NASA Procedural Requirements

NPR 8705.2B
Effective Date: May 06, 2008
Expiration Date: July 06, 2016

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

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

Responsible Office: Office of Safety and Mission Assurance

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixF | AppendixE | ALL |

Appendix A. Definitions

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

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

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

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

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

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

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

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

Crew/Passenger Escape: See definition for escape.

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

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

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

The following examples are provided for clarification of the definition of crewed space system as it relates to the Human-Rating Certification:

Application example 1: A launch vehicle for a crewed spacecraft on a NASA mission is part of the crewed space

system for Earth ascent. In this example, the Human-Rating Certification applies to the launch vehicle and the spacecraft operating together as a crewed space system during the ascent phase of the reference mission.

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

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

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

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

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

Critical Software: Any software component whose behavior or performance could lead to a catastrophic event or abort. This includes the flight software as well as ground-control software.

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

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

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

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

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

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

Exception: A written authorization granting permanent relief from a specific, non-applicable requirement.

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

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

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

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

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

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

Human Error: Either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence.

Human Error Analysis (HEA): A systematic approach to evaluate human actions, identify potential human error, model human performance, and qualitatively characterize how human error affects a system. HEA provides an

evaluation of human actions and error in an effort to generate system improvements that reduce the frequency of error and minimize the negative effects on the system. HEA is the first step in Human Risk Assessment and is often referred to as qualitative Human Risk Assessment.

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

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

Human-Rated Space System: A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards with sufficient certainty to be considered safe for human operations, and provides the capability to safely recover from emergency situations.

The concept of human-rating a space system entails three fundamental tenets:

1. Human-rating is the process of evaluating and assuring that the total system can safely conduct the required human missions.

2. Human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success.

3. Human-rating includes the incorporation of design features and capabilities to enable safe recovery of the crew from hazardous situations.

Human-rating is an integral part of all program activities throughout the life cycle of the system, including design and development; test and verification; program management and control; flight readiness certification; mission operations; sustaining engineering; maintenance/upgrades; and disposal.

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

Human-Rating Certification Package: See Appendix D.

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

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

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

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

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

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

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

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

Override: To take precedence over system control functions.

Passenger: Any human on board the space system while in flight that has no responsibility to perform any mission

task for that system. Often referred to as "Space Flight Participant."

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

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

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

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

Reliability: The probability that a system of hardware, software, and human elements will function as intended over a specified period of time under specified environmental conditions.

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

Risk: The combination of (1) the probability (qualitative or quantitative) including associated uncertainty that the space system will experience an undesired event (or sequences of events) such as internal system or component failure or an external event and (2) the magnitude of the consequences (personnel, public, mission impacts) and associated uncertainties given that the undesired event(s) occur(s).

Risk Assessment: An evaluation of a risk item that determines (1) what can go wrong, (2) how likely is it to occur, and (3) what the consequences are.

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

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

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

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

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

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

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

Technical Authority: The individual who specifically maintains technical responsibility over establishment of, changes to, and waivers of requirements in a designated area. There are three Technical Authorities: Engineering, Safety and Mission Assurance, and Health and Medical.

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

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

Validation: Proof that the product accomplishes the intended purpose. May be determined by a combination of test, analysis, and demonstration.

Verification: Proof of compliance with specifications. May be determined by a combination of test, analysis, demonstration, and inspection.

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

Waiver: A written authorization allowing relief from a requirement.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixF | AppendixE | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov