Failure Modes, Effects and Criticality Analysis for Safety Critical System

[1] Savitha. A , [2]Pushpavathi T. P

[1] Research Scholar, Department of Computer Science, M.S Ramaiah University of Applied Sciences, Bangalore, India,

2 Department of Computer Science, M.S Ramaiah University of Applied Sciences, Bangalore, India,

Abstract—— **Failure Modes, Effects, and Criticality Analysis (FMECA) is a systematic approach to identifying and evaluating potential failure modes in spacecraft systems, assessing their effects on mission performance and safety, and prioritizing corrective actions. Given the complexity and high stakes of spacecraft operations, FMECA serves as a critical tool for mitigating risks and enhancing reliability. This study applies FMECA to spacecraft operations, focusing on key subsystems such as propulsion, power, communication, guidance, thermal control, life support, and structural integrity. Each subsystem is analysed to identify failure modes, evaluate their effects on mission-critical functions, and classify their criticality based on severity and likelihood. Findings highlight the importance of redundancy, robust design, and thorough testing to address high-priority risks, such as propulsion failures, communication signal loss, and life support system malfunctions.**

The results demonstrate the value of FMECA in proactively addressing hazards, reducing the likelihood of mission failure, and ensuring crew and equipment safety. By integrating FMECA into the design and operational phases, spacecraft developers can achieve higher levels of reliability and mission success, paving the way for safer and more efficient space exploration.

Keywords— Hazard Mitigation, Failure Modes, Effects, and Criticality Analysis (FMECA), Probability, Probability), Severity), Failure mode

I INTRODUCTION

Spacecraft operate in one of the most challenging environments known to humanity, where extreme conditions, limited resources, and the inability to perform real-time repairs create significant risks. To ensure mission success and protect valuable assets and, in some cases, human lives, it is essential to identify and mitigate potential failures proactively. Failure Modes, Effects, and Criticality Analysis is a powerful methodology for achieving this objective. FMECA is a systematic approach that identifies potential failure modes in spacecraft systems, assesses their effects on mission performance, and prioritizes them based on severity, probability, and criticality. By focusing on the most critical risks, FMECA enables engineers to implement design improvements, redundancy, and fault-tolerant measures that enhance reliability and safety. In spacecraft operations, where system interdependencies are highly complex, even a minor failure can cascade into catastrophic consequences. For example, a propulsion system malfunction could result in trajectory deviation, while a communication failure could lead to loss of control or data. FMECA helps address such scenarios by offering a structured framework to evaluate and mitigate risks systematically.

This analysis is particularly vital in the context of modern space missions, which involve intricate systems such as autonomous navigation, thermal control, and human life support. As space exploration evolves, the reliance on sophisticated technology increases, making robust risk management practices indispensable. This paper explores the application of FMECA to spacecraft operations, emphasizing its role in enhancing mission success, ensuring system safety, and fostering the development of reliable space technologies [1]. By integrating FMECA into spacecraft design, testing, and operational phases, space agencies and organizations can proactively address risks, reduce costs associated with failures, and advance the frontiers of space exploration [2].

II METHODOLOGY FOR FMECA

Identify the systems and subsystems:

Identify the systems, subsystems, and components to be analysed. Specify boundaries such as mission phases (e.g., launch, orbit, re-entry -for crewed mission). Establish the goals of the FMECA, such as improving system reliability, reducing mission risk, or ensuring safety compliance. Align the FMECA process with the spacecraft development lifecycle, including design, implementation testing, and operations. Include experts from various domains: systems engineering, software development, propulsion, communication, and thermal systems. Ensure representation from quality assurance, risk management, and operations teams. Collect detailed information on system architecture, specifications, and design documents. Review data from similar missions or systems for insights into common failure modes and their consequences [3]. Define the operational scenarios like use cases, environmental conditions, and mission profiles relevant to the spacecraft's operations. Identify Failure Modes like Component-Level Analysis: Examine individual components and subsystems for potential failure modes. Consider failures at the interfaces between subsystems (e.g., data transfer, power supply). Account for external Environmental Influencing factors like radiation, temperature extremes, and micrometeoroid impacts [4].

Analyse effects of failures

Local Effects will determine how the failure impacts the specific component. System-Level effects assess the impact on the entire spacecraft and mission objectives. Mission criticality will identify whether the failure compromises mission success or safety. Prioritize Risks

- Assign ratings for severity, probability, and detectability for each failure mode.
- Calculate the **Criticality Index** to prioritize failure modes based on their impact and likelihood:
- Criticality Index=Severity×Probability×(1−Detectability)

Rank failure modes to focus on those with the highest criticality.

