DOI: 10.13009/EUCASS2025-749
11TH EUROPEAN CONFERENCE FOR AERONAUTICS AND SPACE SCIENCES (EUCASS)

Human Spaceflight Safety: From LEO to the Moon and Mars

Grzegorz Ambroszkiewicz
European Space Agency
Keplerlaan 1, 2201 AZ Noordwijk, The Netherlands
grzegorz.ambroszkiewicz@esa.int

Abstract

As human spaceflight extends beyond Low Earth Orbit (LEO) to the Moon and eventually Mars, ensuring astronaut safety becomes an increasingly complex challenge. This paper examines the evolution of safety methodologies, emphasizing the transition from compliance-based frameworks used on the International Space Station (ISS) to risk-informed approaches tailored for deep space missions. The shift beyond Earth's orbit introduces new environmental hazards that necessitate changes to existing safety strategies, such as increased radiation levels, lunar dust, communication delays, and the need for high autonomy. These factors necessitate a more adaptable safety framework that balances risk with mission objectives. This paper underscores the importance of evolving safety strategies to match the increasing autonomy and complexity of deep space exploration.

1. Introduction

Human spaceflight has historically been conducted within Low Earth Orbit (LEO), where proximity to Earth allows for continuous ground support, rapid resupply missions, and immediate evacuation capabilities. However, as exploration goals shift to the Moon and eventually to Mars, the complexity of ensuring astronaut safety increases significantly. Traditional compliance-based safety methodologies used on the ISS must evolve into more flexible, risk-informed frameworks to accommodate the unique hazards and operational challenges of deep space missions. This paper compares safety strategies employed in LEO with those being developed for lunar and Martian missions, highlighting the growing need for autonomous systems and design-for-maintainability principles.

2. Safety Analysis [2]

A robust safety analysis is essential in identifying potential hazards, applicable safety requirements, and appropriate control and verification methods for human spaceflight systems. The analysis supports proactive identification and mitigation of hazards that could lead to mishaps, ensuring safe operation throughout a mission's lifecycle. The safety analysis process includes:

- Identification of hazardous conditions in system designs
- Assessment of the likelihood/severity and potential impact of these hazards
- Basis for implementing preventive design features and mitigations
- Verification of compliance with defined safety requirements
- Evaluation of failure impacts and hazardous interfaces
- Identification of areas requiring further analysis

A top-down analytical method is used, beginning with high-level undesired events and tracing down to underlying hazardous conditions and their root causes. These may be addressed through design, documented in failure mode analyses, or classified in critical item lists. If redundancy is used as a hazard control, the analysis shall account for potential common cause failures.

A fundamental principle of human spaceflight safety is that all identified hazards with catastrophic or critical consequences must be controlled through design, redundancy, or operational mitigation. This requirement reflects the high-consequence nature of failures in crewed missions and ensures that residual risk remains within acceptable bounds.

DOI: 10.13009/EUCASS2025-749

2.1 Severity Classification [1;4]

Severity definitions provide a common language for risk assessment and prioritization. The following classifications apply:

- Catastrophic Hazards are those that result in:
  - Loss of crew
  - Permanently disabling injury
  - Loss of Vehicle/Station

- Critical Hazards are those that result in:
  - Injury or occupational illness requiring medical intervention by a second crew member and/or Flight Surgeon, and not treatable with first aid alone
  - Loss of a Program Mission Objective
  - Loss of a major Vehicle/Station element
  - Major damage to other essential flight systems

These severity definitions guide system designers and safety analysts in determining the required level of control, verification, and review for each hazard.

3. Hazard Control Strategy [1;4]

A systematic hazard risk reduction hierarchy is followed:

1. Eliminate through Design:
   - Remove the hazard source entirely or avoid hazardous operations by using alternative designs or materials.
2. Reduce Risk via Design Alteration:
   - Incorporate features that lessen hazard severity or likelihood
   - Implement fault-tolerant designs or redundant systems
3. Operational Controls:
   - When design mitigation is insufficient, crew actions, ground commands, or automated sequences may be used to enhance safety. For high-severity hazards, procedural controls alone are considered insufficient.

Effective hazard control typically requires a combination of these methods. Failure tolerance remains the preferred strategy for hazard control. The level of tolerance should be guided by comprehensive system safety analyses. When redundancy is applied, susceptibility to common cause failures must be evaluated, especially if identical components or architectures are used. Employing dissimilar redundancy can help mitigate such risks.

Hazard analyses must also identify Crew Survival Methods (CSMs) such as abort capabilities, evacuation options, safe havens, or emergency medical support that could improve survivability in the event of system failure. CSMs should be described, referenced, and verified, even if not explicitly required by design specifications.

5. Risk Acceptance in Human Spaceflight Programs

Human spaceflight programs have historically evolved under differing safety philosophies depending on mission architecture, stakeholder involvement, and maturity of the operating environment. Two dominant paradigms are evident when comparing the approach taken for the International Space Station (ISS) and Commercial Crew Programs (CCP) with that of the Lunar Gateway program: a compliance-based approach versus a risk-informed methodology.

DOI: 10.13009/EUCASS2025-749

5.1 Compliance-Based Safety (ISS/CCP) [1;3]

The ISS and Commercial Crew programs operate under a compliance-driven framework. This approach emphasizes adherence to prescriptive safety requirements, detailed standards, and certification criteria. Each element must meet explicitly defined requirements, with compliance verified through documentation, testing, and review. In this model:

- Safety success is equated with meeting established design and verification requirements.
- Hazard controls are tightly linked to predefined failure tolerance rules (e.g., two-fault tolerance for catastrophic hazards).
- Survivability systems (e.g., abort, emergency medical) are mandated by design specifications.
- Deviations require waivers or exceptions, often subjected to formal boards or standing review panels.

This model provides a high degree of traceability and consistency, particularly for mature operational environments with a known hazard landscape. However, it may impose design constraints that reduce flexibility and adaptability in novel mission contexts.

5.2 Risk-Informed Safety (Lunar Gateway) [4]

In contrast, the Lunar Gateway program adopts a risk-informed approach, suitable for the relatively untested deep-space environment and modular, multi-agency architecture. Rather than relying solely on rigid requirements, Gateway safety relies on structured hazard analysis to justify the acceptability of residual risk based on mission context, system function, and integrated risk trade-offs. Key features include:

- Greater emphasis on mission risk trades informed by system-level hazard reports.
- Use of risk acceptability arguments in place of universal fault tolerance mandates.
- Evaluation of controls based on their risk reduction effectiveness, not merely their compliance status.
- Flexibility to tailor survivability features (e.g., safe haven, emergency medical) based on module capabilities and roles.

This model enables innovation and international collaboration by focusing on outcome-based safety goals, rather than strictly prescriptive solutions. However, it places greater responsibility on integrators and safety panels to make nuanced, justified risk decisions and maintain a consistent safety posture across distributed teams.

6. Environmental and Operational constraints

Key to ensuring crew safety in Low Earth Orbit (LEO) is the continuous human presence onboard and the availability of real-time support from mission control on Earth. Spacecraft such as the International Space Station (ISS) benefit from a proximity that allows for rapid response to anomalies, regular maintenance, and a robust supply chain. Redundant systems and highly trained crew members, supported by a constant connection to Earth, create a tightly controlled operational environment. However, this safety paradigm is heavily dependent on Earth's closeness and cannot be directly applied to missions beyond LEO without significant adaptation.

Lunar exploration introduces a new set of environmental and operational constraints that shift the foundation of risk management. The Moon presents harsh conditions, including high radiation levels due to lack of a protective atmosphere, extreme thermal cycles, and the presence of highly abrasive lunar regolith, which can compromise mechanical systems and seals. Moreover, future infrastructure like the Lunar Gateway is expected to be uncrewed for extended periods, thereby requiring safety systems capable of operating autonomously. The safety architecture must support remote diagnostics, automated fault detection, and self-recovery protocols. Lessons from the ISS inform the transition, but the emphasis shifts from continuous human oversight to system resilience and smart automation. The capacity to monitor system health and respond to anomalies without immediate human input becomes a central design requirement.

