 **Intact Abort:** Recovery of the space flight system and its crew and passengers to a suitable location without exceeding stability and control, structural or thermal limits of the system, or cognitive, or physiological limits of the crew.

B.25 **Intervention Capability:** The ability of the crew to assert control over all space flight systems functions in nominal and off-nominal situations.

B.26 **Manual Control:** The ability of the crew to bypass nonessential levels of automation and exert direct control of critical space flight systems functions.

B.27 **Passengers:** Any human on board the space flight system while in flight that has not been trained to interact with the system and has no functional responsibility to perform any mission task for that system.

B.28 **Proximity Operations:** Procedures that govern space flight when two or more vehicles are operating near enough to be affected by the other.

B.29 **Public:** All humans not participating in the space flight activity who could be potentially affected by the function or malfunction of the space flight system.

B.30 **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.31 **Safety:** The minimization of risk from damage or harm to hardware, software, facilities, or humans.

B.32 **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. It is usually associated with long-duration space missions and is usually implemented as a discrete location where the capabilities and environments are provided.

B.33 Space Flight System: A flight hardware and software system whose flight profile is partially or completely outside of the Earth's atmosphere.

B.34 Tailoring: The documentation and approval of the adaptation of the requirements of this document to specific program or project needs. The results of this activity are documented in the Human-Rating Plan and must be approved by the cognizant AA's.

B.35 Test Flight: A flight occurring prior to certification.

B.36 Validation: (1) An evaluation technique to support or corroborate safety 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.

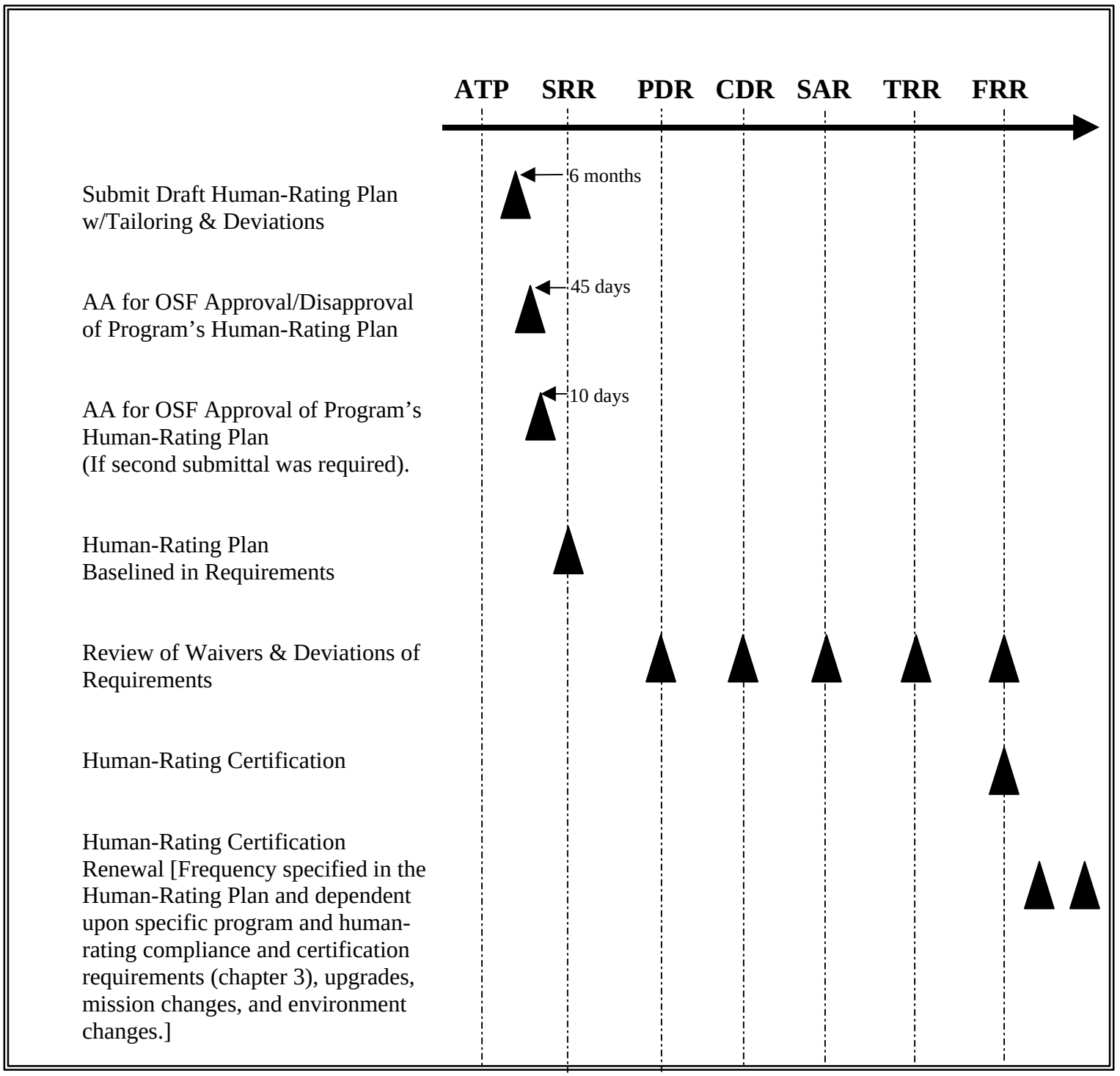
B.37 Variance: Documented and approved permission to perform some act or operation contrary to established requirements.

