STI 10-052

NASA HUMAN-RATING REQUIREMENTS

Frank Groen, Wil Harkins, Michael Stamatelatos

NASA Headquarters, 300 E St. SW, Washington DC, 20546 Email:frank.j.groen@nasa.gov

ABSTRACT

NASA's Procedural Requirements 8705.2B defines the Human-Rating Certification process and related technical requirements for human spaceflight programs developed by and for NASA. The document specifies Agency-level responsibilities related to the certification, processes to be established by the program, and technical requirements.

1. INTRODUCTION

NASA Procedural Requirements (NPR) 8705.2B[1] contains NASA's current Human-Rating requirements. The NPR defines process, procedures, and requirements for the certification of carefully managed missions where safety risks are evaluated and determined to be acceptable for human spaceflight.

The NPR assumes adherence to the high standards of reliability and mission success required for all of NASA's spaceflight missions, which includes compliance with requirements contained in NASA directives that are mandatory for any high value/high-priority space flight program or project conducted by or for NASA. Human-Rating certification goes above and beyond these requirements by requiring that the space system provides the crew with a safe and habitable environment, a level of control over the system, and means of escape from hazardous situations. Certification forces a greater focus on typical safety-enhancing measures such as failure tolerance and safety margins. It also require features unique to crewed space systems, such as abort triggers, logic, and systems, and crew interfaces for the monitoring and (manual) control of the space system.

Beyond establishing these design requirements, the Human-Rating certification process causes the development and operation of crewed space systems to be subject to more scrutiny. This involves a greater role of safety analyses in the design process, a broader scope of such analyses, increased rigor in the validation and verification of standard compliance, and a greater dependence on test flights.

NPR 8705.2B establishes the current Agency-level requirements, which are applicable to the development and operation of crewed space systems developed by NASA used to conduct NASA human spaceflight missions. As was done for NASA's Constellation Program, the requirements are expected to be tailored and refined in Program-level documents specific to the mission and Program's organization. The extent to which commercial crew transportation services to the International Space Station as defined in NASA's 2011 budget request (if approved by Congress) will be expected to comply with requirements contained in or derived from the NPR is currently being debated.

This paper will provide an overview of the requirements contained in the NPR, and addresses some of the lessons learned during application of the standard to the Constellation Program.

2. TENETS OF HUMAN-RATING

NASA's Human Ratings Requirements document (NPR 8705.2B) is based on three key tenets.

The first tenet states that human-rating is the process of designing, evaluating, and assuring that the total system can safely conduct the required human missions. This tenet describes the additional rigor and scrutiny involved in the design, development, certification, and operation of human-rated space systems. Designing a space system, with constraints of mass and volume, often requires compromise to reach a design that can perform the mission, including the safe return of the crew and passengers. In many respects, systems engineering is about managing compromise. The risks associated with each decision must be understood and carefully considered. Throughout the design and development process, the engineering, safety, and health and medical disciplines external to the program must constantly challenge the developers to articulate the rationale for their design decisions. When mass and volume constraints force a compromise, the safest practical option must be selected. Once the system is developed and deployed, additional rigor and scrutiny are applied at every mission readiness review. Development and operation teams continually look for ways to reduce the potential for uncontrolled hazards by exploring potential risks and uncertainties. Reducing the uncertainties in the design and operations, exploring all safety risks, and recognizing the potential for hazards obscured by system complexity are all part of a human-rating mindset.

The second tenet states that human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success. This tenet accounts directly for the presence of humans in the spacecraft or space system. In addition to providing for the basic human needs such as environment, food, and water, the astronauts onboard the spacecraft must be given some level of control over the system. This tenet thus includes all the aspects of flight crew performance necessary for the crew to successfully carry out their mission, without imposing undo risk to the flight crew. Crew situational awareness, crew commanding, cockpit display design and spacecraft environmental factors all are critical factors that affect a crewmember's performance and their ability to safely and successfully operate the system. The same rigor and balance in design trades utilized in tenet one is applied also in tenet two to arrive at the best working environment for the crew that maximizes the probability of mission success, while minimizing the risk to the flight crew.

The third tenet states that human-rating includes the incorporation of design features and capabilities to enable safe recovery of the crew from hazardous situations. The tenet recognizes that the human exploration of space involves inherent risk and, despite our best efforts, the initiation of accident scenarios cannot always be prevented. When mitigation fails and mission continuation is no longer possible, steps must be taken to abort the mission and safely return the crew. When developing spacecraft to carry humans, the design team must incorporate capabilities and safeguards that allow the crew to survive hazardous conditions and safely return the crew.

