Chapter XX

NASA'S Identified Risk of Adverse Outcomes Due to Inadequate Human-Systems Integration Architecture

Daniel M. Buckland MD PhD [1,2], Megan Parisi [3], Kaitlin McTigue [3],
Shu-Chieh Wu PhD [4], Tina Panontin PhD [4], Gordon Vos PhD [1],
Devan Petersen MPH [5], Alonso Vera PhD [3]

[1] NASA Johnson Space Center, [5] KBR
Houston, TX 77058, USA

[2] Duke University
Durham, NC 27705 USA

[3] NASA Ames Research Center, [4] San Jose State University
Moffett Field, CA 94043, USA

ABSTRACT

The NASA Human System Risk Board (HSRB) is responsible for tracking the evolution of the top ~30 human system risks identified to be associated with human spaceflight. As part of this process, the Board is charged with maintaining a consistent, integrated process to evaluate those risks and developing evidence-based risk posture recommendations. Risks are ranked by likelihood and consequence. Intermediate causal relationships between risk contributing factors and countermeasures that link hazards to outcomes are described using Directed Acyclic Graphs (DAGs). The DAGs are also useful for identifying common factors and countermeasures across the top 30 risks as well as communicating how astronaut exposure to spaceflight hazards leads to meaningful mission-level health and performance outcomes.

One of the top risks tracked by the HSRB is The Risk of Adverse Outcomes Due to Inadequate Human-Systems Integration Architecture (HSIA). This risk captures the possibility that due to decreasing real-time ground support during missions beyond LEO, crew will be unable to adequately respond to unanticipated critical malfunctions or detect safety-critical procedural errors. The HSIA risk is ranked red (high) for Lunar surface and Mars missions due to the probability of Loss of Crew and Loss of Mission consequences.

This paper describes the evidence that supports the HSIA risk ranking and presents the central narrative of the HSIA risk DAG-- i.e., anomaly detection, diagnosis, intervention, and task performance. Characterizations of the current state of practice for each of the DAG's central nodes and the future tools needed for successful anomaly response are provided.

INTRODUCTION

For the past 20 years, NASA's human presence in space has concentrated on activities in Low Earth Orbit (LEO), specifically on the International Space Station (ISS). As NASA prepares to return humans to the Moon, followed by human missions to Mars, the agency must address new risks and uncertainties to ensure the health and safety of human crew members.

NASA's Human Research Program (HRP) has identified five hazards of human spaceflight: Altered Gravity Fields, Distance from Earth, Radiation, Isolation and Confinement, and Hostile/Closed Environments (Whiting & Abadie, 2019). Within each of these hazard categories lies several associated risks. The NASA Human System Risk Board (HSRB) has the overall responsibility for tracking the evolution of the 30 human system risks identified to be associated with these hazards (NASA Human Research Program, 2021). Twenty-nine of these 30 risks can result in functional impairment that is expected to worsen as mission duration increases. The "30th" risk, the Risk of Adverse Outcomes due to Inadequate Human-System Integration Architecture (the HSIA Risk), is essentially the risk that the crew will not be able to keep the vehicle alive (NASA Engineering & Safety Center, 2022).

THE HSIA RISK

A Paradigm Shift in HSIA

Human-systems integration architecture (HSIA) is a construct used to describe the communication, coordination, and cooperation between humans and cyber-physical systems that must occur in order to accomplish an operation or mission (Panontin et al., 2021). The whole system –the crew, all engineered systems supporting the mission, human experts on the ground, data systems, screens, communication devices, and physical spaces – is an HSIA that enables the execution of complex mission operations and resolution of safety-critical issues. The HSIA currently in place for human spaceflight is the result of a slow evolution over a series of orbital and lunar missions. Apollo, Shuttle, and ISS-era missions have all heavily relied on experts with access to data on the ground to keep the vehicle alive, via real-time problem solving.

A key challenge with safe exploration beyond LEO is that the legacy HSIA will no longer be safe to use as Distance from Earth (the risk's primary hazard) increases. For Lunar missions greater than 30 days and any Mars mission, communication delays, resupply challenges, increased mission complexity, and limited evacuation opportunities necessitate a paradigm shift in HSIA. Given this increasing need for crew independence and the greater operational complexity in future exploration missions, there is a possibility of adverse outcomes associated with deficiencies in HSIA, specifically that crew are unable to adequately respond to unanticipated critical malfunctions and/or perform safety critical procedures to keep the vehicle functional (Vera et al., 2021).

Discussion of human-systems integration (HSI) tends to target the interface level of HSIA: the medium of communication between humans and systems. One might attempt to "fix" the HSI by changing the user interfaces of a system – a tempting option when the integration and interaction levels of the system are human-driven and complex. The consequences associated with unanticipated critical malfunctions beyond LEO cannot be mitigated at the interface level alone because decreasing ground support drastically reduces intervention options. With fewer humans available to address unanticipated, safety critical events and provide system resilience, any HSI solution to this problem must support all levels: cooperation (e.g., problem solving), coordination (e.g., procedure execution) *and* communication (e.g., telemetry visualization).

Characterizing the HSIA Risk

Evidence characterizing the HSIA risk is extensive. To estimate likelihoods, anomaly occurrence and procedural error rates were determined from historical data from past spaceflight missions including ISS and Apollo (see Figure 1). To assess what the crew would need to do to adequately respond to these events, the investigations and deliberations of ISS Mission Evaluation Room and Anomaly Resolution Teams were observed in real-time (remotely); astronauts, flight controllers and instructors interviewed; flight and operation logs reviewed; and troubleshooting approaches taken in analogous domains examined. To assess effects of communication delays on problem resolution and procedure execution, detailed timelines were reconstructed for past ISS anomaly resolution processes and extrapolated to a Mars transit scenario (NASA Engineering & Safety Center, 2022).

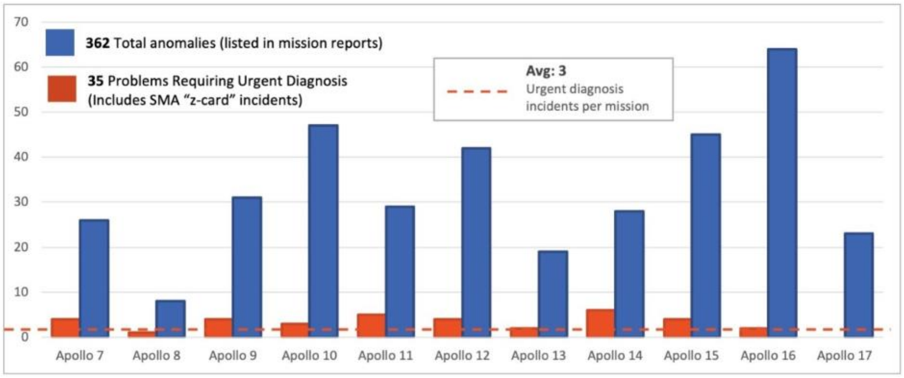

Figure 1: Anomalies on the crewed Apollo missions. The red bars show significant anomalies requiring urgent response, and blue bars show total anomalies listed in Apollo mission reports.

The HSRB ranks each risk by likelihood and consequence. From the assessments described above, it was determined that significant anomalies requiring urgent diagnosis by Mission Control Center (MCC) experts occurred at a rate of 1.7 times per year for ISS averaged over the lifetime and 3-4 times per year in the "burn-in" phase for the vehicle (Panontin et al., 2021). Prior experience from the Apollo program showed 10/11 crewed missions experienced significant anomalies where crew relied heavily on MCC expertise in real-time. These failure patterns are in line with those observed in other complex engineered systems (e.g., oil rigs, launch systems, commercial aviation, etc.) (Vera et al., 2021). This data suggests that general malfunction and error rates are > 10% even for short duration missions (<30 days).

For Low Earth Orbit (LEO) missions and Lunar missions less than 30 days, assuming minimal comm delays, disruptions and bandwidth limitations, malfunctions and errors can affect mission objectives but can be well mitigated by ground support. For Lunar missions greater than 30 days and any potential Mars mission, however, malfunctions and errors can have Loss of Crew and Loss of Mission consequences due to reduced ground support (communication delays and constraints) for more complex operations, as well as reduced resupply and evacuation options. For this reason, the HSRB determines the HSIA Risk is high (i.e., a red risk) for Lunar Orbital & Surface missions and Mars missions (Vera et al., 2021).

DIRECTED ACYCLIC GRAPHS

The HSRB uses Directed Acyclic Graphs (DAGs) as the basis for understanding intermediate causal relationships between risk contributing factors and countermeasures that link hazards to outcomes and as a communication tool for describing how astronaut exposure to spaceflight hazards leads to meaningful mission-level health and performance outcomes. The DAG for the HSIA Risk is depicted in Figure 2.

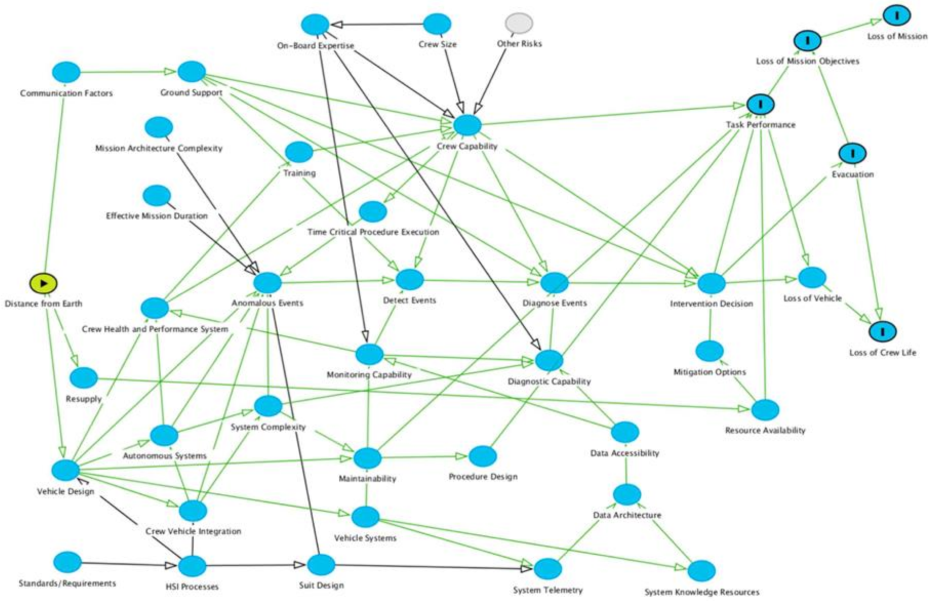

Figure 2. DAG for the Risk of Adverse Outcomes due to Inadequate HSIA

At the heart of the HSIA Risk DAG lies a central pathway from Anomalous Events to intervention performance outcomes (see Figure 3). When anomalous events occur, the team must detect the event, accurately diagnose the event, decide on an intervention, and perform appropriate tasks in time to save the vehicle, the crew, and the mission.

Figure 3: Central path of anomaly response

The capabilities represented in this central path (detection, diagnosis, intervention, task performance) must be enabled in a fundamentally new way on missions beyond LEO, as ground support decreases and mission complexity increases. The following section breaks down this central DAG narrative, cataloging the current state of each node and investigating how these actions can be successfully enabled on missions beyond LEO.

HSIA DAG NARRATIVE

Anomalous Events

Unanticipated, critical problems (including malfunctions, failures, and unexpected interactions of subsystems) can occur in complex engineered systems, regardless of the preparation and expertise utilized in the engineering process (Panontin et al., 2021). The total number of events faced is likely to increase with mission duration (and therefore with distance from Earth). Though these events cannot be avoided entirely, the frequency and severity of these anomalies are impacted by a variety of known factors, including the design of the vehicle, the crew-vehicle integration, autonomous systems, and the complexity of the mission and mission systems. While these factors can act as countermeasures (e.g., a well-designed vehicle can prevent certain anomalies), they can also increase the frequency or severity of anomalies, either because they are done poorly or simply because they introduce complexity.

Detect Events

The first step in anomaly response is recognizing and capturing a notable divergence from what is nominal and/or expected. This detection utilizes ground support and crew capability and is impacted by the monitoring capabilities provided to the human-system team.

Today, anomaly detection heavily relies on the capabilities of experts on the ground in the ISS Flight Control Room (FCR), Multipurpose Support Rooms, and the Mission Evaluation Room (MER) (Panontin et al., 2021). Every day, there are 80+ experts on the ground with a combined 600+ years of system-specific experience sitting console and monitoring data across these rooms. While the number of team members sitting console decreases slightly overnight, the FCR is staffed 24/7 with individuals monitoring data. Each person sitting console monitors an extensive amount of telemetry data pulled from the vehicle (see Figure 4). Crew members on the ISS typically do not have access to the telemetry data monitored by the ground, as crew members are not expected to provide any data monitoring capabilities.

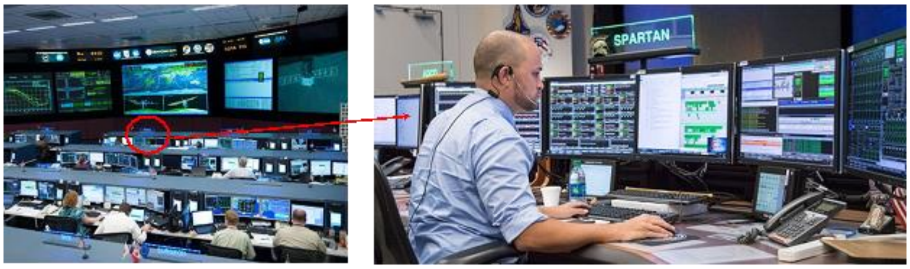

Figure 4: Data monitored by a single ISS flight control station.

On Lunar missions, most data monitoring will likely still take place from the ground, but teams will need to monitor data from multiple vehicles, built by multiple contractors. Presenting this vast amount of data in an accessible and consistent way will be key to successful event detection. Lunar telemetry streams may be delayed by seconds, meaning the crew capability to detect events will need to be strengthened, especially for critical incidents that require immediate action. As missions move beyond the Moon and communication delays increase to up to 20 minutes one-way, the crew, with the help of intelligent onboard systems, will need to perform essentially *all* the data monitoring needed to detect critical events in a timely manner.

Diagnose Events

After the human-system team has detected the event, the team must characterize the problem and determine its causes and impacts. Whether or not an event is successfully diagnosed depends on the availability of the ground and the capabilities of the crew, as well as the sensors, data, tools, and expertise available to the team, or the diagnostic capability.

Like detection, diagnosis today relies heavily ground expertise. The current HSIA for the ISS is ground-based and work-force intensive, relying on many engineers and operators with broad and deep expertise; large, distributed datasets; and expansive analytical and computing power. (Panontin et al., 2021). Diagnosis is an iterative process involving hypothesis generation and testing (NASA Engineering & Safety Center, 2022), and NASA's MER anomaly response teams employ creative and critical thinking to collaboratively troubleshoot anomalies The iterative process is carried out by the ground with a real-time cadence, but when hypothesis testing requires crew involvement, the crew performs on-board troubleshooting activities at the direction of the ground. Ground controllers may also manipulate the vehicle for hypothesis testing without crew awareness.

As missions move beyond LEO, the crew's capability to diagnose events will need to increase to compensate for reduced ground support. Like detection, the ground will likely still play a large role in diagnosing anomalies on Lunar missions, but the small communication delay may necessitate greater reliance on the crew for hypothesis testing. Even with a small communication delay, the ground may avoid "commanding in the blind," or sending a command to the vehicle without knowing its present state. The crew will need the right tools, sensors, and expertise onboard the vehicle to assist in completing diagnostic activities. On a mission to Mars, crew capability will be the primary driver for diagnosis as ground support reduces even further. Depending on the cadence of hypothesis generation and testing, the crew may need to carry out diagnostic activities without *any* ground support.

Intervention Decision

After diagnosing the event, the human-system team must decide what, if any, intervention to employ to correct the causes of the anomaly and/or mitigate the consequences. Like detection and diagnosis, the intervention decision is impacted by the abilities of the ground and the crew, but the decision largely hinges on the mitigation options available to the team.

For the ISS, a large team of MER and MCC engineers generate possible mitigation options, assess them (based on risk, benefit, cost, crew time needed, etc.), and systematically choose a path forward. When physical maintenance and repair is required, the intervention decision is impacted by the ability to resupply (NASA Engineering & Safety Center, 2022). If the crew needs to use a spare onboard the vehicle to address the anomaly, the ground can plan to send another spare at the earliest opportunity. If the intervention requires a component not currently onboard the vehicle, the ground can send the new component with the next visiting vehicle. The ability to resupply can also extend the intervention decision timeframe. If a critical consumable is impaired by the anomaly (e.g., an oxygen leak), the ability to resupply consumables allows for extra time to consider mitigation options.

The mitigation options available decrease for mission beyond LEO. As resupply opportunities decrease with distance from Earth, fewer resources become available for system failure intervention. When a system does fail, crew members will need to focus on repair rather than replacement. Replacing an entire unit due to a component failure is a suboptimal solution when limited spares exist. Crew members will also need to preserve consumables onboard the vehicle whenever possible, increasing the repair cadence when consumables are at risk. Crew capability to make an intervention decision will need to increase as ground support decreases.

Task Performance

If the intervention requires action, the human-system team needs to perform relevant tasks to implement the intervention. Task performance success is impacted by procedure design and by the maintainability of the vehicle, or the ease and rapidity with which systems or equipment can be restored to operational status.

Current ISS procedures are designed around the data, personnel, and resources available on the ground (NASA Engineering & Safety Center, 2022). Certain procedures are executed entirely by the ground with no crew input. When a procedure needs to be executed by the crew, the ground oversees the procedure in real-time, often even verbally commanding the steps. During crew execution of a procedure, it is common to pause and wait for ground input before proceeding. Flight controllers and MER engineers sometimes pause at points in a procedure to consult their investigative fault trees, review data and resources, and debate amongst the team on how best to proceed.

For missions beyond LEO, procedures should be designed with autonomous crews in mind. Crew members will need access to the resources typically used by the ground to alleviate procedure ambiguity, as the ground may not be able to provide real-time guidance and oversight, even with small communication delays. When unanticipated anomalies with no set procedures in-place occur, crew members may need flexibility in pulling from and combining multiple procedures to adequately execute necessary tasks. With increased system complexity on Lunar and Mars missions, the vehicle needs to be designed more specifically for maintainability. Design considerations like standardization, interchangeability, modularization, simplification, accessibility, and identification, as well as human factors, should be considered to improve task performance success when an intervention is needed.

DISCUSSION

As crewed exploration missions venture farther from the Earth, ground support decreases, and crews must act with greater autonomy than ever before. This will require a radical paradigm shift in mission operations. NASA must reimagine the systems, tools, and roles, both onboard and on the ground, to enable the detection, diagnosis, intervention, and task performance capabilities needed to prevent the loss of the vehicle when events requiring immediate response occur. Moreover, the design and implementation of the systems and tools must support the roles and responsibilities levied upon the crew and intelligent systems and be considered from a system architecture perspective to achieve overall human-systems resilience.

Specifically, detection and diagnosis of anomalies require onboard data systems that support monitoring, analysis, and trend identification for vehicle systems via sensors. Artificial intelligence (AI) may be leveraged to augment a small crew's ability to monitor vast amounts of data previously attended to by 80+ experts on the ground in real-time. However, AI will not replace human creativity, critical thinking, and problem-solving. Time-sensitive diagnosis will be performed by the crew with support from enabling technologies such as data visualization and decision aids.

Intervention and task execution test the ability of onboard teams to perform complex operations that have historically been handled by the ground or executed by crew with real-time oversight from ground personnel. AR/VR and other supportive technologies should be investigated to help crew characterize and assess impacts of problems in complex, interconnected systems. Crew will also need to work with limited resources and mitigation options in an unforgiving environment. Standards and requirements for advanced maintainability, reliability, and diagnosability must be established early in the vehicle development cycle to promote systems resilience. In-space manufacturing technologies should be considered to mitigate the limitations of sparing and resupply.

CONCLUSION

This paper describes the driving factors behind the HSIA Risk's classification as red (high). Data from past lunar and orbital missions suggest that unanticipated, safety-critical anomalies requiring immediate response *will* occur on missions beyond LEO, even under the best engineering expectations. As ground support decreases and mission complexity increases, crews must become more autonomous than ever before. A paradigm shift in Human-Systems Integration, both onboard and on the ground, is needed to enable successful anomaly diagnosis, detection, intervention, and task performance on missions beyond LEO. NASA's HSIA team calls on the human-systems engineering community to research technologies that can support a small, isolated crew's ability to problem-solve in complex systems.

REFERENCES

NASA Engineering and Safety Center. 2022. *Safe Human Expeditions Beyond Low Earth Orbit (LEO)*.

NASA Human Research Program. 2021. *Human Research Program Integrated Research Plan*. HRP-47065. [Online] NASA Johnson Space Center. Available at: https://humanresearchroadmap.nasa.gov/Documents/IRP_Rev-Current.pdf (Accessed 24 February 2022).

Panontin, T.L., Wu, S.C., Parisi, M.E., McTigue, K.R.. & Vera, A.H. 2021. *Human-systems integration architecture needs analysis: on-board anomaly resolution during autonomous operations*. NASA Ames Research Center.

Vera, A.H., Vos, G., & Petersen D., 2021. ‘Updates to risk of adverse outcomes due to inadequate human systems integration architecture’ [PowerPoint presentation]. NASA Human System Risk Board.

Whiting, M. & Abadie, L. (2019) *5 hazards of human spaceflight* [Online]. Available at: https://www.nasa.gov/hrp/5-hazards-of-human-spaceflight (Accessed: 24 February 2024)