NASA-STD-3001 Technical Brief

Automated and Robotic Systems

OCHMO-TB-017
Rev A

Executive Summary

As missions, spacecrafts, and operations become progressively more complex, there is an increased reliance on automated systems and a need for diligence in enabling crewmembers to manage automated systems and subsystems. The human operator needs to maintain situation awareness to work effectively with automation, calibrate trust in the system, and avoid errors. Automation functions need to be designed around human roles for specific tasks, with the human operator having ultimate authority. Crewmembers should have the capability to override and/or shut down the automated systems as long as the transition to manual control is feasible and won't cause a catastrophic event. The allocation of responsibilities between humans and automation should seek to optimize overall integrated team performance. "Ineffective user interfaces, poor system designs, or ill-advised functional task allocation will compromise mission success and safety."(HRP Evidence Report, 2013).

Relevant Technical Requirements

NASA-STD-3001 Volume 2, Rev D

[V2 3006] Human-centered Task Analysis
[V2 3102] Human error Analysis
[V2 10004] Controllability and Maneuverability
[V2 10161] Automation System Status Provision
[V2 10162] Automation Mode Change Notification
[V2 10163] Automation Data Availability
[V2 10164] Automation System Responsibility Delineation
[V2 10165] Automation and Robotics Override and Shut-Down Capabilities
[V2 10166] Automation System Configuration
[V2 10167] Range of Control
[V2 10168] Automation Failure Recovery
[V2 10169] Decision Support
[V2 10170] Decision Aid Clarity
[V2 10171] Decision Aid Failure Notification
[V2 10172] Automation Safe Mode
[V2 10173] Safety Default
[V2 10174] System Initiation

Background

Risk of Adverse Outcome Due to Inadequate Human Systems Integration Architecture

Levels of Automation

Levels of Automation refer to the balance of task allocation between human operators and automated systems ***[V2 10167] Range of Control.***

A notional framework for levels of automation is illustrated by the following diagram:

Fully Automated

- The automated system performs all tasks.
- This is the highest level of automation and operation can be accomplished without human oversight.

High-level Automation

- The automated system performs most tasks.
- The human operator engagement is mainly in an oversight or supervisory role. The human operator may perform high-level tasks, for example, monitor the actions and status of the automated system or initiate a sequence of automated tasks at a decision point.

Low-level Automation

- The human operator performs most tasks.
- The automated system executes only tasks as instructed by the human operator or tasks deemed mundane enough to not require human operator supervision.

Manual Control

- The human operator performs specific tasks.
- No automation is used to achieve that specific goal while other high- or low-level automation continues to execute other tasks.

The level of automation for a particular function, operation, or activity sets expectations for the tasks that the crew will perform, including the crew's attention and capability needed to manage the automated system.

The level of automation, however, is adjustable. An automated system may change to a lower or higher level of automation, depending on environmental changes and crew activities, with the expectation that information on the change is available to the crew ***[V2 10161] Automation System Status Provision*** and ***[V2 10162] Automation Mode Change Notification].*** Likewise, the crew maintains the ability to adjust the level of automation themselves if necessary.

Background

Management of Automated Systems
Crew capabilities to manage automated systems are intended to allow the crew to monitor, operate and control the vehicle ***[V2 10167] Range of Control]***, override or shut down automation ***[V2 10165] Automation and Robotics Override and Shut-Down Capabilities***, and assume manual control as driven by their assessment of the vehicle's state of operation.

Monitoring the performance of an automated system helps maintain the situation awareness of the crew necessary to ensure their safety and enhance the chances of mission accomplishment ***[V2 10161] Automation System Status Provision.***

Beyond tasks allocated to the crew at a given level of automation, candidate crew actions may include interventions, such as:

- Request and receive information about the state of a task or subtask
- Force a transition to the next logical step or task
- Transition a task or subtask to a higher level of automation
- Transition a task or subtask to a lower level of automation or manual control
- Pause the automated function, with an option to proceed
- Transition the system to a safe state for re-initialization or recovery
- Abort the automated function

To accomplish a function, operation, or activity, the crew-automation team may perform specific subtasks at different levels of automation. For example, the crew may have manual control of the lateral and longitudinal translation of the spacecraft, while the automation maintains attitude control. This blended control approach is intended to reduce workload and/or improve handling qualities.

