An Approach to Fault Management Design for the Proposed Mars Sample Return EDL and Ascent Phase Architectures

by

Cici Mao

B.S. in Aerospace Engineering
Massachusetts Institute of Technology (2022)

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the degree of

Master of Science in Aeronautics and Astronautics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2024

Authored by:	Cici Mao Department of Aeronautics and Astronautics May 17, 2024
Certified by:	Kerri Cahoy Professor of Aeronautics and Astronautics Thesis Supervisor
Accepted by:	Jonathan P. How R. C. Maclaurin Professor of Aeronautics and Astronautics Chair, Graduate Program Committee

An Approach to Fault Management Design for the Proposed Mars Sample Return EDL and Ascent Phase Architectures

by

Cici Mao

Submitted to the Department of Aeronautics and Astronautics
on May 17, 2024, in partial fulfillment of the
requirements for the degree of
Master of Science in Aeronautics and Astronautics

Abstract

The Mars Sample Return (MSR) campaign aims to bring Martian regolith samples back to Earth. JPL is currently developing the Sample Retrieval Lander (SRL) to receive the samples collected by the Perseverance rover and launch them into Mars orbit using a Mars Ascent Vehicle (MAV) for future Earth return. The telecommunications delay from Earth to Mars requires autonomy on-board the spacecraft for different phases of the mission like Entry, Descent & Landing (EDL) and MAV Launch given limited possible operator intervention. Fault protection (FP) encapsulates these autonomous system behaviors, which aim to protect the spacecraft by limiting or detecting and responding to anomalies. In order to provide sufficient coverage to the possible faults a system may encounter, multiple FP analyses are needed to identify and analyze the fault set of a system to guide future design iterations. This thesis focuses on three tools: Fault Containment Region (FCR), Failure Mode Effects & Criticality Assessment (FMECA), and Fault Tree Analysis (FTA). FCRs are used to identify the boundaries at which faults can occur and propagate in a system, making them useful tools for defining functional boundaries in a system and identifying areas that are single-string, or have no redundancy. FMECAs and FTAs use a bottoms-up and top-down approach, respectively, to identify possible faults and the associated consequences and impacts of each anomaly; together, these tools provide a comprehensive fault set to be used in FP architecture design. Using these tools demonstrates how FP design factors into engineering trades – monitoring or additional redundancy adds additional cost and complexity – and thus the results of these analyses need to be used iteratively with the system design to determine the best approach. As such, it's shown that a majority of EDL and MAV Launch elements are single-string, and while there are opportunities of adding redundancy in EDL sensors, there are few options for MAV Launch given its engineering constraints. While both phases have little redundancy, the option space for EDL is better known given JPL's multiple successful past landings. Future work should conceptualize possible areas of added redundancy to the MAV to lower overall mission risk.

Thesis Supervisor: Kerri Cahoy
Title: Professor of Aeronautics and Astronautics

Acknowledgments

I would like to thank my advisor, Dr. Kerri Cahoy, for her continued support of both my thesis topic and my Master's degree path. Her guidance and her kindness have been integral to my journey over the past year, and I cannot thank her enough for the opportunities she has given me.

I would also like to thank my partner, Brandon John, who has always been my greatest cheerleader and supporter, and never stopped believing in me. I am where I am today in large part because of his encouragement of what I could achieve.

Special thanks also to my Course 16 friends who cheered me on at each new milestone. And lastly, special thanks to my cat planets — Saturn and Pluto — who provided much needed emotional support and keyboard mashing during the writing process.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Once launched from Earth's surface, spacecraft continue on their journey to their intended destinations in space, either remaining in Earth orbit or proceeding into deep space. Once off the Earth's surface, the only method we have of contacting the spacecraft is telecommunication through ground stations, which have limited communication windows. An additional challenge is added when spacecraft are far from Earth, further increasing the latency of transmitted commands and received data

During nominal operations, the mission operations team maintains contact with a spacecraft, provides it with instructions via uplinked commands, and monitors its status with received downlink data. However, if a fault occurs, the operations team is often unable to respond to these events in a timely manner, which motivates the need for an on-board fault protection (FP) system on the spacecraft to be able to monitor, detect, and respond to off-nominal events when immediate ground intervention is not possible.