Mars missions elevate the challenge exponentially. The distance between Earth and Mars introduces communication delays of around 20 minutes one-way, eliminating the feasibility of real-time ground intervention. Crewed Mars missions will face prolonged exposure to deep-space radiation, long-duration transits with no options for emergency

DOI: 10.13009/EUCASS2025-749

return, and the logistical impossibility of resupply or rescue. These constraints demand a paradigm shift in safety philosophy: systems must be designed from the ground up for autonomy and maintainability. Habitats and vehicles on Mars must operate self-sufficiently for years, requiring advanced onboard diagnostics, predictive maintenance algorithms, and fault-tolerant architectures. Technologies such as in-situ resource utilization (ISRU) will be critical for producing oxygen, water, and fuel locally, reducing dependence on Earth-based logistics. Furthermore, psychological support systems must evolve to address the mental health risks associated with extreme isolation, delayed communication, and confinement.

Table 1: LEO/Moon/Mars Environmental and Operational Constraints

	LEO	**Moon**	**Mars**
Distance from Earth	~400 km - near no communication delay	~384,000 km - ~1.3 seconds delay	~55–400 million km - ~20 minutes one-way delay
Real-time Ground Support	Available continuously	Limited, must support partial autonomy	Unavailable, full autonomy required
Radiation Exposure	Moderated by Earth's magnetosphere	High; no magnetic field or atmosphere	High; no magnetic field and limited atmosphere protection
Thermal Environment	Frequent but manageable orbital thermal cycles	Extreme surface cycles with long hot and cold phases	Cold, but more stable daily variation, seasonal and diurnal variation
Atmosphere	None, but Earth proximity allows Earth-like support systems	None, full reliance on pressurized systems	Thin CO_2 atmosphere (~0.6% of Earth), usable for some ISRU
Surface Hazards	N/A (orbital station)	Lunar dust is sharp and abrasive	Martian dust is pervasive and electrostatically charged
Maintenance and Repair	Regular, human-performed with real-time ground support	Intermittent human presence; requires autonomous inspection & maintenance	Fully autonomous or crew-maintained for multi-year durations
Supply and Logistics	Frequent resupply flights possible	Occasional deliveries; long planning cycles	Extremely limited or none; must be self-sufficient
Human Presence	Continuous	Intermittent or crew-tended short missions initially	Continuous for extended missions; long-term settlements
Psychological Stress	Moderate, rotating crews and Earth contact	Higher due to partial isolation and operational pressure	Extreme due to isolation, communication delay, confinement, and duration
Automation Needs	Moderate, human operators onboard and on Earth	High, support systems must function during crew absence	Critical, systems must operate autonomously for long durations
Escape / Rescue Possibility	Rapid emergency return to Earth (within hours)	Delayed rescue, emergency return highly constrained	No realistic emergency return, full self-reliance essential

DOI: 10.13009/EUCASS2025-749

In-Situ Resource Utilization (ISRU)	Not applicable	Potential (e.g., water ice at poles)	Might be essential for survival - oxygen, fuel, water from local resources

9. Conclusion

In conclusion, the approach to safety and risk acceptance must be carefully tailored to the unique environmental and operational constraints of each mission destination. What works in LEO is not directly translatable to the Moon or Mars. As missions move farther from Earth, safety systems must evolve from human-supervised redundancy to fully autonomous, intelligent architectures that prioritize resilience and maintainability. In particular, Martian missions represent a major challenge for traditional safety certification processes. They necessitate a rethinking of how safety is validated, moving toward flexible, design-for-maintainability systems that can adapt to long-duration missions in remote and unforgiving environments. Future mission success will depend not just on surviving space, but on thriving in it, without a safety net from Earth.

References

[1] SSP 51721 International Space Station Program, ISS Safety Requirements Document, September 2019
[2] SSP 30309 International Space Station Program, Safety Analysis and Risk Assessment Requirements Document, November 2005
[3] SSP 30599 International Space Station Program, Safety Review Process, February 2015
[4] GP 10024, Gateway Program, Hazard Analysis Requirements, August 2021