The crew is expected to have the capability to operate and control the integrated space vehicle and systems where:

1. The capability is necessary to execute the mission
2. The capability would prevent a catastrophic event
3. The capability would prevent an abort

The capability of the crew to manage the automated systems and control the vehicle supports the certification of the integrated space vehicle to function with the crew during all flight phases.
Even with proper consideration of human factors in the design of automated systems, the crew-automation team performance may fail to enhance the productivity, safety, and effectiveness of space missions. There are many reasons for this, including:

1. Fault of an input or output sensor/system leading to failure of the automated system
2. Un-anticipated external environmental factors
3. Operations that extend beyond the intended operational envelope of the automated system
4. Human error linked to poor situation awareness and/or inadequate training

Background

Importance of the Crew's Role
The importance of the crew-automation team performance is evident throughout human space exploration and aviation. Manual control capability and usage by programs are summarized in the table below.

- Aviation: In recent aviation accidents, erroneous signals from an aircraft sensor triggered an automated system that repeatedly pushed the nose of the plane down. Pilots were not properly trained and did not understand what was happening and why. The system pushed the nose down until the aircraft crashed.

- Space Exploration:
  - The crew of Gemini 8 prevented their own deaths through creative supervision and overriding the automation when their thrusters incurred electromechanical failure.

  - The Apollo 11 mission succeeded in landing on the moon despite two computer-related problems that affected the Lunar Module (LM) during the powered descent. The landing had been planned to be automated, but because of a navigation error caused by the computer, an unexpected boulder field was in the eventual landing zone. The pilot intervened during the landing and flew the LM to a safer site without hazards.

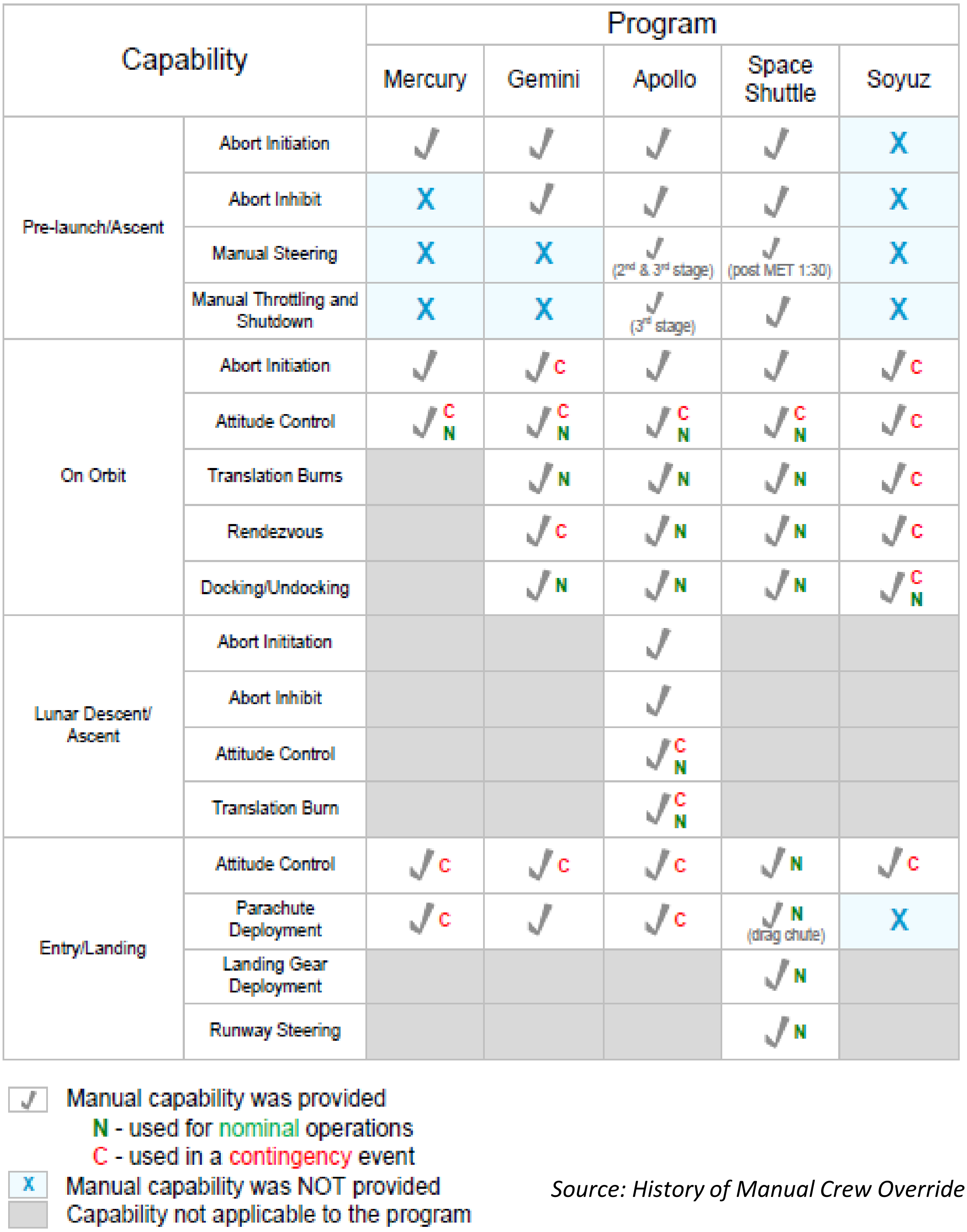
Summary of US. Missions for Which Manual Control was Necessary to Prevent Loss of Crew or Loss of Mission