However, the capability of being able to respond to faults requires understanding of what "nominal" means. For missions such as NASA's upcoming Mars Sample Return (MSR) campaign, the launch of a Mars Ascent Vehicle (MAV) off the Martian surface is a novel concept with little heritage in achieving liftoff from the surface of Mars - there is no prior environmental and launch data. While NASA has experience lifting off a space vehicle from the moon, the MAV will be lifting off from Mars, which requires greater energy and control due to a larger planetary mass and atmosphere.

Another unique challenge to fault protection arises during rapid event sequences where recovery time is minimal to nonexistent. A close analog to MAV Launch is Entry, Descent, and Landing (EDL), which describes the sequence of events of a spacecraft entering a planet's atmosphere and successfully touching down on its surface – for Mars, this is known as the "7 minutes of terror". EDL and MAV Launch are examples of rapid event sequences, and require careful pre-planning of fault responses to limit any potentially catastrophic interruptions to their timelines.

In this thesis, we will analyze the EDL and MAV Launch phases of a representative analog of the proposed MSR architecture [15, 33] and produce a Fault Containment Region (FCR) diagram based on the current design to understand how faults can propagate throughout the system. We will also identify potential failure modes using the Fault Tree Analysis (FTA) and Failure Mode Effects & Criticality Assessment (FMECA) tools, and additionally triage the criticality of the failures within the FMECA. The results of these analyses will be used to explore the factors impacting fault protection approaches for the MAV Launch and EDL mission phases, comparing their similarities and differences.

1.1 Motivation

Space exploration has been pushing the boundaries of science and technology as we continue to build systems with increasing complexity to explore and learn about the worlds outside our own. MSR seeks to fulfill the long sought after goal of returning a selection of samples from Mars to Earth. A major milestone has recently been achieved with the successful landing and sample collection by the NASA Perseverance rover. The sample return campaign has significant scientific value in providing geological records of Mars to better understand the planet's history and climate, and was deemed the top priority in the 2023 Planetary Science Decadal Survey [8].

The next major milestone in the MSR campaign is getting the Sample Retrieval Lander (SRL) to Mars. The SRL houses the MAV on the Martian surface until it's ready to be launched. As with many other spacecraft, the SRL will require fault protection to keep it safe throughout its various mission phases, often requiring unique configurations for each phase. While SRL progresses through phases of Cruise, EDL, Surface Operations, and MAV Launch, this thesis will focus on two phases: EDL and MAV Launch. While the two may seem to be polar opposites — landing a spacecraft vs. launching an ascent vehicle — both are rapid-fire sequences where many critical events have to succeed. As such, there are many parallels that can be drawn from the FP approach for EDL to MAV Launch. However, the MAV is both a novel system and one that operates in the highly unpredictable and largely uncharacterized Martian launch environment while EDL is better understood, with significant past heritage and success [18, 27, 39, 41, 45] . Analyzing these phases from a fault protection perspective will provide insight into how assumed risk and engineering requirements influence FP design.

1.2 Mars Sample Return

MSR architecture has evolved significantly in the last two decades as a result of both technological advancements and also due to cost and feasibility concerns with the designs. The core of the various architectures is a mission concept that involves a method of collecting and caching Martian regolith samples and launching them off the Martian surface, carrying them to Earth-based labs for analysis. While initial proposals led by the Jet Propulsion Laboratory (JPL) began in 2001 [46], it was not until 2018 that NASA – in collaboration with ESA – committed to MSR. In the years following, MSR's architecture has continued to be reworked, with notable changes such as consolidating from two landers to one, and the replacement of a "fetch" rover with helicopters [37, 42]. Figure 1-1 depicts an overview of the current MSR architecture released in Fall 2022, including the major spacecraft elements and concept of operations (conops) [16].

The portion of MSR relevant to this thesis is the Sample Retrieval Lander (SRL), which will be launched in 2028 and arrive on Mars in 2030 [38]. The primary goal of SRL is to successfully obtain cached samples from Perseverance — either from the

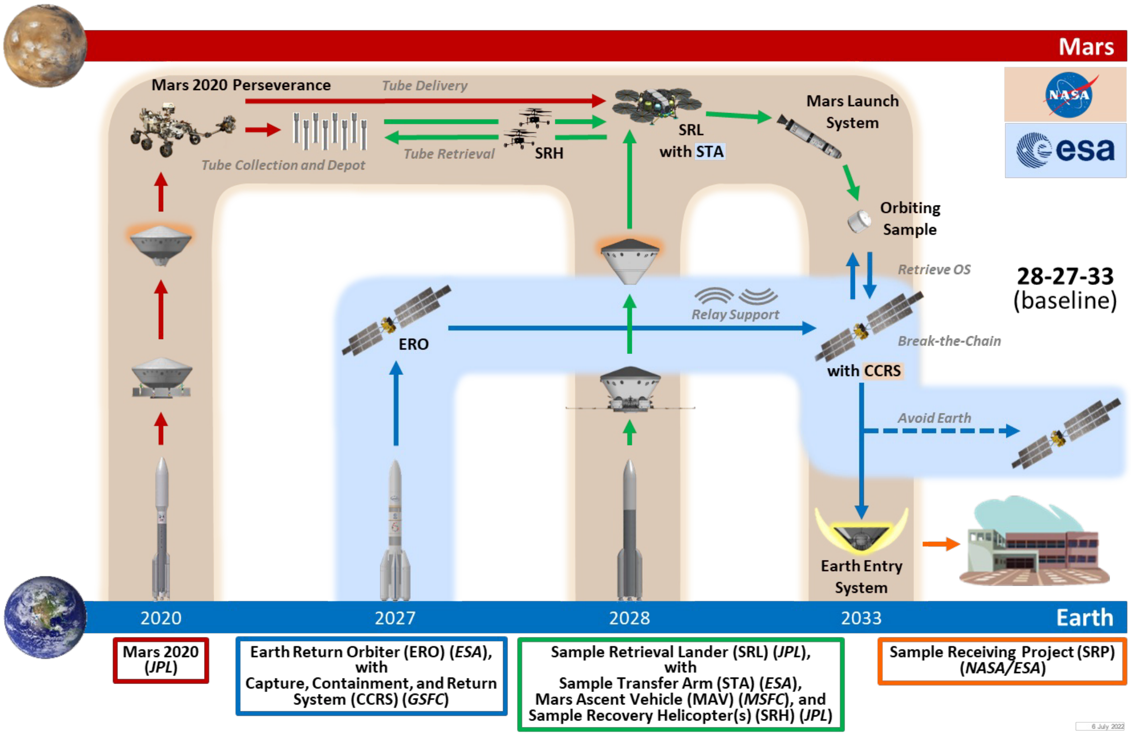

Mars
Mars 2020 Perseverance
Tube Delivery
Tube Collection and Depot
Tube Retrieval
SRH
SRL
with STA
Mars Launch
System
Orbiting
Sample
Retrieve OS
28-27-33
(baseline)
Relay Support
ERO
Break-the-Chain
with CCRS
Avoid Earth
Earth Entry
System
2020
2027
2028
2033
Earth
Mars 2020 (JPL)
Earth Return Orbiter (ERO) (ESA), with Capture, Containment, and Return System (CCRS) (GSFC)
Sample Retrieval Lander (SRL) (JPL), with Sample Transfer Arm (STA) (ESA), Mars Ascent Vehicle (MAV) (MSFC), and Sample Recovery Helicopter(s) (SRH) (JPL)
Sample Receiving Project (SRP) (NASA/ESA)
6 July 2022

Figure 1-1: Overview of the 2022 MSR mission architecture including separate designations between the mission components handled by ESA versus NASA and a brief high-level conops [16].

rover directly, or by using the Sample Recovery Helicopters (SRH) — to load them into the MAV, to keep the MAV safe during Mars surface operations, and to eject the MAV at the beginning of its launch sequence. SRL contains both SRHs, the MAV, and the Sample Transfer Arm (STA), a robotic arm used to pick up and place samples from Perseverance into the Orbiting Sample (OS) payload located within the MAV. After MAV is launched, it will continue into a Mars orbit where it will release the OS to be ready for pick-up by the Earth Return Orbiter (ERO) for Earth return.

Landing and operating a spacecraft on Mars is no longer an unprecedented goal — it has now been achieved 8 times by NASA. The technology used in EDL continues to be developed and improved from mission to mission, increasing landing safety, accuracy, and precision. EDL on SRL doesn't come without new challenges, however, such as targeting a landing zone more precisely than ever attempted before, but there is a lot of heritage and data about the EDL environment that can be drawn from. On the other hand, the MAV is a new development entirely. Though there is plenty of data on Earth-based launch vehicles, MAV will be the first rocket to be launched from the surface of another planet and must tackle challenges posed by the Martian environment. While humans have launched rockets to Earth from the Moon, Mars poses several significant challenges such as dealing with its significantly stronger gravity, further distance, and presence of an atmosphere, making the prior lunar experience irrelevant on Mars. In addition, there are significant mass constraints on the MAV design due to compounding fuel requirements for Earth launch, EDL, and MAV launch, making it one of the highest development-required aspects of MSR.

1.3 Fault Protection

After spacecraft are launched beyond Earth's orbit, they can only be interacted with via wireless communication systems. Any knowledge of the spacecraft and its subsystems are flowed down to Earth via telemetry and data products that provide windows into what's happening onboard. While this data is useful for the Ground Operations team to understand the spacecraft's status, it is largely up to the spacecraft to continue to maintain its health and functionality during its lifetime. In order to do so, the spacecraft is equipped with fault protection to address issues, or faults, that occur.

Faults can arise on spacecraft from the space environment alone, including thermal conditions or ionizing radiation. In some cases, like in the case of the July 2023 loss of contact with Voyager-2, operations mistakes can also place spacecraft in an unsafe state [4]. Getting spacecraft back into a safe state can either be completed via ground intervention, autonomous onboard behaviors, or both, depending on the problem(s). Due to limited communication windows and long traverse times for deep space missions [32], it's impractical for the operations team to be constantly monitoring all of the spacecraft telemetry and respond to faults manually. Similarly, time critical failures such as battery depletions, electrical shorts, or overvoltage events need an immediate response from spacecraft systems to prevent damage. The need for immediate responses also extends to other time critical events like those during EDL or MAV launch, where the spacecraft must be able to successfully perform multiple actions in quick succession without interruption. Onboard autonomous processes are necessary to monitor the spacecraft, identify faults, and respond accordingly.

1.3.1 Elements of Fault Protection

Fault protection consists of fault avoidance and fault tolerance in spacecraft design, which collectively aim to mitigate the risk and impact of faults occurring in the system [6]. Fault avoidance consists of methods to mitigate fault occurrence, either in hardware design or operational processes. This can include using robust designs that minimize complexity and failure points, operating the spacecraft in ways that minimize environmental risks, and using radiation-hardened components to minimize the effects of ionizing radiation on electronics. However, even when using best practices, it's impossible to prevent all possible fault cases, which motivates the need to design for fault tolerance.

Fault tolerance consists of methods to mitigate the impacts of faults once they occur. Within design space, this can include adding physical or functional redundancy, such as multiple sensors or heaters, which allows for the loss of a component without losing its associated function. Systems are also designed to limit fault propagation via fault containment regions (FCRs) so that a fault in one area doesn't affect another, or that the loss of one component doesn't take out the rest. However, once in flight, the goal becomes designing the spacecraft system to detect, identify, and respond to faults that arise. In order to detect faults, spacecraft are equipped with monitors that measure and report various data – this can include temperature, voltage, switch state, watchdog timers, etc. These monitors can be physical hardware or within flight software depending on the use case, and will trip a response if what they're measuring goes out of expected bounds. Fault responses can also be conducted in hardware or software, but will carry out the appropriate actions tied to the monitors that initiated them.

In order to properly design the system fault protection for a spacecraft, it's necessary to identify and understand the set of possible faults that can occur, and the potential impacts of the occurrence. That is, it's important to know what faults can happen and what issues they can cause. This area of fault protection is the central focus of this thesis and the analyses we will be exploring, which will be further discussed in Section 2.

1.3.2 Limitations of Fault Protection

Though fault protection is critical for protecting spacecraft from faults, it comes at a cost. For example, adding physical redundancy into the system adds additional hardware, which increases cost, mass, and complexity. Adding hardware monitors may also result in these same impacts. On the software side, adding fault responses increases the complexity of the system, which will require additional time and cost in verifying and validating the design — and like all systems, increasing complexity increases risk of faults, even within fault protection.

The design of a mission often motivates a negotiation between the necessary level of fault protection versus acceptable risk. The type of mission and the space environment that the spacecraft will experience are major factors in how much risk the spacecraft is in, and how much risk the mission can accept. Large flagship missions such as MSR require a greater level of fault protection because the missions are so expensive and tolerate very little risk – they need to succeed. Missions that go to harsh environments or involve communications challenges also require robust fault responses. In contrast, smaller missions with greater acceptable risk and stricter mass/cost constraints likely don't need robust fault protection systems. Earth orbiting missions in particular have faster and more frequent communications windows and in some orbits are less susceptible to ionizing radiation due to being shielded by Earth's magnetic field, which helps reduce their expected occurrence of faults.

Another major challenge with designing fault protection is knowing how the system will be operating. In order to properly monitor the spacecraft, we must know what the spacecraft "looks" like when everything is nominal, or operating correctly. It wouldn't be possible to flag a fault occurrence if we didn't have enough information to decide what it meant to be off-nominal. This isn't a major problem with well known aspects of spacecraft engineering that are often thresholded, such as voltage range operating requirements or thermal limits, but can be difficult for new endeavors. Another important decision process is where to set monitor limits relative to minimum survival limits, how much margin to retain so that there is time to react and resolve — but that is a separate challenge.

As with all other aspects of space systems engineering where the mantra is “test as you fly, and fly as you test”, it is important to test FP as you fly — otherwise, unexpected emergent behaviors can result in failure. The Hakuto-R Mission 1 Lander is an example of how a correctly designed and implemented fault response resulted in mission failure due to an unexpected operating environment [20]. The operating company, ispace, released a report [19] stating that their lander crashed into the lunar surface after running out of propellant when attempting to touch down. When approaching the lunar surface, the lander flew over a crater ridge which resulted in a spike from its altimeter reading. The associated fault protection kicked in, and flight software ignored future readings on the altimeter under the assumption that the measurement jump was due to hardware failure. Unfortunately, this meant the lander assumed its true altitude was what it measured prior flying over the crater, so it hovered at 3 km above the crater floor thinking it was about to touch the surface. It never received mechanical feedback on successful touchdown, so it continued to use propellant until it ran out of fuel and crashed. The primary reason this failure mode occurred was due to ispace changing their intended landing site without revalidating their landing procedures — but the introduction of a crater rim resulted in a data measurement response in the altimeter that triggered the fault protection to mark the hardware as sick. Without accurately knowing the operating environment, ispace accidentally introduced a failure mode that resulted in mission loss because their sensor’s definition of “off-nominal” changed. While the discrepancy was an oversight in ispace’s case, the uncertainty in operation is a major factor in FP design, and in some cases, whether FP should be used at all.

Development of FP for complex systems is a systems engineering task that requires consideration of the potential risks, operational environments, and non-technical drivers of a mission. This thesis will focus on the EDL and MAV Launch phases of MSR, both of which pose unique FP challenges of being time-critical sequences of events, and the latter being completely novel. The fault protection required for each phase is necessarily tailored to them, and we will explore methods of analyzing fault scenarios and discussing comparisons between these phases.

1.4 Challenges for SRL

The MSR-SRL project recently underwent an Independent Review Board (IRB) investigation which concluded that the 2023 design was not feasible within the budget and timeline being proposed. The project is likely going to be re-architected to properly respond to the IRB's concerns, but this thesis will focus on the design of SRL at the time of the IRB.

MSR-SRL poses many unique engineering challenges for EDL and MAV launch. While EDL has a lot of heritage design and mission data to draw from past successful Mars landers and rovers, the MAV will be the first rocket to launch off the surface of another planet.

SRL will be the 10th mission NASA lands on Mars, so while the EDL design will be challenging, it is not without precedent. A number of parameters changed between past missions and SRL such as landing location, spacecraft mass and geometry, etc. These changes require addressing in EDL design, but the dynamics of EDL are well understood and these changes can be modeled. There is some level of certainty that can go into the design, and optimizations can be made without introducing unknown risk to performance.