The objective of the Human-Rating Certification process is to achieve definition and implementation of processes and technical requirements consistent with these tenets. This requires not just that technical standards are complied with, but that Human-Rating considerations are integral to program activities throughout system lifecycle, and that developers are challenged to defend their design decisions.

3. REQUIREMENTS OVERVIEW

The requirements in NPR 8705.2 can be subdivided into three groups:

- A definition of the Human-Rating Certification process and related responsibilities of the Program and other entities in the NASA organization.
- Certification requirements applied to the Program.
- Technical requirements related to system safety, system control, and crew survival/abort.

3.1. Human-Rating Certification Process

The Human-Rating process defines the major responsibilities related to the certification of crewed space systems as human-rated. Human-rating certification can be obtained for the integrated space system and for a specified mission. Certification cannot be obtained for individual elements of the space system, such as launch vehicles, or independent of a defined mission.

A major role in the certification process is assigned to the Program Manager, who is responsible for implementing the certification and technical requirements. The Program Manager summarizes and further documents the results of the human-rating processes at major design reviews.

The Technical Authorities (Engineering, Safety and Mission Assurance, Health and Medical) provide the necessary checks and balances to assure safe and reliable systems. The Technical Authorities, who are independent of the programmatic authority chain, define standards (or areas requiring program-level standards), and disposition requests for relief from such standards. They challenge the developers to describe the rationale for their design decisions and help identify safety risks and safer alternatives. Concurrence by the Technical Authorities is required at major design reviews and before flights.

A further role is defined for the Director of JSC, as a representative of the flight crew. The crew's consent to those risks must be obtained during the development of the space system, and prior to each flight. The NPR requires that the crew is also part of the Human-System Integration team that is responsible for cockpit design and human integration.

Progress of the Program towards Human-Rating certification is reviewed by the Agency at major design reviews. Certification is ultimately issued by the NASA Associate Administrator, with concurrence from the Technical Authorities, crew, and the Mission Directorates that are part of the programmatic authority chain. The certification is issued after ORR, but prior to Flight Readiness Review. Compliance with the certification, and operation within the bounds of the certification, is verified during FRR.

While compliance with directives and standards can provide the framework for safety, the Program Manager is ultimately responsible for providing safe and reliable systems that are safe enough for human missions. Roles related to the acceptance of residual crew safety risks as implied by the NPR are characterized in Figure1. This model is specific to NASA's organization, and consistent with NASA's top-level government policy defined in NPD 1000.0. [2].

The Program Manager is responsible for the formal acceptance of risks, e.g., additional risks that are due to non-compliance with standards. However, the Program Manager can only do so if the Technical Authorities determine that those risks are within an acceptable range. Finally, the Program Manager can only accept such risks if the crew consents (volunteers) to take those risks.

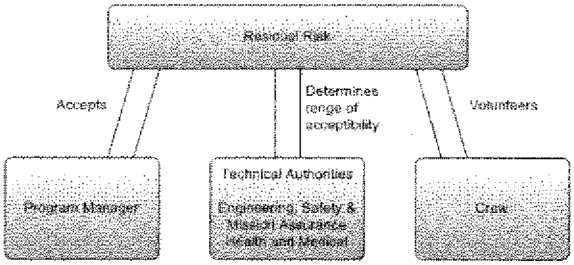

Figure 1: Roles related to the acceptance of residual risk.

3.2. Certification Requirements

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

Early in the certification process, the Program Manager must define the scope of the human-rating activity. This includes a definition of the space system to be human-rated and the mission that the system is to be human-rated for. Human-rating certification is formally applied to the crewed space system, consisting 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 such as launch vehicles. The crewed space system is part of the larger space system used to conduct the mission. The certification process and requirements may affect functions and elements of other mission systems, such as control centers, launch pads, and communication systems.

The certification requirements define required elements of the process for the development and operation of space system implemented by the program manager. This includes the establishment of a Safety and Mission Assurance program, safety analysis processes, the definition of crew survival strategies, and the establishment of processes for the evaluation of human workload and the impact of potential human errors. The human-system integration (hardware and software) for the crewed space system must be lead by a Human-System Integration Team Manager consisting of human-system integration team, consisting of astronauts, mission operations personnel, training personnel, ground processing personnel, human factors personnel, and human engineering experts.

Separate certification requirements require that the outcome of these processes, and the impact that these processes had on the design, be summarized for the major design reviews. For example, one such requirement states that the program must present how the safety analysis activities related to loss of crew were used to understand the relative risks and uncertainties within the design and subsequently influence decisions related to the system design and application of testing. The intent is for the program to show that safety analyses are iteratively used to make design decisions to eliminate hazards, control initiating events or enabling conditions related to hazards, and/or mitigate the resulting effects related to the hazard. The intent is thus not to track all decisions and provide a linkage to the assessment that influenced those decisions; rather, the intent is to summarize how the analyses were used.

Specific elements of these requirements will be discussed in later sections.

3.3. Technical Requirements

Chapter 3 of the NPR contains the technical requirements. The requirements in this chapter consist of design requirements that are specific to systems used for human spaceflight systems consistent with the tenets of Human-Rating. These requirements apply in addition to the requirements contained in technical standards mandated by NASA's Technical Authorities, and four standards called out in the NPR 8705.2B, namely

- NASA-Standard-3000 Volume I - II, Man-Systems Integration Standards.
- NASA-Standard-3001 Volume I, Space Flight Human Systems: Crew Health.
- FAA HFDS - Human Factors Design Standard.
- MIL-STD-1472, Department of Defense Design Criteria Standard - Human Engineering

As the titles suggest, these focus on human-systems integration and crew health.

The technical requirements contained in the NPR identify capabilities in three areas, namely system safety, human control of the system, and crew survival and aborts. The requirements are not intended to be all inclusive or an absolute prescription for human-rating, and compliance with these requirements is not considered to assure a safe system for human missions into space. The technical requirements are intended to provide the foundation of capabilities upon which the Program Manager will build by identifying and incorporating additional unique capabilities for each reference mission, based on an understanding of origins and assumptions behind requirements, as well as history lessons, legacy solutions, expert opinions, and best practices. Specific requirements are listed in Appendix A of this paper. The NPR provides rationale and interpretations for many of the requirements.

Beyond the ability to sustain a safe, habitable environment for the crew, the system safety requirements address failure tolerance, tolerance to inadvertent operator actions and hazardous behavior of critical software, the ability to detect, annunciate, isolate and or recover from faults, ability to utilize health and status data during and after a mission, the ability to perform critical functions autonomously without communication with Earth, and the ability of the crew to access equipment in case of emergencies.

The system control requirements state that the crewed space system must provide the capability for both the crew and mission control (remotely) to monitor, operate, and control the crewed space system and subsystems, where this capability is necessary to execute the mission, prevent a catastrophic event, or prevent an abort. Here, the crew should be able to manually override higher-level software control and automation (such as automated abort initiation, configuration change, and mode change) when the transition to manual control of the system will not cause a catastrophic event.

The crew must have the ability to manually control the flight path and attitude of their spacecraft throughout the mission, with the exception of the atmospheric portion of Earth ascent when structural and thermal margins have been determined to negate the benefits of manual control.

The ability to monitor, operate, and control must also be provided for unmanned vehicles possible during proximity operations where an unmanned vehicle is within the safety zone of a crewed vehicle.

4. FAILURE TOLERANCE REQUIREMENTS

Compared to earlier revisions of NPR 8705.2, revision B modified its approach to the definition of system safety requirements. As the NASA Aerospace Safety Advisory Panel (ASAP) observed [3], rather than relying primarily on redundancy via fixed failure tolerance requirements, NPR 8705.2B seeks a risk-informed design approach in which decisions regarding failure tolerance and other safety-enhancing features are made based on an understanding of the level of safety, and the significance of individual safety risk contributors.

This approach is reflected by requirement 3.2.2 (see Appendix A), which states that the specific level of failure tolerance and implementation is to be derived from an integrated design and safety analysis, with a minimum of one failure tolerant. The requirement is supplemented by requirement 3.2.3 which states that emergency equipment such as fire suppression systems, fire extinguishers and emergency breathing masks, launch/entry pressure suits, and systems used exclusively for launch aborts, may not be counted as part of the system's failure tolerance. The failure tolerance requirement thus pertains to systems and equipment that prevent the initiation of a catastrophic event, rather than mitigate consequences once an initiating event occurs.

As defined in the NPR, safety analysis as intended by NPR 8705.2 combines existing techniques such as Hazard Analyses, Fault Tree Analyses, Failure Modes and Effects Analysis, Damage Modes and Effects Analysis, Critical Items Lists as well as probabilistic risk analyses such as Probabilistic Risk Assessment (PRA) [4], and simulation modeling techniques (e.g., physics-based abort analyses such as those performed for the Ares I vehicle [5]).

The term 'integrated safety and design analysis' then refers to the active and iterative application of such techniques, and the use of the collective results from these analyses to assess and prioritize safety risks of proposed design solutions. Such assessments and prioritizations then serve to inform decisions regarding required levels of failure tolerance and other safety enhancing measures such as margins and abort triggers. This is in contrast to using individual (stove-piped) techniques as assurance tools to verify compliance with deterministic safety criteria such as fixed failure tolerance requirements.

The formulation of this system safety requirement is not without criticism. One critique is that the failure tolerance requirement can be interpreted as a single failure tolerance requirement, and that the burden of proof should be reversed to use the integrated analyses to argue the reduction from a nominal level of failure tolerance (e.g., two). Such reductions could then be made based on findings that they would not lead to significant increases of safety risk. No determination has been made whether the requirement should be changed.

A second critique, voiced by ASAP [3], is that the approach can only be viable if a common understanding of "sufficiently safe" exists to guide design decisions. In the case of the Constellation Program, guidance exists in the form of Loss Of Crew (LOC) probability requirements established by the Program. ASAP argued however that acceptable risk levels, including associated confidence levels, must be defined at the Agency level to ensure consistency across programs, including commercial efforts. In response, NASA is preparing a change to its policy to make the adoption of Agency-level safety goals and associated thresholds part of the Human-Rating certification process.

5. REFERENCES

1. NASA, *Human Rating Requirements for Space Systems,* NPR 8705.2B w/ change 1 (2009)
2. NASA, *Governance and Strategic Management Handbook,* NPD 1000.0A (2008)
3. NASA Aerospace Safety Advisory Panel, *Annual Report for 2009* (2010)
4. NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners* (2002)
5. Mathias, D., Lawrence, S., Go, S., Werkheiser, M., *Engineering Risk Assessment of Ares I,* to be presented at PSAM 10, Seattle (2010)

ACKNOWLEDGEMENT

The authors of this paper want to acknowledge Gary Langford, NASA MSFC for his contributions to this paper.

APPENDIX A: TECHNICAL REQUIREMENTS

Following are the technical requirements contained in Chapter 3 of NPR 8705.2B. The full document, available at http://nodis3.gsfc.nasa.gov/main_lib.html contains rationale for many of these requirements.

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

3.2.2 The space system shall provide failure tolerance to catastrophic events (minimum of one failure tolerant), with the specific level of failure tolerance (one, two or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis (per the requirement in paragraph 2.3.7.1) (Requirement). Failure of primary structure, structural failure of pressure vessel walls, and failure of pressurized lines are excepted from the failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance. Other potentially catastrophic hazards that cannot be controlled using failure tolerance are excepted from the failure tolerance requirements with concurrence from the Technical Authorities provided the hazards are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance.

3.2.3 The space system shall provide the failure tolerance capability in 3.2.2 without the use of emergency equipment and systems.

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

3.2.5 The space system shall tolerate inadvertent operator action, as described in 3.2.4, in the presence of any single system failure.

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

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

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

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

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

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

3.3.1 The crewed space system shall provide the capability for the crew to monitor, operate, and control the crewed space system and subsystems, where: a. The capability is necessary to execute the mission; or b. The capability would prevent a catastrophic event; or c. The capability would prevent an abort.

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

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

a. The remote capability is necessary to execute the mission; or b. The remote capability would prevent a catastrophic event; or c. The remote capability would prevent an abort.

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

3.4.2 The crewed spacecraft shall exhibit Level 1 handling qualities (Handling Qualities Rating (HQR) 1, 2 and 3), as defined by the Cooper-Harper Rating Scale, during manual control of the spacecraft's flight path and attitude.

3.5.1 The space system shall provide the capability for the crew to monitor, operate, and control an uncrewed spacecraft during proximity operations, where: a. The capability is necessary to execute the mission; or b. The capability would prevent a catastrophic event; or c. The capability would prevent an abort.

3.5.2 The crewed space system shall provide the capability for direct voice communication between crewed spacecraft (2 or more) during proximity operations.

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

3.6.1.2 The space system shall provide abort capability from the launch pad until Earth-orbit insertion to protect for the following ascent failure scenarios (minimum list): a. Complete loss of ascent thrust/propulsion. b. Loss of attitude or flight path control.

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

3.6.1.4.1 The space system shall provide the capability for the crew to initiate the Earth ascent abort sequence.

3.6.1.4.2 The space system shall provide the capability for the ground control to initiate the Earth ascent abort sequence.

3.6.1.5 If a range safety destruct system is incorporated into the design, the space system shall automatically initiate the Earth ascent abort sequence when range safety destruct commands are received onboard, with an adequate time delay prior to destruction of the launch vehicle to allow a successful abort.

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

3.6.3.1 The crewed space system shall provide the capability to autonomously abort the mission during lunar transit and from lunar orbit by executing a safe return to Earth.

3.6.4.1 The crewed space system shall provide the capability to autonomously abort the lunar descent and execute all operations required for a safe return to Earth.

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

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

3.6.7.2 The crewed space system shall provide a safe haven capability for the crew inside the spacecraft after Earth landing until the arrival of the landing recovery team or rescue forces.

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