NASA Program	Number of Missions	Number (and Percentage) of Missions Requiring Crew Control to Prevent LOC or LOM		
		LOC	LOM	Total
Mercury	6	3	0	3 (50%)
Gemini	10	2	1	3 (30%)
Apollo, Skylab, and ASTP (Command/Service Module	15	4	7	11 (73%)
Space Shuttle	135	1	0	1 (1%)
Total Capsule Design	31	9	8	17 (55%)
Total with Space Shuttle	166	10	8	18 (11%)

Source: History of Manual Crew Override

Background

History of the Use of Manual Control



Capability		Program				
		Mercury	Gemini	Apollo	Space Shuttle	Soyuz
Pre-launch/Ascent	Abort Initiation	✓	✓	✓	✓	X
	Abort Inhibit	X	✓	✓	✓	X
	Manual Steering	X	X	✓ (2nd & 3rd stage)	✓ (post MET 1:30)	X
	Manual Throttling and Shutdown	X	X	✓ (3rd stage)	✓	X
On Orbit	Abort Initiation	✓	✓ C	✓	✓	✓ C
	Attitude Control	✓ C N	✓ C N	✓ C N	✓ C N	✓ C
	Translation Burns	▨	✓ N	✓ N	✓ N	✓ C
	Rendezvous	▨	✓ C	✓ N	✓ N	✓ C
	Docking/Undocking	▨	✓ N	✓ N	✓ N	✓ C N
Lunar Descent/ Ascent	Abort Inititation	▨	▨	✓	▨	▨
	Abort Inhibit	▨	▨	✓	▨	▨
	Attitude Control	▨	▨	✓ C N	▨	▨
	Translation Burn	▨	▨	✓ C N	▨	▨
Entry/Landing	Attitude Control	✓ C	✓ C	✓ C	✓ N	✓ C
	Parachute Deployment	✓ C	✓	✓ C	✓ N (drag chute)	X
	Landing Gear Deployment	▨	▨	▨	✓ N	▨
	Runway Steering	▨	▨	▨	✓ N	▨

✓ Manual capability was provided
N - used for nominal operations
C - used in a contingency event
X Manual capability was NOT provided
▨ Capability not applicable to the program

Source: History of Manual Crew Override

Background

Autonomous vs. Automated

The terms autonomous and automated often get mixed up. They are two different things:

- **Automated:** Automation is generally characterized as a capability to execute a specific behavior as initiated and prescribed by a human, but where the execution is controlled by a mechanical or electronic device rather than the human.