In contrast to EDL, MAV launch is a completely novel goal of launching a rocket off a different planet. Even engineering rockets that launch off of Earth is a difficult task. Many companies aim to develop reliable launch vehicles, but only a few have successfully produced ones that have been able to be certified. Amongst these successes, companies still often need multiple design iterations and launch attempts before achieving a reliable design. The Earth launch environment is also fairly well known, especially after data collected from the hundreds of launches achieved. In contrast, the MAV aboard SRL must succeed on the first try, and in a launch environment that is largely unknown. Though data exists on the Martian atmosphere from orbiter data and successful landings, the aerodynamics that a rocket would experience in launch can currently only be simulated. This uncertainty plays a significant factor in the MAV design.

Another major challenge in the MAV design is the significance of mass impacts on the system. Not only is the MAV mass-constrained for its own propellent requirements to launch from Mars, every gram on the MAV waterfalls down into even greater mass required on SRL, which has an upper limit set by the launch requirements. Traditionally, robustness in spacecraft involves adding redundant hardware, but for a system like MAV that is significantly mass constrained, we enter a catch-22. The uncertainty around the MAV environment can't all be addressed with redundant systems, or backups. This motivates the need to assess and identify the most critical elements of MAV design and compromise between mitigation or acceptance of the possible risks.

1.4.1 FP Analysis Focus

Despite the differences between the EDL and MAV launch phases of MSR-SRL, there are a lot of conclusions from EDL that can be applied to MAV launch within the realm of fault protection. Both phases begin after a "point of no return", after which their timeline begins, with notable characteristics including time critical events, short total duration, and completely autonomous behaviors. This rapid timeline in particular is challenging for FP fault responses as the reaction time needed to address and recover from a fault may contribute to mission failure instead. Many FP responses involve either resetting spacecraft computers or placing the spacecraft in a safe mode for ground diagnosis – doing so during EDL and MAV launch would not be feasible.

EDL and MAV launch also have the issue of uncertainty that challenges FP fault monitoring – while you can monitor the spacecraft during these phases, if we don't have an understanding of abnormal state, we can't autonomously flag any issues. In order to mitigate faults during phases where monitors and responses have limited efficacy, other forms of fault protection are needed such as redundancy, shielding, and other forms of system robustness. We will be identifying how these methods can be implemented for EDL. And for MAV launch where these methods are increasingly challenging to implement, we will discuss the decisions and implications of the resulting design. In conjunction with our FCRs, FMECAs, and FTAs, which identify failure propagation and modes, we will analyze how SRL approaches FP in EDL versus MAV launch and the impacts of the FP design on the mission. We will also mention additional FP analysis tools such as STAMP analysis [28], which allow for a systems-level approach to identifying emergent faults, and success trees, which is an FTA complement analysis focusing on the path to success rather than failures.

1.5 Organization of Thesis

This thesis is organized into five chapters. Chapter 1 is a general introduction to the topics in this work. Chapter 2 details the background necessary for the remainder of the thesis, including overviews of the hardware for both EDL (Section 2.1.1) and MAV (Section 2.1.2), the operations involved in each (Section 2.2), and how to use the three FP tools included in this thesis (Section 2.3). Chapter 3 implements the three FP techniques for the EDL phase, and Chapter 4 does the same for MAV Launch. Finally, Chapter 5 discusses the results, both within each phase and also how they compare to each other.

Chapter 2

Approach

Fault Protection for MSR is an inherently complex, and as of yet unresolved, topic. This thesis doesn't claim to be a comprehensive analysis, but instead attempts to explain and demonstrate fault protection as a process, using a MSR/SRL as a representative example.

Data in this thesis is drawn exclusively from public sources. While MSR/SRL specifics are used whenever possible, there are many design decisions that are not yet public (or indeed, not yet even made, as NASA requested budget-focused redesign proposals shortly before this thesis was finalized [12, 36]). Some details about MSR-SRL's design (as noted in Section 2.1) and operations (Section 2.2) have been inferred based on prior missions (such as Curiosity from MSL [2, 18, 26, 41, 43, 44, 45] and Perseverance from M2020 [7, 23, 27, 30, 31, 39]).