Develop Mitigation Strategies like design improvements by modifying the designs to eliminate or reduce the likelihood of failure (e.g., using more robust materials, simplifying components). Plan for redundancy by Adding redundant systems or fail-safe mechanisms for high-criticality components. Independent testing and validation to enhance testing protocols to identify and address potential issues early (e.g., fault injection testing). Real-Time monitoring mechanism to detect and address failures during operation. Create a detailed FMECA table summarizing failure modes, effects, criticality ratings, and mitigation strategies. Provide clear, actionable recommendations for addressing high-priority risks. Review findings with the design and operations teams to ensure feasibility and effectiveness. Update the FMECA iteratively as the design evolves, incorporating new data and insights. Deploy monitoring systems to detect failures in real-time and implement contingency plans [5]. Use operational data to refine the FMECA for future missions. Figure 1 shows the steps to carryout software FMECA for mission software.

Figure 1: Steps to carry out SFMEA

Benefits of FMECA Implementation

- Proactively identifies and mitigates potential risks, enhancing spacecraft reliability.
- Provides a structured framework for prioritizing design and operational improvements.
- Aligns with safety and quality standards, ensuring regulatory compliance.
- Improves mission success rates by reducing the likelihood of critical failures.

Address the challenge like difficulty in quantifying software failure probabilities by providing solution to Use historical data, simulation tools, and expert judgment [6]. Address the challenge resource constraints for implementing redundancy by providing solution to prioritize redundancy for the most critical components. Address the challenge dynamic mission conditions by providing solution to Incorporate adaptive monitoring and real-time diagnostics like onboard autonomy. By following these steps, FMECA implementation ensures a comprehensive approach to risk management in spacecraft operations, paving the way for safer and more reliable missions [7].

III PRELIMINARY HAZARD WORKSHEETS

All the subsystems have to be considered for the FMECA list. **FMECA table** tailored for spacecraft operations. This table includes critical components, potential failure modes, their effects, causes, and recommended actions.

Table 1: FMECA worksheet for the spacecraft operations

Component	Failure Mode	Effect	Cause	Severity	Probability	Criticality	Recommended Action
Propulsion System	Loss of thrust	Inability to maintain	Fuel leak, valve failure, or	High	Moderate	High	Redundant thrusters;

Component	Failure Mode	Effect	Cause	Severity	Probability	Criticality	Recommended Action
		trajectory or orbit	software error				periodic testing
	Excessive thrust	Unstable orbit or overshoot	Control system bug	High	Low	Moderate	Thorough software validation
	Thruster nozzle clogging	Reduced or uneven thrust	Contaminants in fuel	Moderate	Moderate	Moderate	Filter fuel; maintenance checks
Power System	Battery overcharge	Overheating, fire risk	Faulty charging system	High	Low	Moderate	Add charge control system; monitoring
	Solar panel degradation	Insufficient power generation	Radiation damage, micrometeoroid impact	Moderate	High	High	Redundant panels; shielding
Communication	Signal loss	Loss of command and telemetry	Antenna failure, interference	High	Moderate	High	Redundant antennas; interference testing
	Data corruption	Erroneous commands or telemetry	EMI, software error	Moderate	Moderate	Moderate	EMI shielding; error correction coding
Guidance System	Sensor failure	Navigation errors, loss of orientation	Radiation, hardware fault	High	Moderate	High	Redundant sensors; shielding
	Algorithm error	Misalignment, incorrect trajectory	Software bug	High	Low	Moderate	Rigorous testing; code review
Thermal System	Overheating	Component damage	Insufficient heat dissipation	High	Moderate	High	Improved thermal design; monitoring
	Freezing of components	Loss of functionality	Exposure to extreme cold	High	Low	Moderate	Thermal insulation; heaters
Life Support System	Oxygen generation failure	Crew suffocation	Electrolyser failure, power loss	Catastrophic	Low	High	Redundant systems; backup power
	CO_2 removal failure	Crew poisoning	Absorption bed saturation	Catastrophic	Moderate	High	Scheduled replacement; monitoring
	Water recycling failure	Dehydration, waste buildup	Filtration system clogging	High	Moderate	High	Redundant filtration; maintenance
Structure	Structural fatigue	Loss of integrity, potential failure	Material fatigue, micrometeoroid impact	High	Low	Moderate	Advanced material testing; shielding
	Improper assembly	Component detachment	Manufacturing defects	High	Low	Moderate	Rigorous inspection, quality control

- Severity: Ranked as Low, Moderate, High, or Catastrophic based on the impact on mission and crew safety.
- Probability: Likelihood of occurrence, rated as Low, Moderate, or High.
- Criticality: Combined assessment of severity and probability.

- Recommended Actions: Specific mitigations or precautions to reduce the risk.

This table1 serves as a guide for identifying and mitigating critical risks in spacecraft operations, ensuring mission success and safety. Each mission may require customization of the FMECA table based on specific systems and objectives.

IV RESULTS AND DISCUSSION

Identification of Failure Modes :The FMECA identified numerous failure modes across spacecraft subsystems, categorized into mechanical, electrical, software, thermal, and human factors-related failures. Key failure modes include like Propulsion system failures with loss of thrust or excessive thrust impacting trajectory. Power system failures like battery overcharge, solar panel degradation, or power interruptions. Communication failures like signal loss, data corruption, or antenna malfunctions. Software issues like incorrect algorithms, real-time task delays, and unexpected software crashes. Criticality Analysis is carried out with failure modes were ranked based on severity, probability, and detectability [8]. High-criticality risks were observed in the following areas like software errors in guidance and navigation systems, propulsion system valve failures leading to trajectory deviations, solar panel malfunctions causing power shortages. Moderate risks included structural fatigue, data logging issues, and thermal imbalances. Proposed Mitigation Strategies like Redundancy with critical subsystems, such as communication and propulsion, were identified for redundancy. Fault Tolerance with advanced error detection and recovery mechanisms were suggested for software and power systems. Preventive maintenance with regular checks and updates for components prone to degradation, such as batteries and sensors. Risk reduction was particularly evident in the propulsion and software systems [9].

FMECA provides a structured methodology for identifying and addressing potential risks, ensuring spacecraft resilience in challenging environments. The process enhances system reliability by focusing resources on the most critical failure modes. The study highlighted significant interdependencies among spacecraft subsystems. For example:

- Power system failures directly impact communication, thermal, and life-support systems.
- Software errors can cascade into mechanical or electrical malfunctions.

A holistic view of system design and operations is essential to address these interdependencies.

Modern spacecraft increasingly rely on autonomous systems, which introduce complex failure modes. Ensuring fault tolerance in such systems requires advanced techniques like formal verification and machine learning for software complexity measurement. While redundancy reduces risk, it increases cost, weight, and system complexity. Optimal trade-offs must be achieved to balance safety with mission constraints. As space missions evolve toward higher autonomy and adaptability, traditional FMECA processes need to incorporate real-time risk assessment and dynamic failure handling capabilities. The results align with industry standards such as NASA-STD-8719.13, demonstrating the FMECA's role in meeting safety and reliability benchmarks. **Future Prospects include e**merging technologies, such as AI-driven diagnostics and advanced simulation tools, can enhance the effectiveness of FMECA in spacecraft operations. Real-time monitoring and predictive maintenance tools can further reduce risk and increase mission success rates.

V CONCLUSION

Failure Modes, Effects, and Criticality Analysis (FMECA) is a vital tool for ensuring the safety, reliability, and success of complex systems like spacecraft operations. By systematically identifying potential failure modes, evaluating their effects, and prioritizing critical risks, FMECA provides a robust framework for proactive risk management. This paper demonstrated how FMECA can be applied to spacecraft operations, highlighting its importance in addressing challenges posed by the harsh space environment, intricate system interdependencies, and mission-critical functions. The analysis emphasized the need for redundancy, robust design practices, comprehensive testing, and adherence to safety standards. The outcomes of FMECA help engineers and mission planners to implement effective mitigations, from improving software fault tolerance to enhancing material durability and subsystem reliability. As space exploration advances, the use of FMECA will remain a cornerstone for ensuring the resilience of spacecraft systems, safeguarding investments, and protecting human lives. By integrating FMECA into all stages of spacecraft development, from design to operational phases, organizations can enhance mission success rates and foster continuous improvements in system reliability. In conclusion, FMECA is not only a technical tool but also a strategic asset in the pursuit of safe and sustainable space exploration.

ACKNOWLEDGMENT

Authors deeply acknowledge the support and encouragement extended by staff of computer science department for their valuable support throughout this activity.

REFERENCES

[1] IEC 60812 “Procedures for failure mode and effect analysis (FMEA)”

[2] BS 5760-5 “Guide to failure modes, effects and criticality analysis (FMEA and FMECA)”

[3] SAE ARP 5580 “Recommended failure modes and effects analysis (FMEA) practices for non-automobile applications”

[4] NASA Software Safety Guidebook - NASA-GB-8719.13

[5] Space product Assurance - FMEA/FMECA analysis - ECSS-Q-ST-30-02C

[6] Using FMEA to Improve Software Reliability, Kraig Strong, Excerpt from PNSQC 2013 Proceedings

[7] SW FMEA for ISO-26262 Software Development, Hyung Ho Kim, https://www.researchgate.net/publication/308858523

[8] Software Safety Analysis of Ball Position Control System using SFMEA, Kadupukotla Satish Kumar, Panchumarthy Seetha Ramaiah, International Journal of Computer Applications (0975 - 8887) Volume 143 - No.5, June 2016

[9] Failure Modes and Effects Analysis for a Software-Intensive Satellite Control System, Myron Hecht, Eltefaat Shokri, Elisabeth A. Nguyen, https://www.researchgate.net/publication/265851785