- **Autonomous:** Autonomous behavior, in contrast, can be self-initiating and adaptive in response to specific contextual variables, achieving goals while operating independently of external guidance. In practice, it is the combination of elements that function together to produce the capability to meet a need without intervention by humans **NASA-STD-3001 Definitions**. It is the ability of a space system to perform operations independent from any Earth-based system. This includes no communication with, or real-time support from, mission control or other Earth systems.

NPR-8705.2C Human-Rating Requirements for Space Systems

3.2.11 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.

Note: This capability means that the crewed system does not depend on communication with Earth (e.g., mission control) to perform functions.

Spacecraft Autonomy

- Future human spaceflight missions will place crews at large distances and time delays from Earth, requiring autonomous capabilities for crews and ground to prevent Loss of Mission (LOM) or Loss of Crew (LOC).
- Autonomy can greatly enhance future exploration missions to the lunar surface as well as enable operations in extreme environments.
- Without autonomy, humans and robotic spacecraft have successfully navigated satellites, performed soft landings, deployed instruments, and returned samples to Earth.
- With autonomy, future missions will have the ability to make mission-critical decisions such as those required to navigate and avoid hazards without the need for human interaction.
- This capability will enable the exploration of more extreme environments, reduce the delay in decision-making, and decrease the overall cost of mission operations.
- Automated and autonomous systems must be designed to keep the user in the loop and promote situation awareness of system operational states. It is important to have automated and autonomous systems designed to *enable* human operators to be in the loop and to maintain situation awareness with respect to the operational state of the system as needed.

Application

- Successful integration of humans with automated systems is required to accomplish both current and future NASA mission goals. Effective human-automation integration requires that automated systems and their human interfaces be designed to support all levels of human operation. NASA-STD-3001 Volume 2 includes many technical requirements dedicated to the appropriate design and implementation of automated systems.

- Design requirements are to ensure that different levels of automation are available, depending on which level best suits the task/situation. While higher levels of automation can result in increased crew performance (e.g., fewer errors) and lower workload, they can also result in poorer situation awareness and loss of crew skills. Task and trade analysis, in conjunction with function allocation evaluations, should determine the appropriate level of automation ***[V2 10164] Automation System Responsibility Delineation.***

- Systems are not to be so reliant on automation that human operators cannot safely recover from emergencies or operate the system manually if the automation fails ***[V2 10168] Automation Failure Recovery.***

- The operators need to be able to determine and effect what level of automation the system is operating in, as well as which processes are being automated. The analysis will determine cases where alerting may be required when automation takes control from human operators or switches to a higher level of automation ***Volume 2 Section 10.6 Automated and Robotic Systems.***

- Automation needs to keep the human operator involved, informed and support situation awareness:
    1. The human operator needs to maintain situation awareness to work effectively with automation, calibrate trust in the system, and avoid errors ***[V2 10161] Automation System Status Provision, [V2 10163] Automation Data Availability.***
    2. The operator needs access to information about system health and the projection of system state to understand how well automation is likely to perform and calibrate trust (knowing which situations can rely on automation, which situations require increased oversight by the operator, and which situations are inappropriate for automation). The operator needs to be aware of automation performance decrements or failures to be ready to resolve the situation or take over the task ***[V2 10168] Automation Failure Recovery.***
    3. The operator needs to be informed when the mode changes: Conspicuous indication of the current mode will help prevent operators from making mode errors (i.e., taking an inappropriate action or failing to take a needed one, caused by thinking the system is in one mode when it is in another mode). Notification by displays or other means gives the operator the ability to prepare for a mode change, or to adjust behavior to a new mode environment. Designers need to define the best methods to inform and notify humans before the change takes place and again when it happens ***[V2 10162] Automation Mode Change Notification.***

Application

- Automation function needs to be designed around human roles for specific tasks, with the human operator having ultimate authority. The operator needs to be able to modify automation configuration information, including setup/input parameters, initial conditions, and terminating conditions. Some configurations should not be allowed to be manipulated due to performance or safety considerations, which are specific to each system ***[V2 10166] Automation System Configuration.***

- Crewmembers must have the capability to monitor, operate, and control automated systems when the override and/or shut down of the automated system or transition to crew control or manual control will not directly cause a catastrophic event. *NASA-STD-3001 Volume 2* emphasizes the importance of the crew's ability to override and shut down the automated systems in safety-critical situations. This not only contributes to overall mission success but also ensures crew safety/survival ***[V2 1016]5 Automation and Robotics Override and Shut-Down Capabilities, [V2 10172] Automation Safe Mode, [V2 10173] Safety Default.***

- Interfaces should enable the crew to monitor the performance of an automated system and understand what was done by the automation and how successfully the task was accomplished.

- Considerations for the incorporation of crew capabilities to manage spacecraft automated systems should include, but are not limited to, the following:

  1. Is the function critical for crew safety or the primary mission objective?
  2. Is the time required to perform the function within the crewmember response time and performance envelope, considering the off-nominal environment due to automatic control system failure?
  3. Is information generated and provided by the automated system sufficient to ensure the crew can seamlessly enter the control loop?
  4. Is sufficient information being provided to the crew to successfully perform the function?
  5. Are there sufficient controls or inhibits in place to preclude inadvertent engagement of override capabilities?
  6. Is the overall function reliability improved for crew safety and mission success with crew control or manual control, considering human reliability and mission duration impact?
  7. Does the overall risk/benefit trade support implementation of override capabilities when considering technical, cost, and schedule impacts versus not implementing override capabilities and increasing risk to crew safety and mission success?

The technical requirements included in this document are limited to those directly related to automation systems. Other NASA-STD-3001 technical requirements related to human-system performance will also apply in the design of automated systems (e.g., usability, workload, errors, and crew interfaces).
Volume 2 Section 10 Human Performance and Crew Interfaces

Application

Training

Human operator training to use safety-critical automated systems shall include classroom and hands-on training covering:

1. The system's purpose and functionality
2. Standard and emergency operating procedures
3. Integration with other systems
4. Capabilities and limitations
5. Transitioning between the different automation functions in nominal and off-nominal situations.

- Training on automated systems requires special attention; operators must not only understand how the system works but also when it doesn't and why (boundary conditions). Hands-on training for handover is especially important. Training will allow the user to develop an adequate model of how reliable or unreliable the automation is under specific conditions. The better the user understands the automation, the more likely the user is to trust the automation appropriately.

- Training, including human-in-the-loop nominal and off-nominal scenarios, should be sufficient for the crew to gain mastery of why, when, and how to manage automated systems to the appropriate level of automation or assume manual control.

Decision Support

- Decision Aids - (sometimes referred to as decision support systems) are automated systems that provide support to human decision-making processes, either unsolicited or by user request (Wiener, 1988). Design requirements are to ensure that decision support is available to the crew.

- Decision aids can narrow the decision alternatives to a few or suggest a preferred decision based on available data. The human operator needs to understand why the automated system is recommending actions, and the consequences of those actions, to make an informed decision ***[V2 10170] Decision Aid Clarity.***

- The human operator is to remain in control and has the authority to decide when and how to use decision aids. Decision aids should provide pertinent data or information, analysis, and/or suggested solutions for continued operations. The system ultimately needs to enable the operator to make those decisions, whether or not it is the operator that acts on them ***[V2 10169] Decision Support.***

- The human operator needs to be made aware when a decision aid is unable to assist with a decision due to a lack of information or limitations in design ***[V2 10171] Decision Aid Failure Notification.***

Application

Verification
There are typically four different types of verification methods applied during spacecraft verification: Inspection, Analysis, Demonstration, and Test. The information below should be used as general guidance in planning verification for automated systems.

1. Inspection
Inspection methods are used to verify the physical characteristics of the design and its compliance with the requirements. Examples of inspection used for automation verification:

- Confirm display of automation mode (perhaps also the number of modes designed into the system).
- Confirm that diagnostic tools are provided to help with fault isolation.
- Confirm that automatic self-checking components are incorporated in the design.

2. Analysis
Analysis is a process used in lieu of (or in addition to) testing and inspection. Analysis techniques may include statistics and qualitative analysis, computer and hardware simulations, and computer modeling. Examples of Analysis used for automation verification:

- Task Analysis is critical for determining how/when to implement decision aids. When verifying automation, the workflow and allocation of tasks can be dynamic, depending upon the operator’s attention, workload, expertise, complexity, and criticality of the task ***[V2 3006] Human Centered Task Analysis.*** *Reference OCHMO-TB-005 Usability, Workload, Error.*
- Function allocation is a key activity when developing automation. In general, functions performed well by machines should be considered for automation; whereas tasks that require complex pattern recognition, flexibility, adaptability, and those performed under uncertainty are better suited for humans. ***Volume 2 Section 10.6 Introduction - Automated and Robotic Systems.***
- Human Error analysis methods help identify where potential mistakes and failures can result, and thus opportunities for the inclusion of automation ***[V2 3102] Human Error Analysis.***

For more information regarding Automation verification, see Chapter 10, Crew Interfaces, of the Human Integration Design Handbook (HIDH).

Completing an EVA activity using the robotic arm with a crewmember on the end from inside the shuttle requires careful allocation of functions and task planning. Credit: NASA Evidence Report 2013: Risk of Inadequate Design of Human and Automation/Robotic Integration.

Application

3. Demonstration

A demonstration is the showing that the use of an end product achieves the individual specified requirement. It is generally a basic confirmation of performance capability, differentiated from 13 testing by the lack of detailed data gathering. Examples of Demonstrations used for automation verification:

- Demonstrate the automated system functions together with other existing systems or tools.
- Demonstrate the system functions under normal and failure modes of operation (i.e., alerts sound when the system is within failure limits).
- Demonstrate allocation of roles and responsibilities and a means to change it.
- Demonstrate operator override and shutdown capabilities.
- Demonstrate accessibility of information critical for interacting with the automated system (status or trend data).

4. Test

Automation components shall be tested during the design phase with the complete system in a realistic environment, including other automated components of the system and human participants, to ensure they function together as an effective whole, in normal, failure, and degraded conditions.

Automation issues frequently arise when performing in the full operational context. Automated systems need to be tested as they will function in the operational environment to ensure test performance accurately predicts operational performance of the system.

Automated systems are to be designed and evaluated iteratively, using human-centered techniques. An iterative human-centered design and evaluation process needs to be carried out, from the outset, as part of the broader engineering verification and validation process to ensure adequate human-automation teaming.

- Testing of the automated system is done in a realistic simulation environment with representative human operators before implementation.
- Alternative schemes for the allocation of functions can be tested in the context of the whole system through the use of high-fidelity simulations.
- The automated system can be tested under normal operations, failure conditions, and degraded conditions.
- New automation components are tested with the complete system, including other automated components of the system and human participants, to ensure they function together as an effective whole.

Back-Up

Referenced Technical Requirements

View the current versions of NASA-STD-3001 Volume 1 & Volume 2 on the OCHMO Standards website

NASA-STD-3001 Volume 2 Revision D

[V2 3006] Human-Centered Task Analysis Each human spaceflight program or project shall perform a human-centered task analysis to support systems and operations design.

[V2 3102] Human Error Analysis Each human spaceflight program or project shall perform a task-based human error analysis (HEA) to support systems and operations design.

[V2 10004] Controllability and Maneuverability The 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 when manual control is the primary control mode or automated control is non-operational.

[V2 10161] Automation System Status Provision The automated system shall provide the human operator with the following information:

a. system state (e.g., position, location, hazardous condition, running, paused, faulted, completed, overridden, stopped, readiness)

b. projection of future state, including failure or decrements in performance (e.g., battery power versus traverse distance and assessment of uncertainty in projection of future state) and mode (e.g., Full/Partial/Manual/Test)

c. system health

d. configuration information (e.g., setup/input parameters, initial conditions, and terminating conditions)

[V2 10162] Automation Mode Change Notification The system shall notify the human operator of mode changes of any safety-critical operations.

[V2 10163] Automation Data Availability Automated or robotic systems shall record and make available operational and performance data to both crew and ground support personnel.

[V2 10164] Automation System Responsibility Delineation Automated systems shall indicate whether a human operator or system is expected to perform a particular operation at a specific time.

[V2 10165] Automation and Robotics Override and Shut-Down Capabilities Automated or robotic systems shall provide the human operator the ability to safely override and shut down automated systems or subsystems.

[V2 10166] Automation System Configuration Automated or robotic systems shall provide the human operator the ability to modify system configuration within the safety and performance limits of the system.

[V2 10167] Range of Control Automated or robotic systems shall provide the human operator with a range of control options that accommodates the expected operating conditions.

[V2 10168] Automation Failure Recovery The automated or robotic system shall enable the human operator to safely assume control of the system if a failure occurs or there is an inability to function (e.g., beyond designed ability).

[V2 10169] Decision Support The automated or robotic system shall allow the human operator to determine when to use a decision aid and which decision aiding strategy to employ.

View the current versions of NASA-STD-3001 Volume 1 & Volume 2 on the [OCHMO Standards website]

Referenced Technical Requirements

NASA-STD-3001 Volume 2 Revision D

[V2 10170] Decision Aid Clarity Decision aid systems shall provide explanations and rationales, and consequences of potential actions.

[V2 10171] Decision Aid Failure Notification Decision aids shall notify the human operator when a problem or situation is beyond the aid’s capability.

[V2 10172] Automation Safe Mode The automated or robotic system shall take protective action (e.g., avoidance maneuver, protective stop) or request that the operator safely take control if the system's operational safety threshold is exceeded.

[V2 10173] Safety Default The automated or robotic system shall maintain safe operations if the human operator does not assume control when requested.

[V2 10174] System Initiation Autonomous robotic systems shall be initiated only by human operators, including restart after an emergency or protective stop.

Reference List

1. Automation / Autonomy Guidelines and Standards for Space Vehicles Rapid Response Project, Human Factors and Behavioral Performance, April 202
2. Gary Johnson: Lessons Learned from 50+ Years in Human Spaceflight and Safety JSC-2018-009
3. Marquez, J and Rameriz, M. "Level of Automation and Failure Frequency Effects on Simulated Lunar Lander Performance", *https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140013198.pdf*
4. Marquez, J. "Risk of Inadequate Design of Human and Automation/Robotic Integration", *https://humanresearchroadmap.nasa.gov/risks/risk.aspx?i=163*
5. Marquez, J. Risk of Inadequate Design of Human and Automation/Robotic Integration Microsoft Word - SHFE_HARI_with Exec Summ.docx (nasa.gov)
6. NASA OCHMO Rapid Response Task #1 Analysis of Industry and Government Human-Automation Interaction Standards and Guidelines, NASA 2021
7. NextSTEP-2 Appendix H Human Landing System BAA Attachment A17 Human Landing Systems (HLS) White Paper for Manual Control and Windows, https://beta.sam.gov/api/prod/opps/v3/opportunities/resources/files/031c3815fa2479f19a97b4eb1305cce9/download
8. Wiener, E. L. (1988). Cockpit automation. In E. L. Wiener & D. C. Nagel (Eds.), Human Factors in Aviation. San Diego, CA: Academic Press
9. Woods, D and Dekker, S., "Anticipating the effects of technological change: A new era of dynamics for human factors", Theoretical Issues in Ergonomics Science, 1:3, 272-282, *https://www.tandfonline.com/doi/abs/10.1080/14639220110037452*