



Reliability analyses and risk assessments for restricted planetary sample return missions

Giuseppe Cataldo^{a,*}, Kyle Grello^a, Amy Braverman^b, Peter Gage^{c,d}

^aNASA Goddard Space Flight Center, 8800 Greenbelt Rd., Greenbelt, MD 20771, USA

^bJet Propulsion Laboratory, California Institute of Technology, 4800 Oak Road Dr., Pasadena, CA 91109, USA

^cNeerim Corporation, 5937 Chelton Dr., Oakland, CA 94611, USA

^dNASA Ames Research Center, PO Box 1, Moffett Field, CA 94035, USA

Abstract

Restricted planetary sample return missions aim to bring back to Earth material from solar system bodies which, according to scientific consensus, might have hosted indigenous life forms. These missions must comply with backward planetary protection requirements to protect the Earth-Moon system from potentially harmful contamination from these bodies. This work describes multidisciplinary reliability analyses used to support the elaboration of an assurance case for a Mars sample return, although the methodology is relevant for any mission in the restricted return category. The assurance case requires both quantitative and qualitative evidence to justify the approach for a safe potential return of the sealed Martian sample tubes that the Perseverance rover has been collecting on Mars. Specifically, standard reliability techniques were employed to assess contributions to quantitative targets that correspond to a 0.999999 probability of maintaining containment of the Martian material through delivery to Earth, while qualitative assessments were made to support a low-credibility impact determination to backward planetary protection. These quantitative targets represent engineering goals that would be assessed to prove that all precautions being taken for the safety of the missions are, or will remain, operational and implemented in a robust manner. A mathematical framework was also created that enables probabilistic success tree analyses with any kind of probability distributions and dependencies among the tree events, while interrogating the relationships between different parts of the tree. This approach extends the state of the art from more traditional probabilistic risk assessments and overcomes the limitations of current reliability analysis software.

© 2025 Published by Elsevier Ltd.

Keywords: Reliability, mission success, planetary protection, restricted sample return, assurance case, fault tree analysis

1. Introduction

Due to their complexity and global significance, space missions require thorough reliability analyses and risk assessments during their development phase to ensure mission success. While some of these risk assessments follow standard procedures that are common to all space missions, as is the case for rocket launches for example, other assessments depend on the nature of the mission itself. Missions with humans on board or returning material to Earth from planets that might have hosted indigenous life require additional analyses to ensure the safety of the crew or of Earth's biosphere.

*Corresponding author.

Email address: giuseppe.cataldo@nasa.gov (Giuseppe Cataldo)

There are several well-known approaches available to model and analyze system failure modes and reliability, including fault tree analyses (FTA), failure mode effects (and criticality) analyses (FME(C)A), and reliability block diagrams. FTAs have been used since the 1960s [1] in a variety of areas beyond aerospace such as nuclear engineering [2, 3], power systems [4], robotics [5, 6] and many others. The authoritative work by Ruijters and Stoelinga (2015) [7] provides a comprehensive survey of fault tree analysis, establishing the current state of the art in modeling, analysis and tools. It identifies key limitations in traditional FTA approaches and highlights the need for more sophisticated methodologies to handle complex, dynamic systems, serving as a baseline for understanding how recent research has evolved beyond classical reliability analysis techniques. These include algebraic [8, 9], Bayesian [10, 11, 12], Petri Nets [13, 14], Markov Chain [15, 16, 17] and Monte Carlo [18, 19, 20] methodologies. Recent work by Liu et al. (2024) [21] demonstrates how traditional FTA and FMECA methods are being adapted for extreme operating environments where conventional analysis assumptions may not hold. The integration of fuzzy logic represents an evolution beyond deterministic classical approaches and contributes to the field by applying fuzzy fault tree analysis to subsea manifold systems, addressing the unique challenges of underwater oil and gas operations. Other advances can be found in Hu et al. (2024) [22], whose work on autonomous underwater glider fault diagnosis represents a paradigm shift from purely analytical approaches to hybrid methodologies that combine physics-based reliability models with data-driven machine learning techniques.

The work presented here introduces innovations in the application of reliability analysis tools such as FTA/FMECA and their numerical implementation for space missions whose requirement verification can be performed under an assurance case framework. An assurance case is an assembly of evidence and arguments asserting that safety has been robustly addressed, and it may combine quantitative and qualitative evidence into a unified case that justifies the approach adopted to achieve the mission goals [23]. The missions of concern here are restricted sample return missions, which are defined as those that would be returning to Earth material from a solar system body which, according to scientific consensus, might have harbored indigenous life forms [24].

In line with current NASA planetary protection policies [24, 25], restricted sample return missions are required to comply with Backward Planetary Protection (BPP) requirements associated with the return of planetary samples to Earth's biosphere. These BPP requirements affirm the need to protect the Earth-Moon system from possible harmful extraterrestrial contamination that may be returned from other solar system bodies. For this type of mission, NASA mandates a strategy of robust containment, that is "utilizing dissimilar, redundant approaches to achieve an overall containment system that is minimally sensitive to engineering operations, stressful environmental conditions, and credible off-nominal scenarios in use from point-of-collection to containment in a receiving facility on Earth" [24].

An example of restricted sample return mission is Mars Sample Return (MSR), a series of missions conceived of by NASA and the European Space Agency to bring to Earth sealed tubes of rock cores, regolith, and atmospheric samples from Mars [26]. The study of these samples could provide answers about the geologic and climate history of Mars, including the potential for ancient life [27, 28, 29, 30, 31]. This paper will use the MSR architecture concept that was established in December 2023 as an example application of a broader methodological approach for prediction of system reliability. Under said architecture, the Sample Retrieval Lander (SRL) [32, 33] would land on Mars, retrieve the sealed sample tubes, and launch them into Mars orbit inside a container called the Orbiting Sample (OS). The Earth Return Orbiter (ERO) [34, 35] would detect the OS in Mars orbit and, with the Capture, Containment, and Return System (CCRS) payload [26] that would sit on top of the ERO spacecraft, would capture the container, protect it inside another container to avoid the release of potentially hazardous Mars particles¹, and return it to Earth through an Earth Entry System (EES). This would be a vehicle designed to withstand the loads imparted by Earth reentry and landing.

Under NASA policy [25], the development of an assurance case is proposed as an option to achieve BPP compliance for restricted sample return missions. In the context of the MSR approach that was being developed at the time of this work, BPP performance against quantitative targets that correspond to a 0.999999 probability of maintaining solid particle containment within each of the three risk elements (in-flight particle control, particle containment assurance during Earth approach/entry/descent, and particle containment assurance during Earth landing – see Section 2) would be reported within the assurance case. The specific qualitative and quantitative arguments to be used in the assurance case, as well as its overall structure, remain in development. The overall success of safety precautions of the mission

¹These are defined as any particles ≥ 50 nm in size that have not been sterilized.

would be assessed in the context of both the engineering approach (i.e., how potential failure states are identified and addressed) and the probability of successful implementation estimated through testing or modeling. This approach provides assurance when the desired success probabilities are extremely high and therefore difficult to assess with certainty.

Overall, this paper presents methodologies and tools that were developed to bridge existing gaps in an effort to improve the state of the art. While the paper refers to work performed through December 2023 (and as such it should be seen as a case study and a snapshot in time), these techniques are applicable to BPP assessments of any architecture and represent a potential additional tool at hand for restricted sample return missions. Specifically, this manuscript describes the reliability analyses performed to support a preliminary quantitative risk assessment to verify BPP compliance as part of a possible broader assurance case, along with qualitative information pertaining to the identification and treatment of potential failure states.

Such verification was established and supported utilizing traditional reliability program practices, including FTA and FMECA [36, 37]. While FTA and FMECA are standard reliability analysis techniques implemented on many aerospace projects, their implementation in this application as the guiding framework for establishing compliance with complex BPP metrics and characterizing overall planetary risk was innovative. Specifically, the logic framework seen commonly in FTA (detailed further in Section 3.1) was utilized to capture all the contributing factors (e.g., failures, faults, environment) to each BPP risk element. Within that framework, and based on available models or data, each of those factors was then classified as requiring 1) a detailed probabilistic model to assess contributions to 0.999999 targets or 2) a qualitative risk assessment developed to support a low-credibility impact determination to BPP. Further, the systematic process of identifying faults and their associated mitigations in a FMECA (detailed further in Section 3.2) was used as a significant input to the detailed qualitative assessments to determine if there were acceptable levels of risk associated with the contributing factor. This linked the FMECA efforts to the overall FTA-based BPP risk element framework, as opposed to more traditional risk assessment approaches such as those applied to the Space Shuttle, where quantitative fault trees/probabilistic risk assessments were the main focus [38, 39, 40, 41]. This process was iterative in nature and substantially different from common design practices that use reliability analysis when the design is complete to check the system performance and fix anything catastrophic. Conversely, in the case presented here, the hardware and concept of operations were influenced by this BPP analysis right up to the finalization of the preliminary design, looking at planetary protection requirement violations, thus identifying risk mitigation strategies and/or other ways to eliminate such non-compliances.

Finally, another novel aspect is the numerical execution of the FTA-based probabilistic success tree analysis. In standard practice and with common software packages, the types of probability density functions are limited to analytically known forms and often do not allow for potential statistical dependence among parameters. The complexity of restricted sample return missions requires less restrictive assumptions on the probability density functions while being able to address these dependencies. The work presented here overcomes these limitations, bringing an additional contribution to the state of the art (see, for comparison, Ref. [42], where an analytical methodology is described that can handle arbitrary types of probability density functions but without dependencies among basic events).

This manuscript is organized as follows: Section 2 provides a brief review of the reliability requirements in the context of planetary protection for restricted sample return missions. Section 3 presents a description of the different types of reliability analyses performed. Section 4 shows the mathematical and numerical approaches to performing a success tree analysis. Finally, Section 5 provides a summary of findings and an overview of future perspectives.

2. Planetary protection requirements

As part of the MSR efforts (described in detail in Refs. [34, 43]) to comply with planetary protection policies [24, 25], several qualitative and quantitative reliability requirements were established for the CCRS payload, which would execute the capture and return of the sealed Martian sample tubes to Earth. The three following planetary protection risk elements were defined and acceptable risk levels were established as mission success/reliability requirements for each one of them:

1. In-flight particle control

Particle control aims at tracking and managing particle transport while guiding the design of particle barriers and containers. In particular, particle transport tracks everything that cannot be contained. It is worth noting that the

Sample Retriever Lander would try to limit the particle load on the OS before inserting it into the Mars Ascent Vehicle and reaching CCRS. Additionally, particle loads on the exterior surfaces of the ERO spacecraft would be minimized to ensure particles are not disturbed and released later in the mission within Earth's biosphere.

2. Particle containment assurance during Earth approach, entry, and descent

Containment of the sealed sample tubes through approach, entry, and descent is fundamental to both mission success and compliance to planetary protection requirements. In fact, the EES would travel unprotected from micrometeoroid and orbital debris during the approach sub-phase, i.e., after it is released from ERO a few days before landing. Damage to the EES from impacts caused by micrometeoroids and orbital debris over the lifetime of the ERO mission may therefore cause structural integrity failure during the entry and descent sub-phases through the Earth's atmosphere. The approach, entry, and descent risk element is differentiated from the landing risk element by two features: 1) micrometeoroid and orbital debris risk is only estimable through modeling that carries significant uncertainty [44], 2) structural failure on entry has a high potential for material release and little-to-no potential post-release mitigation [45]. Another element of containment assurance during this phase is to redirect the ERO spacecraft away from the Earth-targeting trajectory after EES release to minimize the risk that uncontained material existing on or within the spacecraft enters into Earth's biosphere.

3. Particle containment assurance during Earth landing

Containment upon landing requires withstanding the impact loads when touching the soil of the Utah Training and Test Range. As noted in Ref. [43], *Containment Not Assured* (CNA) is defined as the state in which one or more requirements for ensuring containment of Mars material have not been met. CNA does not necessarily equate to Mars material release. If the probability of CNA, P_{CNA} , exceeds a target probability, additional analyses and/or mitigation measures may be undertaken.

It is important to note that after dual containment is established in Mars orbit, there is no credible load case that would break containment until entry loads are induced in Earth's atmosphere. In addition, during transit, several biocidal space conditions including vacuum, solar heating, and solar UV irradiation, to name a few, as well as the lack of liquid water, enforce biological stasis, preventing any potential biological entity to survive [46].

The overall goal of the methodology used in this case study to support performance verification was to evaluate performance against quantitative targets corresponding to a 0.999999 probability of maintaining containment implementation for every risk element described above. Each of the risk elements was broken down and allocated to the various causal factors that contribute to them. Those causal factors were determined iteratively and systematically using functional/hardware breakdowns of the risk elements and documented in requirements flows and a corresponding fault tree/success tree analysis. In some cases, where a quantified estimate of the causal factor could be established with confidence (test data, modeling, etc.), they were allocated quantitative probabilistic requirements. In other cases, where a quantitative basis could not be established with certainty, those causal factors were further analyzed using a more qualitative assurance case risk assessment.

In addition to the acceptable risk level requirements, several requirements related to single- and dual-fault tolerance were established for CCRS related to reducing risk of contamination. Those requirements, which help guide many elements of the CCRS design, covered the following:

- Ensuring the EES and its contained samples are not inadvertently released with an Earth trajectory before a predetermined release window
- Propagation of faults that would impact the ability to perform the ERO spacecraft's Earth avoidance maneuver, which is designed to move ERO off of the Earth intersect trajectory required for EES release
- Propagation of faults that would impact the ERO spacecraft's safety critical monitoring to ensure that the state of safety-related EES release inhibits are well known before starting any Earth-targeting maneuvers

The strategy for establishing compliance with these single- and dual-fault tolerance requirements is further discussed in Section 3.1 and Section 3.2.

While this paper concentrates on requirements that are enumerated in planetary protection standards [24], there may be additional low-likelihood, high-consequence risks that are currently underappreciated but could have a meaningful contribution to mission risk [45]. Human factors such as insider threats or cybersecurity (for example, a

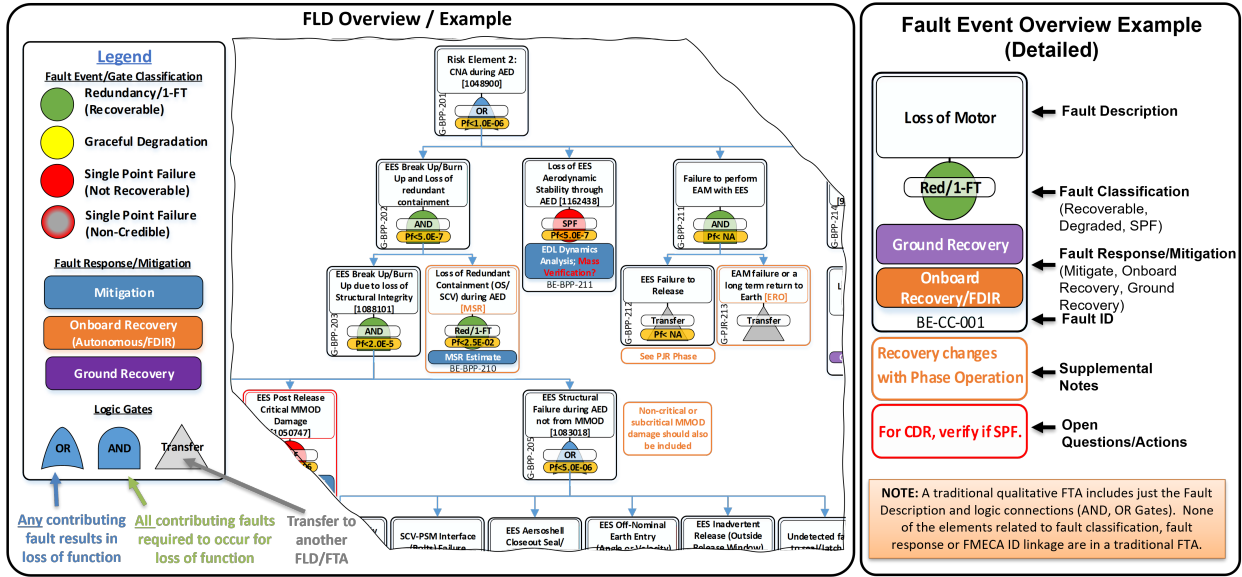


Figure 1. Example of a fault logic diagram.

malignant intervention by bad actors or spacecraft interception before it reaches Earth) should not be ignored when the decision is ultimately made to release the samples for return to Earth.

3. Reliability analyses

Verification of the various quantitative and qualitative planetary protection requirements was supported by multiple reliability analyses, including fault tree analysis (FTA) / fault logic diagrams (FLDs), failure modes, effects, and criticality analysis (FMECA), and numerical reliability predictions or estimates. These analyses evaluated system faults or failures and used various methods to characterize mission impact and the associated credibility and likelihood. Assurance cases and verification of the planetary protection fault tolerance requirements were primarily supported by FTA and FMECA, while verification of the probabilistic BPP requirements for each risk element was supported by FTA and numerical reliability predictions.

3.1. Fault Tree Analysis / Fault Logic Diagrams

FTA is a failure space-based logic tree that follows a “top-down” development approach, starting with the top event of interest (e.g., hazard, failed end-state, feared event) and working down to contributing component fault/failure events (including loss of function). FTA logic trees provide a hierarchical decomposition of possible faults and failures from the top event of interest to system functions to the driving hardware and software elements. Failure space encompasses all possible failure modes, conditions, and states that could lead to system malfunction and is the complement of the success space, where the system operates correctly. The content of the FTA draws from several sources of information, including the design (per requirements), success trees, functional decomposition, and the FMECA (see Section 3.2).

FLDs, which are based on the same failure space and top-down logic-based graphical architecture of events of interest, discriminate among events that minimally affect the mission, those that result in graceful degradation of the system, and those that result in catastrophic loss of mission (e.g., due to single-point failures); all are used to identify risk drivers. The FLD highlights the system characteristics and behavior necessary to control the outcome of these events and thus minimize potential problems through onboard fault protection, contingency procedures, and constraints or mission rules. Additionally, FLD development can identify gaps where fault management intervention (on orbit or on ground) is required (Fig. 1).

Entry ID Sys-Assy-###	Item/Interface Definition				Failure		Failure Effects Pre-Mitigation (e.g. no redundancy)				Mitigation		Criticality Post Mitigation				
	System	Assembly	Interface Item	Function / Description	Failure Mode	Failure Cause	Phase / Operational Mode	Local: Part / Circuit	Next Higher: Board, Box or Assy	End Effects: Mission	Failure Mode Detection	Compensating Provisions: 1) Design/Analysis (e.g., Redundancy, Structural Margins, Preventative Features, etc.) 2) Testing / Inspection 3) Manufacturing / Assembly 4) Other (Work-arounds, etc.)	Likelihood	Consequence	Severity	D/P	RPN
SD-CC-009	S&D	Cable Cutters	Pyro Cutters (2) for 1" cables	Provides the ability to sever spacecraft thermistor and spawire cable bundles;	Pyro device fails to fire;	Degraded initiator; Booster failure; Cutter failure/binding; Manufacturing defect;	LMOSP - Containment Phase (COP)	Spawire and/or Thermistor cables are not severed/cut;	Loss of ability to jettison CE; Mission return would take longer;	Degraded ability to return samples/main containment; Degraded ability to meet full mission success	Telemetry from the Retraction Mechanisms	1) Design/Analysis - Fully redundant initiators, boosters & electrical connections (Mechanically single string); Both initiators capable of fully severing the cable and both are fired; Use of NASA standard initiators (NSI); Braycote 601EF space-rated lubricant used for O-rings/seals; 2) Testing / Inspection - Vibe, Acoustic, Thermal, Stress, Proof load tests; Non-synchronous cable cutter activation test to confirm no binding during retraction; Functional tests by Vendor; 3) Manufacturing / Assembly - NDE, Clean-Room Assembly, adherence to Contamination Control Plan (CCP); Teflon/Kapton wrap between cable bundles; 4) Other - SPF risk mitigations documented in verifications of S&D SPF Requirement (CCRS-STRUCT-1126005)	1	3	3	5	15
SD-CC-010	S&D				Inadvertent firing of pyros;	Self actuation; Inadvertent electrical actuation;	LMOSP - Containment Phase (COP)	Spawire and/or Thermistor cables are inadvertently severed/cut	Loss of CE avionics and sensor suite; Loss of mission if this occurs before capture/containment;	Loss of Sample Return/Containment; Minimum mission success not achievable;	Telemetry from the Retraction Mechanisms	1) Design/Analysis - Inhibits in the avionics release card architecture and Thermal analysis to ensure activation temperatures are not exceeded; 2) Testing / Inspection - Vibe, Acoustic, Thermal, Stress, Proof load tests 3) Manufacturing / Assembly - NDE, Clean-Room Assembly, adherence to Contamination Control Plan (CCP); Teflon/Kapton wrap between cable bundles; 4) Other - Auto-ignition of pyros are significantly higher than the max proto-flight temperature (+90C; ZPP is >450C & THPP is >400C); Charge material chosen for aging performance & pedigree;	1	4	1R	5	20

Figure 2. Example of a FMECA extracted from a larger table

Each of the MSR planetary protection risk elements identified in Section 2 (particle control, CNA during approach, entry, and descent, and CNA during landing) was modeled using an FTA/FLD approach to assess all potential contributing causal factors. Where applicable, the FTA/FLD included probabilistic requirements for top-level events, allocations down from those top-level requirements/events, and predicted values for lower-level contributing events. The predicted values came from a variety of sources, including micrometeoroid and orbital debris models, structural models, and reliability prediction techniques, which will be discussed in more detail in Section 3.3. The roll-up of those predicted values versus the probabilistic requirements was calculated based on the logic gate architecture within the probabilistic success trees along with their identified lower-level event failure rates/distributions. This will be discussed in more detail in Section 4.

In addition, within the FTA/FLD graphical display, it is easy to identify where single- and dual-fault tolerance requirements may or may not be violated based on the clear identification of single-point failures and single-fault tolerance. This was used extensively and on an iterative basis to determine where there were violations of the planetary protection single- and dual-fault tolerance requirements and to identify high-level risk mitigation strategies, architecture retention rationales, and/or pathways forward to eliminate the violation.

3.2. Failure Modes, Effects, and Criticality Analysis

The FMECA is a systematic “bottom-up” approach that starts with a failure analysis of the components/major hardware assembly elements to determine the impacts of failure on the component, sub-system/system, and mission. The purpose of the FMECA is to identify where there is the potential for irreversible physical and/or functional damage, identify how damage/failures propagate or not, identify how damage/failures impact the system (locally and globally), and assess mission failure risks and response/recovery plans. A FMECA assesses causes/mechanisms, effects, severity, likelihood, and detectability of failure modes. Furthermore, within the FMECA, detailed mitigating features or actions are identified for each failure mode. The content of the FMECA for CCRS drew from several sources of information, including the design (per requirements), mission equipment lists, interface control documents, and functional decomposition.

Within the FMECA, failure modes for each major hardware element of CCRS were analyzed at the component level to understand impacts on the component, sub-system/system, and ultimately the mission and overall BPP. The results of the FMECA were cross-checked with the FTA/FLD to ensure all component-level failures that resulted in impacts to the BPP risk elements were adequately included as contributing events in the overall FTA/FLD architecture, which was ultimately used to support verification of probabilistic BPP requirements. For example, performing the detailed FMECA for containment sensor false alarms allowed for capturing more accurate faults, mitigations, and credibility rankings in the CNA sections of the BPP risk element FTAs/FLDs.

The mitigations and compensating provisions identified for faults in the FMECA were also utilized as the basis for many of the assurance case risk assessments for faults relevant to the BPP risk elements that could not be quantified with any level of certainty.

Additionally, within the FMECA documentation, it was easy to identify where single-fault tolerance requirements may or may not be violated, based on the clear identification of single-point failures and their impacts on overall mission success criteria (including maintaining BPP). Similar to the FTAs/FLDs, this was used extensively and on an iterative basis to determine where there were BPP single-fault tolerance requirement violations and identify high-level risk mitigation strategies, architecture retention rationales, and/or paths forward to eliminate the violation. The FMECA and FTA/FLD were both used for assisting in determining compliance with single-fault tolerance requirements, but the FTA/FLD was generally more effective in identifying dual-fault tolerance violations as the FMECA focuses more on single-failure analysis.

3.3. Numerical reliability assessment and prediction

In support of FTA/FLD development and ultimately probabilistic requirement verification, numerical reliability predictions were developed as needed for contributing events to the BPP risk elements (see Section 2). These assessments were generally focused on events outside of structural failure and micrometeoroid and orbital debris impacts, which were estimated using other techniques that have less uncertainty than standard reliability structural calculations. Further details can be found in Section 4.1.

Reliability prediction methodology can vary based on the type of component (electrical, mechanism/electro-mechanical, structural), availability of data, and intended usage environment. The general approach for each of those assessment types is detailed in the following sections.

3.3.1. Electronic components

Electronic reliability predictions come from a variety of methods and sources, which were identified on a per-component basis within the detailed reliability analysis. Listed by order of preference, electronic component reliability data is based on the following:

- Manufacturer-provided reliability test data or specifications
- NASA Goddard Space Flight Center's historical reliability performance data
- Handbooks (e.g., [47, 48, 49, 50, 51])

Handbook data, while sometimes used for quick trade studies and initial estimates for custom-built hardware or other units for which data cannot be obtained, is generally not as accurate as vendor-verified performance data on the actual component being utilized or historical performance of like or similar components on other NASA projects. However, handbook data are generally more readily available and, using common Bayesian statistical methods, it can provide the basis for analyses utilizing actual component-reliability performance data.

If handbook data were utilized, failure rates were first derived from Ref. [47] following its parts count approach. This approach involves first building a system component baseline based on a system or subsystem parts list. The failure rate per component is then calculated utilizing a base failure rate for a similar or identical component provided within Ref. [47], which is then modified based on chosen quality levels, environmental factors for the given mission profile, and operating parameters. As more detailed component operating temperature and design parameters (power rating, voltage stress, etc.) became available, the analysis was generally transitioned to a more accurate parts stress-based analysis.

This process was adhered to utilizing industry-standard reliability prediction software PTC Windchill [52, 53], which allows for both a parts count calculation approach based on Ref. [47] and a more detailed parts stress approach. In general, a parts count prediction method, as described in Notice 2 of Ref. [47], was used for the CCRS payload electronic reliability prediction analysis due to the lack of maturity of the hardware design and conservative nature of parts count methods. As the electronic designs mature, a more accurate part stress approach can be utilized.

Due to most electronics requiring multiple faults before impacting BPP, the mechanical and structural probability of failure estimates drove the preliminary results.

3.3.2. Mechanisms and electro-mechanical components

Reliability assessments and predictions of mechanisms and electro-mechanical components can also come from a variety of sources. Like electronic components, mechanism reliability derived from manufacturer-provided reliability test data (e.g., mechanism life tests), specifications, or historical reliability performance data is preferred if available. Most projects do not have the time and/or money to pursue sufficient mechanism testing to prove reliability with any level of confidence. Therefore, if that is the case, and if comparable heritage-based reliability data are not available, other methods must generally be pursued.

Physics-based models of reliability would be the next preferred approach. This can include stress-strength-based models of reliability or mechanical reliability models outlined in sources such as the Naval Surface Warfare Center (NSWC) Mechanical Reliability Handbook [49].

If those models are insufficient for modeling a specific mechanism or if detailed component information (e.g., material, stress levels, dimensions, cycling rate) is not yet available, then industry-standard mechanical reliability databases such as the Non-Electronic Parts Reliability Database [50] are utilized. Again, these databases generally are not as accurate as vendor-verified performance data on the actual component being utilized or the historical performance of like or similar components on other NASA projects. However, handbook data are generally more readily available and provide a rough order-of-magnitude estimate in the absence of more preferred mechanical reliability modeling approaches.

Physics-based models of reliability, developed using NSWC-11-based techniques, were used for a majority of the mechanism probability of failure estimates related to BPP causal factors.

3.3.3. Structural components

Structural components, including those that are fracture-critical or fatigue-sensitive, are generally assumed to have a high reliability $R(t) = 100\%$, or a failure rate $= 0$. For those cases, high levels of reliability can be assumed based upon generally low cycle-required lives and standard structural design practices, which drive a requirement for sufficient design margin (margin of safety $MS > 0$) over ultimate load cases [54]. However, due to the order of magnitude of the BPP probabilistic requirements, these normal reliability assumptions were not adopted, and the CCRS project opted for more detailed probabilistic structural modeling for any structure-based failures (see Section 4.1).

4. Probabilistic success tree analysis

A traditional quantified fault tree exists in failure space and thus probabilities of failure are represented throughout the identified contributing events. In the case of the BPP risk assessment, a success space-oriented probabilistic event tree, with a detailed understanding of dependencies between individual events, was desired to characterize the overall risk to Earth's biosphere. Therefore, a slightly modified success tree analysis was developed using fault tree-like processes to meet this goal.

The developed probabilistic success tree is a tree-structured, directed graph consisting of vertices and directed edges that connect some of those vertices to one another. Each vertex represents a requirement, and each edge represents a dependency of that requirement on one or more *child* vertices. In the success tree analyzed here, every vertex has exactly one *parent*. Vertices with no children are called *leafs*, and a vertex with no parent is called a *root*. Vertices that are neither leafs nor roots are called *interior* vertices, and implement either "AND" or "OR" logic that combines the information provided by their children. In our rendering, leafs are placed at the top of the tree, directed edges flow downward towards the root at the bottom of the tree. For a visual example, please see Figure 4.

The probabilistic success tree analysis starts at the leafs, whose behavior is captured through the results of Monte Carlo experiments over a large number, say B , of independent trials based on the probabilities gathered as described in Sections 3.3 and 4.1. Each trial is either a "success" or a "failure" depending on whether the requirement corresponding to the leaf is met or not. The aggregate result is generally reported as a probability of CNA for the leaf ($P_{CNA} = n_{CNA}/B$, where n_{CNA} is the number of cases in which CNA occurs), and as long as the leafs are all independent, no information is lost. That is the case in the experiment we analyze here, but in general it may not be. Our success tree analysis method handles dependence by maintaining the full, length- B sequences of successes (coded as ones) and failures (coded as zeros) for each leaf vertex and propagating them all the way down the tree to the root. As we shall see, this allows us to compute measures of dependence between *any* two vertices in the tree, facilitating

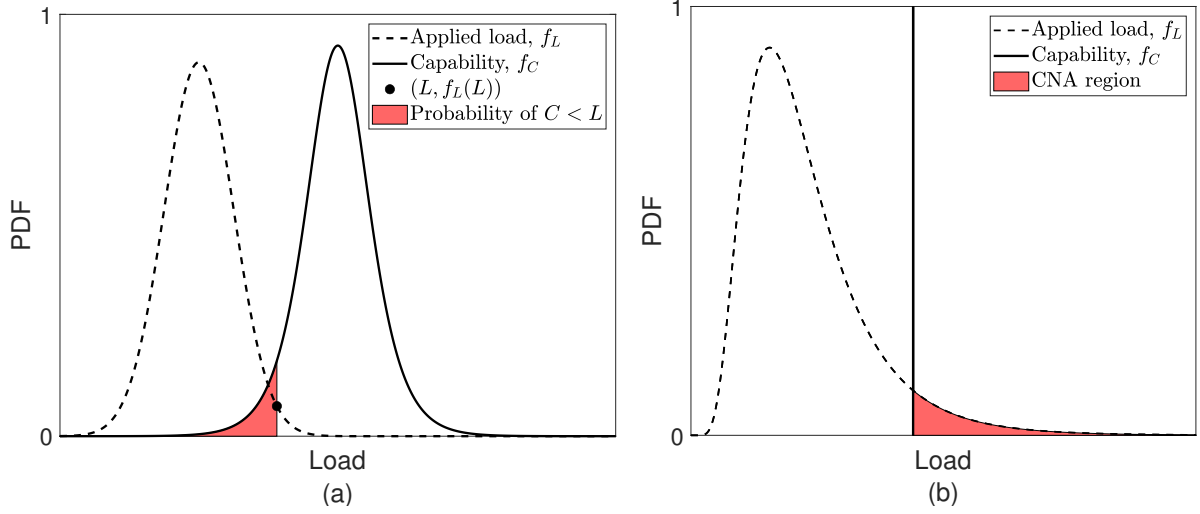


Figure 3. Probability density functions for applied load, f_L , and capability, f_C . At left, the probability of a specific load L is denoted with a circle, and the cumulative probability of the capability C being lower than L is shaded red. At right, for the special case where the capability is defined by a precise threshold, the red shading indicates the CNA region.

better understanding of the success tree's internal dependencies and structure than is possible with traditional analysis software.

In the following subsections, we describe the computational experiments for which the outcomes define our success trees. Then we discuss the data structures, implemented in the Julia programming language using packages `Graphs.jl` and `MetaGraphs.jl`, which we use to represent success trees and propagate their leaf probabilities down to the root. Finally, we carry this calculation out for BPP risk element 3 and present an analysis of the results.

4.1. Experiments and data collection/generation

Engineered systems fail when the applied environment or load exceeds the capability or strength of the system to accommodate that load. A population of nominally identical systems can have a distribution of actual capability, due to variations in properties of the system, which can be affected by details of material processing, fabrication, and system integration. Similarly, there is a distribution of possible service environments to which a system can be exposed. Figure 3(a) shows the relationship between load and capability distributions. The probability that CNA occurs at a specific load L is the combined probability that the load L is applied (the point indicated in Fig. 3(a)) AND the cumulative probability that the capability C is lower than L (the shaded region in Fig. 3(a)). The total probability of CNA is given by the integration of this combined probability for all load levels, as indicated in the equation below:

$$P_{CNA} = \int_0^{+\infty} f_L(x) \left(\int_0^L f_C(y) dy \right) dx \quad (1)$$

For systems with known PDFs for both loading and system capability, this integration can be performed directly. For systems with negligible variability in capability, the PDF for capability is a single spike, as shown in Fig. 3(b). At loads below this threshold capability, the probability of CNA is zero, because the cumulative probability that C is lower than L is zero. Above the threshold capability, the cumulative probability that C is lower than L is 1, so the total probability of CNA is simply the total probability that the applied load exceeds the capability threshold (shaded area in Fig. 3(b)).

As discussed in Section 3.3, capability PDFs for electronic and electro-mechanical components and mechanisms can be obtained from the literature, vendor manuals or data sheets, and from previous missions, tests or experiments, to support calculation of total probabilities. PDFs are often not available a priori for complex systems for which both load and capability depend on a large number of parameters. In such cases, it is common to use Monte Carlo analysis to run a series of trials that make pairwise comparisons of load and capability for randomly assigned values of all

relevant independent parameters that drive load and capability values. With a sufficiently large number of trials, the aggregate fraction cases with capability less than load provides an estimate of failure rate.

However, given the high reliability values (≥ 0.999999) imposed by requirements, the Monte Carlo approach required thousands or millions of samples to be able to look far into the tails of the distribution. This challenge would be exacerbated when dealing with computationally expensive high-fidelity models, which could only be used for a very limited number of runs and provide only a step-like function with very poor resolution, especially in the tails. Simplified versions of high-fidelity models, called low-fidelity surrogates, could be used millions of times and would achieve the required smoothness in the tails. However, these were subject to additional uncertainty induced by bias and/or variability due to the fact that the low-fidelity model was only an approximation to the high-fidelity model. With such stringent requirements, one could not rely on low-fidelity models alone.

Other approaches (summarized in Ref. [55]), such as importance sampling, subset simulations and first/second-order reliability methods (FORM/SORM), suffer from the same limitations. Instead, we adopted the multi-fidelity importance sampling approach described in Ref. [56] for two reasons. First, a multi-fidelity approach leverages a series of fast, low-fidelity models to generate millions of samples while keeping a few (generally ≤ 25) expensive, high-fidelity model runs in the loop to retain accuracy. The high-fidelity models, in our case, could only be used a handful times because their large computational cost was at least 2.5 hours per run. Second, the approach in Ref. [56] proved in offline experiments that it could recover probabilities of success as high as 0.999999999. This is three orders of magnitude greater accuracy than is specified by the requirements, thus offering a powerful tool to estimate such stringent values.

4.2. Models

4.2.1. Approach, entry, and descent

Information about micrometeoroid and orbital debris risk is generally provided by NASA’s standard environment models: the Meteoroid Engineering Model (MEM) [57] and Orbital Debris Engineering Model (ORDEM) [58]. These models provide directional descriptions of impactor flux, density, velocity, and mass. Results from these two models are then fed into NASA’s Bumper or The Aerospace Corporation’s Meteoroid and Orbital Debris Risk Assessment (MODRA) software tool to map the environmental distribution of impactors to the vehicle’s surface. To determine the consequences of impacts, the Bumper/MODRA assessment relies on ballistic limit equations [59, 60], which relate the severity of the impact (in terms of penetration depth) to several parameters such as impactor diameter, velocity, incidence angle and impactor/target material properties. Ballistic limit equations are low-order models, and they are tailored to correlate with experimental data from ground-based hypervelocity impact testing and higher-order models. For MSR, the dominant threat component is micrometeoroid exposure due to the long duration of the ERO spacecraft’s journey through interplanetary space and in Mars orbit. Since average meteoroid impact velocities significantly exceed ground-based testing capabilities (< 7 km/s), numerical simulation tools called hydrodynamic codes (hydrocodes) are used to simulate realistic impact scenarios. Hydrocode results are coupled with physical hypervelocity impact test data to generate ballistic limit equations that more accurately capture damage consequences over the full space of possible impactor parameter combinations. The ultimate outcome of the risk assessment is a probability of “critical damage”, defined as damage to the EES aeroshell that could result in *containment not assured* during approach, entry, descent, and landing. For additional details, see Ref. [44].

4.2.2. Landing

To predict key metrics pertaining to sample integrity and verify containment assurance upon landing, the System-Level Impact Model (SLIM) was developed [61, 62]. The SLIM is an LS-DYNA [63] finite element model of the EES landing event, in which all the key EES structural components, from the aeroshell to the samples within the sample tubes, are explicitly modeled, as is the soil upon which it lands. The full range of kinematic and soil conditions that the EES is required to withstand can be simulated with SLIM. This model was validated through experimental data gathered in a series of drop tests conducted on an impact tower at the Jet Propulsion Laboratory, where physical EES engineering models were accelerated downward and impacted a gravel bed, replicating the landing event. Impact velocities reached up to 60 m/s, well above the estimated flight landing velocity of ~ 43 m/s. For the soil, impact tests were conducted at the Utah Training and Test Range by lifting EES-like hardware via a helicopter and dropping it into soil that is representative of the Playa45 terrain in the EES landing ellipse.

4.2.3. In-flight particle control

For the particle control risk element, the probabilities were calculated either from the aforementioned micrometeoroid and orbital debris models or from reliability estimates as described in Section 3.3. Finally, whenever a probability estimate was not available from any of the methods and tools described herein, careful engineering judgment was relied upon and noted for future work.

4.3. Data structures and computation

The Julia Programming Language [64] provides a number of packages for representing and studying graph structures. The main package is `Graphs.jl` [65], which serves as a base for various others, including `MetaGraphs.jl` [66]. The Graph structure itself is the collection of vertices identified by integers in the order in which the vertices are created and directed edges specified by their starting and ending vertices. We represent requirement structures as a special type of graph known as a tree. For our purposes, trees are hierarchical graph structures in which each vertex has only one outgoing edge.

In our case, the structure of the tree will represent the relationships among requirements through parent-child relationships between vertices in the graph. The parent of a vertex is the destination vertex of its single outgoing edge. If a vertex has no parent, it is called the root of the tree. A vertex’s children are all the vertices of whom it is the parent. Vertices with no children are called leafs. Vertices that are neither the root nor a leaf are called interior vertices. We endow interior vertices with a logical type: AND vertices and OR vertices. For an AND vertex to be true, all its children must be true. For an OR vertex to be true, at least one of its children must be true.

`MetaGraphs` allows one to attach metadata to vertices and edges, if desired. We use `MetaGraphs` to append the following fields to each vertex in our tree:

- Vertex number (integer, e.g., 5)
- Name (Entry ID, e.g., BPP-RE3-005)
- Event (Fault/Event, e.g., CNA of the OS)
- Parent name (Parent ID if the vertex has a parent, NA otherwise, e.g., BPP-RE3-004)
- Parent number (Vertex number of parent if the vertex has a parent, NA otherwise, e.g., 4)
- Gate (AND, OR, root, or leaf)
- Marginal probability of CNA (P_{CNA} estimate, e.g., 10^{-6})
- X (placeholder for a vector of zeros and ones such that the proportion of ones is the marginal probability)

Edges do not have metadata and are identified by their source vertex and destination vertex. Every vertex knows its parent and children through the `inneighbors` and `outneighbors` functions defined in the `Graphs` package. Initially X is an empty vector.

Data resulting from experiments defined in Section 4.1 were used to define and populate the tree. Marginal probabilities of CNA, P_{CNA} , for the leafs were treated as the parameters of independent Bernoulli distributions, one for each leaf. In this setting, we define a “failure” as an outcome of zero, representing a sample (equivalently a trial of a Monte Carlo experiment) in which the requirement represented by a vertex was not met. A “success” is an outcome of one, indicating that a requirement was met. Henceforth we shall refer to a success as a “non-failure” in order to remind ourselves that probabilities of failure are typically small. The X field of each leaf was assigned a length- B vector of zeros and ones generated as $B = 10,000,000$ independent Bernoulli realizations with a non-failure probability of $p = 1 - P_{CNA}$. In the future, we expect to ingest X directly from computational model runs. These runs may be performed in a way that renders certain collections of leafs statistically dependent, but that changes nothing about how we handle these inputs. Dependence will be preserved as long as the b -th elements of X across the different leafs represent the same trial of the numerical or physical experiment.

Once the X fields of the leafs were populated, the next step was to propagate this information through the interior vertices all the way to the root. The interior vertices were processed in *topological order* [67], which ensured that all children of vertex were processed before the vertex itself. Now, let $ch(v)$ denote the set of vertices that are children

of vertex v . Let the X field of vertex v be denoted by $v.X$ and let the b -th entry of $v.X$ be $v.X[b]$. Algorithms 1 and 2 show how the X fields of interior vertices were constructed from the X fields of their children, for interior vertices representing AND and OR gates, respectively. The procedure finished when the X fields of all nodes had been calculated. At that point, the marginal probability of non-failure was computed as the average X field value, for interior vertices and ultimately for the root vertex.

Algorithm 1 AND gate logic

```

 $B \leftarrow 10,000,000$ 
 $v.X \leftarrow \mathbf{0}_B$                                  $\triangleright \mathbf{0}_B$  is the length- $B$  vector of zeros
 $Y \leftarrow \mathbf{0}_B$                                  $\triangleright Y$  holds the total number of non-failures across children of  $v$ 
for  $b = 1, 2, \dots, B$  do
  for  $u \in ch(v)$  do
     $Y[b] \leftarrow Y[b] + u.X[b]$ 
  end for
  if  $Y[b] == \#ch(v)$  then                         $\triangleright \#ch(v)$  is the number of children of  $v$ 
     $v.X[b] \leftarrow 1$                              $\triangleright$  If all children of  $v$  are non-failures, then  $v$  is a non-failure
  end if
end for

```

Algorithm 2 OR gate logic

```

 $B \leftarrow 10,000,000$ 
 $v.X \leftarrow \mathbf{0}_B$                                  $\triangleright \mathbf{0}_B$  is the length- $B$  vector of zeros
 $Y \leftarrow \mathbf{0}_B$                                  $\triangleright Y$  holds the total number of non-failures across children of  $v$ 
for  $b = 1, 2, \dots, B$  do
  for  $u \in ch(v)$  do
     $Y[b] \leftarrow Y[b] + u.X[b]$ 
  end for
  if  $Y[b] > 0$  then                                 $\triangleright \#ch(v)$  is the number of children of  $v$ 
     $v.X[b] \leftarrow 1$                              $\triangleright$  If at least one child of  $v$  is a non-failure, then  $v$  is a non-failure
  end if
end for

```

4.4. Example using risk element 3

Figure 4 shows the probabilistic success tree for risk element 3 (landing), which is one of three separate trees representing the outcomes of the experiments discussed in Section 4.1. In the figure, vertices are identified by their Entry IDs of the form BPP-RE3-***, where *** is a three-digit integer. Leaf vertices are shown as green hexagons, and interior vertices are blue. Circles indicate AND gates and rectangles indicate OR gates. Leafs are at the top, and the root vertex is at the bottom. Arrows indicate directional flow of information from child vertices to their parents. No child has more than one parent, but nothing about our method or computation precludes that.

Probabilities of CNA (P_{CNA}) for 33 of 102 leafs were missing in our input data for risk element 3, due to lack of experimental data or computational model results. For these leafs, P_{CNA} was arbitrarily set to 0.00001, which is an order of magnitude larger than the requirement. This choice was very conservative and likely a worst-case. After this adjustment, the leaf mean probability of non-failure was 0.9994604, the minimum was 0.9770103, and the maximum was 1.0. Here, the minimum and maximum of the leaf probabilities (over all leafs) were computed by making a histogram of the leaf probabilities and picking off the largest and smallest. After propagation to the root vertex, we found that BPP-RE3-001 had a $p = 1.0$ of non-failure in 10,000,000 trials and under the presumed conditions. There is at least one reason why this may not be realistic. In this example, all the leafs were purposefully constructed to be independent of one another. In other settings where there is dependence, particularly positive correlations between

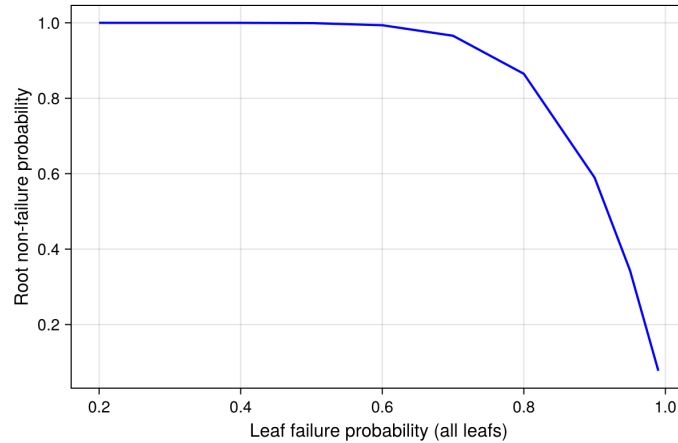


Figure 5. Plot of BPP-RE3-001 non-failure probability as a function of leaf failure probability (same for all leaves).

to have different failure probabilities. This will be the subject of future analysis. For now, these results give some support to the idea that the tree’s topology itself confers a degree of robustness on BPP-RE3-001’s outcome.

5. Conclusions

This work presented a methodology to support performance verification against quantitative targets corresponding to a 0.999999 probability of maintaining containment of the sealed Martian sample tubes that might be brought to Earth as part of the Mars Sample Return program. This approach to backward planetary protection risk assessment was innovative in the combination of qualitative failure assessments (e.g., FMECA) and quantitative probability models that were integrated in a FTA/FLD-based logic framework. This approach works especially well where probabilistic uncertainty is high, or unknown, for some contributors in a complex risk model. While quantitative assessments are still an important contributor to assessing risk and should be relied upon, this approach provides a viable alternative to potentially alleviate consuming valuable project resources trying to develop high-uncertainty probability models, which could potentially drive the overall risk assessment.

In addition, we demonstrated a new approach to tree analysis that allows for more detailed control of fault tree-like simulations than is usually possible with standard software. This enables us to interrogate the relationships between different parts of the tree using non-parametric statistical models based on simulations. We use the Julia programming language, which provides both speed and efficiency so that engineers can assess impacts of different assumptions in real time. Although not demonstrated here, our method applies equally well when the basic, leaf-level outcomes exhibit dependence rather than independence and when the tree is such that a requirement failure affects more than one requirement failure probability below it (i.e., in the direction of the root).

Overall, the methodology presented here improves the state of the art and provides a useful tool for assembling an assurance case that demonstrates sufficient performance while remaining conceptually accessible to a diverse set of stakeholders. In so doing, it contributes to defining an appropriate risk posture to inform decisions regarding the containment of the potentially returned sealed Martian sample tubes. Nonetheless, the reader is reminded that proving such high reliability values remains a daunting task, given the impossibility to collect experimental data to generate statistics to or below a one-in-a-million level.

Notes and acknowledgments

This document is being made available for information purposes only. The decision to implement Mars Sample Return would not be finalized until NASA’s completion of the National Environmental Policy Act (NEPA) process. In addition, this work is based on a previous baseline MSR architecture from December 2023, in which ERO-CCRS would return the OS to Earth within approximately five years of landing on Mars to retrieve samples collected by

the Perseverance rover. The CCRS project completed system development to a Preliminary Design Review level of maturity in mid-December 2023, after which it was stopped indefinitely pending the results of the re-architecture effort.

Funding provided by the National Aeronautics and Space Administration and the European Space Agency is gratefully acknowledged. Portions of the research were carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration (80NM0018D0004).

The authors would like to acknowledge Brian Clement, Aaron Siddens and Kevin Carpenter at the Jet Propulsion Laboratory for insightful technical discussions and several reviewers for their feedback.

References

- [1] W. F. Larsen, Fault tree analysis, Tech. Rep. 4556, Picatinny Arsenal, Dover, New Jersey, technical report prepared for US Army (1974). URL <https://apps.dtic.mil/sti/pdfs/AD0774843.pdf>
- [2] P. McNelles, Z. C. Zeng, G. L. Guna Renganathan, Y. Akl, L. Lu, A comparison of fault trees and the dynamic flowgraph methodology for the analysis of FPGA-based safety systems part 1: Reactor trip logic loop reliability analysis, *Reliability Engineering & System Safety* 153 (2016) 135–150. doi:10.1016/j.res.2016.04.014.
- [3] K. Durga Rao, V. Gopika, V. S. Rao, H. Kushwaha, A. Verma, A. Srividya, Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment, *Reliability Engineering & System Safety* 94 (4) (2009) 872–883. doi:10.1016/j.res.2008.09.007.
- [4] A. Volkanovski, M. Čepin, B. Mavko, Application of the fault tree analysis for assessment of power system reliability, *Reliability Engineering & System Safety* 94 (6) (2009) 1116–1127. doi:10.1016/j.res.2009.01.004.
- [5] M. L. Visinsky, J. R. Cavallero, I. D. Walker, Robotic fault detection and fault tolerance: A survey, *Reliability Engineering & System Safety* 46 (2) (1994) 139–158. doi:10.1016/0951-8320(94)90132-5.
- [6] Y. Sato, K. Inoue, H. Kumamoto, The safety assessment of human-robot systems: 3rd report, on the quantification of consecutive failure logic, *Bulletin of JSME* 29 (257) (1986) 3945–3951. doi:10.1299/jsme1958.29.3945.
- [7] E. Ruijters, M. Stoelinga, Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools, *Computer Science Review* 15 (2015) 29–62. doi:10.1016/j.cosrev.2015.03.001.
- [8] G. Merle, J.-M. Roussel, J.-J. Lesage, Algebraic determination of the structure function of dynamic fault trees, *Reliability Engineering & System Safety* 96 (2) (2011) 267–277. doi:10.1016/j.res.2010.10.001.
- [9] J. Ni, W. Tang, Y. Xing, A simple algebra for fault tree analysis of static and dynamic systems, *IEEE Transactions on Reliability* 62 (4) (2013) 846–861. doi:10.1109/TR.2013.2285035.
- [10] S. Montani, L. Portinale, A. Bobbio, Dynamic Bayesian networks for modeling advanced fault tree features in dependability analysis, in: *Proceedings of the European Safety and Reliability Conference (ESREL)*, 2005, pp. 1415–1422.
- [11] H. Boudali, J. Dugan, A new Bayesian network approach to solve dynamic fault trees, in: *Annual Reliability and Maintainability Symposium*, 2005. Proceedings, 2005, pp. 451–456. doi:10.1109/RAMS.2005.1408404.
- [12] T. Graves, M. Hamada, R. Klamann, A. Koehler, H. Martz, A fully Bayesian approach for combining multi-level information in multi-state fault tree quantification, *Reliability Engineering & System Safety* 92 (10) (2007) 1476–1483. doi:10.1016/j.res.2006.11.001.
- [13] D. Raiteri, G. Franceschinis, M. Iacono, V. Vittorini, Repairable fault tree for the automatic evaluation of repair policies, in: *International Conference on Dependable Systems and Networks*, 2004, 2004, pp. 659–668. doi:10.1109/DSN.2004.1311936.
- [14] X. Zhang, Q. Miao, X. Fan, D. Wang, Dynamic fault tree analysis based on Petri nets, in: *Proceedings of 2009 8th International Conference on Reliability, Maintainability and Safety*, 2009, pp. 138–142. doi:10.1109/ICRMS.2009.5270223.
- [15] J. Dugan, S. Bavuso, M. Boyd, Fault trees and sequence dependencies, in: *Annual Proceedings on Reliability and Maintainability Symposium*, 1990, pp. 286–293. doi:10.1109/ARMS.1990.67971.
- [16] H. Boudali, P. Crouzen, M. Stoelinga, A compositional semantics for dynamic fault trees in terms of interactive Markov chains, in: K. S. Namjoshi, T. Yoneda, T. Higashino, Y. Okamura (Eds.), *Automated Technology for Verification and Analysis*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 441–456. doi:10.1007/978-3-540-75596-8_31.
- [17] W. Han, W. Guo, Z. Hou, Research on the method of dynamic fault tree analysis, in: *The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety*, 2011, pp. 950–953. doi:10.1109/ICRMS.2011.5979422.
- [18] H. Boudali, A. Nijmeijer, M. Stoelinga, DFTSim: A simulation tool for extended dynamic fault trees, in: *Proceedings of the 42nd Annual Simulation Symposium (ANSS)*, San Diego, California, USA, 2009, p. 31.
- [19] X. Liang, H. Yi, Y. Zhang, D. Li, A numerical simulation approach for reliability analysis of fault-tolerant repairable system, in: *Proceedings of 2009 8th International Conference on Reliability, Maintainability and Safety*, 2009, pp. 191–196. doi:10.1109/ICRMS.2009.5270210.
- [20] H. Aliee, H. R. Zarandi, Fault tree analysis using stochastic logic: A reliable and high speed computing, in: *2011 Proceedings - Annual Reliability and Maintainability Symposium*, 2011, pp. 1–6. doi:10.1109/RAMS.2011.5754466.
- [21] C. Liu, C. Zhou, L. Tan, J. Cui, W. Xiao, Reliability analysis of subsea manifold system using fuzzy fault tree analysis, *Scientific Reports* 14 (2024) 22873. doi:10.1038/s41598-024-73410-y.
- [22] S. Hu, Q. Liang, S. Wang, H. Huang, B. Li, J. Tian, Q. Hu, Anomaly analysis and fault diagnosis of underwater glider based on deep learning method, in: *OCEANS 2024-Halifax*, IEEE, 2024, pp. 1–6.
- [23] ISO/IEC/IEEE, Systems and software engineering – Systems and software assurance – Part 2: Assurance case, International Standard ISO/IEC/IEEE 15026-2:2022, International Organization for Standardization, Geneva, Switzerland (2022).
- [24] NASA Office of Safety and Mission Assurance, Implementing planetary protection requirements for space flight, NASA Technical Standard 8719.27 (2022).
- [25] NASA Office of Safety and Mission Assurance, Planetary Protection Provisions for Robotic Extraterrestrial Missions, NASA Procedural Requirements (NPR) 8715.24 (2021).