B.38 Verification: The process of proving or demonstrating that requirements have been satisfactorily met through design and/or operational elements.

B.39 Verification Plan: A formal document listing the specific technical process to be used to show compliance with each requirement.

B.40 Waiver: A variance that authorizes departure from a specific safety requirement where a certain level of risk has been documented and accepted.

Appendix C: Notional Timeline for Program's Human-Rating Certification



Appendix D: Implementation of Reliability, Abort, and Escape Requirements

Earth-to-Orbit (ETO) Space Flight Systems

The nature of the ETO space flight system exposes it to the risk of numerous missions over its lifetime but permits the use of aborts and crew escape systems to increase the probability of crew survival. Experience has shown that for the foreseeable future the reliability of the main propulsion system and other critical systems will limit the overall reliability of the ETO space flight systems. Although benign (contained) failures of engines and other systems during ascent can be dealt with through the use of abort modes, the relatively high probability of catastrophic failure of the main propulsion system utilizing current and expected near-term technology requires the inclusion of a safe and effective crew escape system.

Beyond Earth Orbit (BEO)

BEO missions require unique abort and survival modes. Missions designed for BEO require sufficient power, consumables, and trajectory design to maximize abort capabilities to ensure crew survivability. These abort modes include, but are not limited to, powered return, free return, pre-positioning capabilities, and safe haven. In general, this mission profile requires the space flight systems and its propulsion system to have sufficient propellant to fly off-nominal trajectories. Critical systems should also be designed so that failures do not result in a catastrophic event. The design should 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 should 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. Consideration should be given to pre-positioning consumables, spare parts, and other critical logistics and services to improve abort and safe haven capabilities.

The BEO mission must meet a high probability of safe crew return over the life of the program. However, the higher mission complexity and length is offset by the fact that there may be only a few missions conducted at that level of technical and safety risk. As experience with the mission grows and the possibility of establishing a permanent outpost or colony arises, the reliability goal for each individual mission must rise to account for the increased flight rate and consequent exposure. 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.

Crew Rescue

The crew rescue mission achieves its reliability through appropriate system design for reliability, simplicity of hardware, and failure tolerance. Flight experience has shown

that it is likely to be used at least once during the life of an SS program, most likely due to a medical contingency. Since it may be attached to the SS for extended periods of time and is essential to the SS mission, it should be designed for operational availability on demand and high reliability throughout its on-orbit life. To achieve acceptable levels of reliability and availability, on-orbit checkout and maintenance capabilities may be required.

Since crew rescue vehicles provide emergency escape, traditional abort and escape modes are not applicable. This space flight system must be able to transport severely injured or ill crewmembers, in need of medical evacuation, safely to Earth.

Crew Transfer

The main function of a crew transfer system is to ferry crewmembers to or from space flight systems. Since life support systems aboard a crew transfer vehicle may be limited, abort modes must be provided to allow for the safe recovery of crewmembers.

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). The abort mode provided, for any given failure, should ultimately result in the safe accommodation of the crew.

Non-Crewed Systems

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 should be provided.

Space Station (SS)

An extended SS 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 illness, or crew 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 should be provided at all times through some type of escape vehicle (such as Soyuz or permanently docked ETO space flight systems).

For SS 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 return.

Planetary Surface Systems (PSS)

A PSS is similar to an SS in that it will typically have an extended mission duration, but it differs in that the capability for an immediate crew return will not always be feasible. Therefore, providing a local means of dealing with emergencies is required. In most cases, an immediate evacuation in response to an emergency may not be practical. For these situations, emergency medical and safe haven capabilities must be provided, including remote medical treatment.

Extravehicular Mobility Unit (EMU)

EMU's operate in the vicinity of a larger space system. Therefore, the minimum reliability of the EMU must provide for enough reserve capacity to allow the crewmember to safely return to the larger space flight systems. This reliability must be allocated over the number of required missions of the EMU.

EMU's should include crew self rescue devices worn by each EVA crewmember during all periods when there is no vehicle to credibly rescue an inadvertently detached EVA crewmember. This device could be the Simplified Aid for EVA Rescue or an equivalent capability.

Appendix E: Modified Cooper–Harper Rating Scale