- [26] B. V. Sarli, E. Bowman, G. Cataldo, T. B. Feehan, T. Green, K. Gough, A. Hagedorn, P. Hudgins, J. Lin, M. Neuman, E. Parvez, J. Rondey, C. E. Szalai, C. Yew, NASA's Capture, Containment, and Return System: Bringing Mars Samples to Earth, *Acta Astronautica* 223 (2024) 370–303. doi:10.1016/j.actaastro.2024.05.048.
- [27] D. Beaty, M. Grady, H. McSween, E. Sefton-Nash, B. Carrier, F. Altieri, Y. Amelin, E. Ammannito, M. Anand, L. Benning, J. Bishop, L. Borg, D. Boucher, J. Brucato, H. Busemann, K. Campbell, A. Czaja, V. Debaille, D. des Marais, M. Dixon, B. Ehlmann, J. Farmer, D. Fernandez-Remolar, J. Filiberto, J. Fogarty, D. Glavin, Y. Goreva, L. Hallis, A. Harrington, E. Hausrath, C. Herd, B. Horgan, H. Humanyun, T. Kleine, J. Kleinhenz, R. MacKelpang, N. Mangold, L. Mayhew, J. McCoy, F. McCubbin, S. McClennan, D. Moser, F. Moynier, J. Mustard, P. Niles, G. Ori, F. Raulin, P. Rettberg, M. Rucker, N. Schmitz, S. Schwenzer, M. Sephton, R. Shaheen, Z. Sharp, D. Schuster, S. Siljestrom, C. Smith, J. Spry, A. Steele, T. Swindle, I. ten Kate, N. Tosca, T. Usui, M. van Kranendonk, M. Wadhwa, B. Weiss, S. Werner, F. Westall, R. Wheeler, J. Zipfel, M. Zorzano, The Potential Science and Engineering Value of Samples Delivered to Earth by Mars Sample Return, *Meteoritics and Planetary Science* 54 (3) (2019) 667–671. doi:10.1111/maps.13242.
- [28] T. Haltigin, E. Hauber, G. Kminek, M. Meyer, C. Agee, H. Busemann, B. Carrier, D. Glavin, L. Hays, B. Marty, L. Pratt, A. Udry, M.-P. Zorzano, D. Beaty, B. Cavalazzi, C. Cockell, V. Debaille, M. Grady, A. Hutzler, F. McCubbin, A. Regberg, A. Smith, C. Smith, R. Summons, T. Swindle, K. Tait, N. Tosca, T. Usui, M. Velbel, M. Wadhwa, F. Westall, Rationale and Proposed Design for a Mars Sample Return (MSR) Science Program, *Astrobiology* 22 (S1) (2022) S–27–S–56, PMID: 34904885. doi:10.1089/ast.2021.0122.
- [29] M. Grady, R. E. Summons, T. Swindle, F. Westall, G. Kminek, M. Meyer, D. Beaty, B. Carrier, T. Haltigin, L. Hays, C. Agee, H. Busemann, B. Cavalazzi, C. Cockell, V. Debaille, D. Glavin, E. Hauber, A. Hutzler, B. Marty, F. McCubbin, L. Pratt, A. Regberg, A. Smith, C. Smith, K. Tait, N. Tosca, A. Udry, T. Usui, M. Velbel, M. Wadhwa, M.-P. Zorzano, The Scientific Importance of Returning Airfall Dust as a Part of Mars Sample Return (MSR), *Astrobiology* 22 (S1) (2022) S–176–S–185, PMID: 34904884. doi:10.1089/ast.2021.0111.
- [30] T. Swindle, S. Atreya, H. Busemann, J. Cartwright, P. Mahaffy, B. Marty, A. Pack, S. Schwenzer, Scientific Value of Including an Atmospheric Sample as Part of Mars Sample Return (MSR), *Astrobiology* 22 (S1) (2022) S–165–S–175, PMID: 34904893. doi:10.1089/ast.2021.0107.
- [31] B. Carrier, D. Beaty, A. Hutzler, A. Smith, G. Kminek, M. Meyer, T. Haltigin, L. Hays, C. Agee, H. Busemann, B. Cavalazzi, C. Cockell, V. Debaille, D. Glavin, M. Grady, E. Hauber, B. Marty, F. McCubbin, L. Pratt, A. B. Regberg, C. Smith, R. Summons, T. Swindle, K. Tait, N. Tosca, A. Udry, T. Usui, M. Velbel, M. Wadhwa, F. Westall, M.-P. Zorzano, Science and Curation Considerations for the Design of a Mars Sample Return (MSR) Sample Receiving Facility (SRF), *Astrobiology* 22 (S1) (2022) S–217–S–237, PMID: 34904886. doi:10.1089/ast.2021.0110.
- [32] B. K. Muirhead, A. Karp, Mars sample return lander mission concepts, in: 2019 IEEE Aerospace Conference, IEEE, 2019, pp. 1–9.
- [33] G. T. Story, A. C. Karp, B. Nakazono, G. Zilliac, B. J. Evans, G. Whittinghill, Mars Ascent Vehicle Hybrid Propulsion Effort, in: AIAA Propulsion and Energy 2020 Forum, 2020, p. 3727. doi:10.2514/6.2020-3727.
- [34] G. Cataldo, L. Affentranger, B. G. Clement, D. P. Glavin, D. W. Hughes, J. Hall, B. V. Sarli, C. E. Szalai, The Planetary Protection Strategy of Mars Sample Return's Earth Return Orbiter Mission, *Journal of Space Safety Engineering* 11 (2) (2024) 374–384. doi:10.1016/j.jsse.2024.04.013.
- [35] K. Geelen, O. Sutherland, P. Baglioni, F. Spoto, J. Huesing, A. Haldemann, F. Beyer, P. Schoonejans, A. Accomazzo, T. Loureiro, L. Affentranger, D. Nicolis, C. Steiger, E. Yau, Mars Sample Return Campaign - Status of the ESA provided Elements, in: Proceedings of the International Astronautical Federation, 72nd International Astronautical Congress, Dubai, United Arab Emirates, 2021, pp. 1–12.
- [36] NASA Office of Safety and Mission Assurance, NASA Policy for Safety and Mission Success, NASA Policy Directive (NPD) 8700.1 (2022).
- [37] NASA Office of Safety and Mission Assurance, NASA RELIABILITY AND MAINTAINABILITY (R&M) STANDARD FOR SPACE-FLIGHT AND SUPPORT SYSTEMS, NASA Procedural Requirements (NPR) 8729.01 (2017).
- [38] E. Paté-Cornell, R. Dillon, Probabilistic risk analysis for the NASA space shuttle: a brief history and current work, *Reliability Engineering & System Safety* 74 (3) (2001) 345–352. doi:10.1016/S0951-8320(01)00081-3.
- [39] F. Hsu, The Space Shuttle probabilistic risk assessment framework A structured multiphase multi-layer modeling approach for large and complex engineered systems, in: 2008 7th IEEE International Conference on Cybernetic Intelligent Systems, IEEE, 2008, pp. 1–9.
- [40] T. L. Hamlin, M. A. Canga, R. L. Boyer, E. B. Thigpen, 2009 Space Shuttle Probabilistic Risk Assessment Overview, in: 10th International Probabilistic Safety Assessment and Management Conference, 2010, pp. 1–21.
- [41] T. Hamlin, J. Kahn, E. Thigpen, Y. Lo, Shuttle risk progression: Use of the shuttle probabilistic risk assessment (PRA) to show reliability growth, in: AIAA SPACE 2011 Conference & Exposition, 2011, p. 7353.
- [42] E. Yılmaz, B. J. German, A. R. Pritchett, Optimizing resource allocations to improve system reliability via the propagation of statistical moments through fault trees, *Reliability Engineering & System Safety* 230 (2023) 108873. doi:10.1016/j.ress.2022.108873.
- [43] G. Cataldo, B. V. Sarli, P. Gage, T. White, T. B. Feehan, F. Pellerano, Planetary protection trades and lessons learned from designing Mars Sample Return's Capture, Containment, and Return System, *Acta Astronautica* 232 (2025) 174–180. doi:10.1016/j.actaastro.2025.01.046.
- [44] B. V. Sarli, M. D. Squire, W. P. Schonberg, G. Cataldo, J. Williamsen, B. Tulaba, V. Cabrera, C. Cline, S. Dellinger, K. Hoffman, J. Hyde, A. Jenkin, Q. McKown, J. Needels, G. Peterson, R. Stein, K. Steward, J. Warner, T. White, Micrometeoroid and orbital debris risk assessment and mitigation for Mars Sample Return, *AIAA Journal*, Submitted (2026).
- [45] P. Gage, G. Cataldo, Probabilistic Allocations for Structural Integrity for Mars Sample Return's Earth Entry System, *AIAA Journal of Spacecraft and Rockets*, Submitted (2026).
- [46] A. C. Schuerger, Synergistic Interactions among Vacuum, Solar Heating, and UV Irradiation Enhance the Lethality of Interplanetary Space, *Microorganisms* 12 (10) (2024). doi:10.3390/microorganisms12101976.
- [47] Department of Defense, United States of America, MILITARY HANDBOOK 217 - RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT (1991).
- [48] Quanterion Solutions Incorporated, Handbook of 217Plus:2015, Notice 1 - Reliability Predictions Models (2015).
- [49] Naval Surface Warfare Center, Carderock Division, Handbook of Reliability Prediction Procedures for Mechanical Equipment (2011).
- [50] Quanterion Solutions Incorporated, Nonelectronic Parts Reliability Data (NPRD) (2023).
- [51] Quanterion Solutions Incorporated, Electronic Parts Reliability Data (EPRD) 2014 - Volume 1 (2014).
- [52] Windchill Risk and Reliability - Practitioner's Guide (2021).
- [53] Getting Started Guide - Windchill Quality Solutions 10.0 (2011).

- [54] J. C. Vander Kam, P. Gage, Estimating Orion Heat Shield Failure due to Ablator Cracking, *Journal of Spacecraft and Rockets* 58 (5) (2021) 1263–1270. doi:10.2514/1.A35003.
- [55] S. Marelli, R. Schöbi, B. Sudret, UQLab user manual – Structural reliability (Rare event estimation), Tech. rep., Chair of Risk, Safety and Uncertainty Quantification, ETH Zurich, Switzerland, report UQLab-V2.1-107 (2024).
- [56] B. Peherstorfer, B. Kramer, K. Willcox, Multifidelity preconditioning of the cross-entropy method for rare event simulation and failure probability estimation, *SIAM/ASA Journal on Uncertainty Quantification* 6 (2) (2018) 737–761. doi:10.1137/17M1122992.
- [57] A. V. Moorhead, NASA Meteoroid Engineering Model (MEM) Version 3, Tech. rep., NASA (2020).
- [58] A. B. Vavrin, A. P. Manis, J. Seago, D. Gates, P. Anz-Meador, Y.-L. Xu, R. Barahona, A. Malachi, I. Bigger, M. J. Matney, J. C. Liou, NASA Orbital Debris Engineering Model ORDEM 3.1-Software User Guide, Tech. rep., NASA (2019).
- [59] W. P. Schonberg, M. D. Squire, Development of ballistic limit equations in support of the Mars sample return mission, *Journal of Space Safety Engineering* 11 (3) (2024) 417–424. doi:10.1016/j.jsse.2024.06.003.
- [60] W. P. Schonberg, M. D. Squire, Iterating on a design – further developments in the evolution of the ballistic limit equations for the Mars Sample Return Project, *Journal of Space Safety Engineering* 12 (1) (2025) 119–131. doi:10.1016/j.jsse.2024.12.004.
- [61] A. Siddens, S. Perino, A. Sprunt, Earth Landing Loads for the Mars Sample Return Earth Entry System, in: 2022 Spacecraft Launch Vehicle Dynamic Environments Workshop, June 28-30, 2022.
- [62] A. Siddens, J. Pempejian, D. Coleman, M. Vena, M. Yu, A. Costain, Impact Testing for Model Validation and Hardware Verification for Mars Sample Return Landing Phase, in: 20th International Planetary Probe Workshop, Marseille, France, Aug 28-Sept 1, 2023.
- [63] Livermore Software Technology, An Ansys Company, LS-DYNA Keyword User's Manual, Version R13, http://ftp.lstc.com/anonymous/outgoing/jday/manuals/LS-DYNA_Manual_Volume_I_R13.pdf, Accessed July 3, 2025 (2021).
- [64] J. Bezanson, A. Edelman, S. Karpinski, V. B. Shah, Julia: A fresh approach to numerical computing, *SIAM Review* 59 (1) (2017) 65–98. doi:10.1137/141000671.
- [65] J. Fairbanks, M. Besançon, S. Simon, J. Hoffman, N. Eubank, S. Karpinski, Juliagraphs/graphs.jl: an optimized graphs package for the julia programming language, <https://github.com/JuliaGraphs/Graphs.jl/> (2021).
- [66] S. Bromberger, Metagraphs.jl, <https://juliagraphs.org/MetaGraphs.jl/stable/license/> (2017).
- [67] Wikipedia, https://en.wikipedia.org/wiki/Topological_sorting (2024).