Due to these limitations and the changing MSR baseline design, the particular FP results of this thesis should not be relied on. The important takeaways come from the FP analyses (Section 2.3) used to obtain these results, and discussions of how to interpret and apply the results to improve the reliability of the mission.

2.1 Approach

After separation from the booster used for initial launch, the MSR-SRL spacecraft travels from Earth to Mars in the cruise configuration, with dedicated hardware controlling the flight to Mars. The key components of this phase are shown in Figure 2-1. One of the first stages of EDL is cruise stage separation, which sends the lander (held within a protective aeroshell) towards the Martian atmosphere. The lander includes MAV along with other payloads for use on Mars.

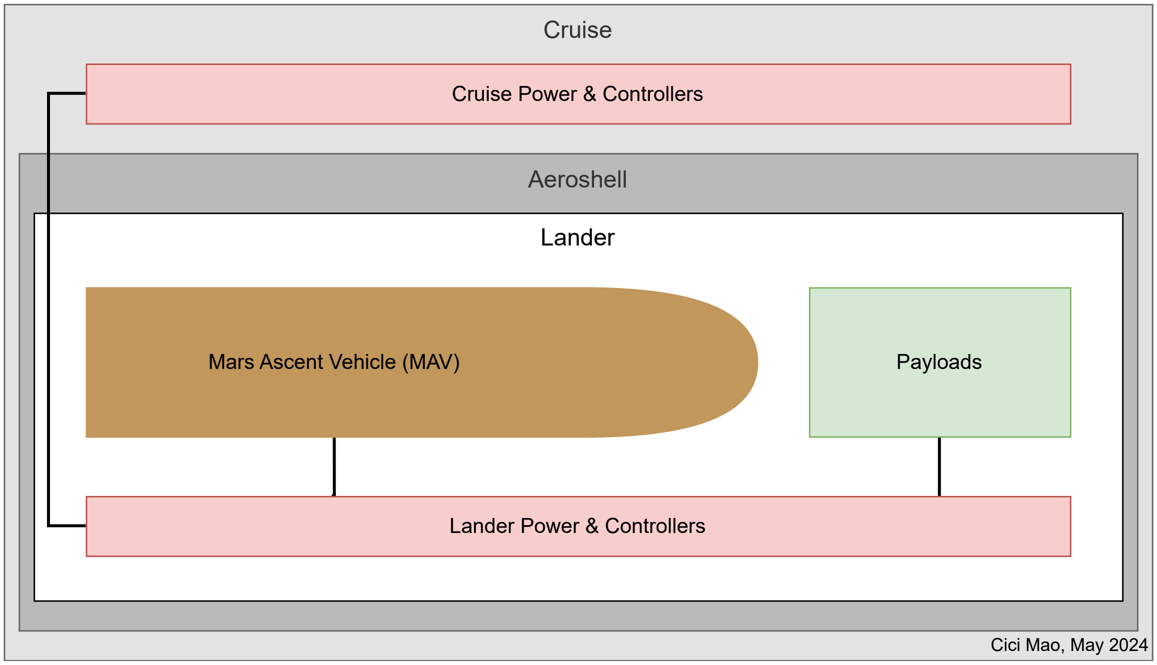

Cruise
Cruise Power & Controllers
Aeroshell
Lander
Mars Ascent Vehicle (MAV)
Payloads
Lander Power & Controllers
Cici Mao, May 2024

Figure 2-1: Notional high-level SRL cruise stage block diagram

2.1.1 EDL Block Diagram

During the transit between Earth and Mars, SRL will be in its cruise stage configuration (see Figure2-2), which provides navigation, power, and thermal regulation to the spacecraft. The cruise stage is detachable and sits on top of the aeroshell, which houses the lander and EDL hardware, and contains solar arrays, flight electronics, navigation and telecom systems, and propulsion. The aeroshell is comprised of the backshell and heatshield, which protects the lander during initial entry into Mars atmosphere. The backshell also contains the parachute and an additional camera, and both it and the heatshield are ejected prior to final descent and touchdown. More details of the EDL process will be explained in Section 2.2.1.

The cruise stage provides critical functionality and control to the spacecraft during

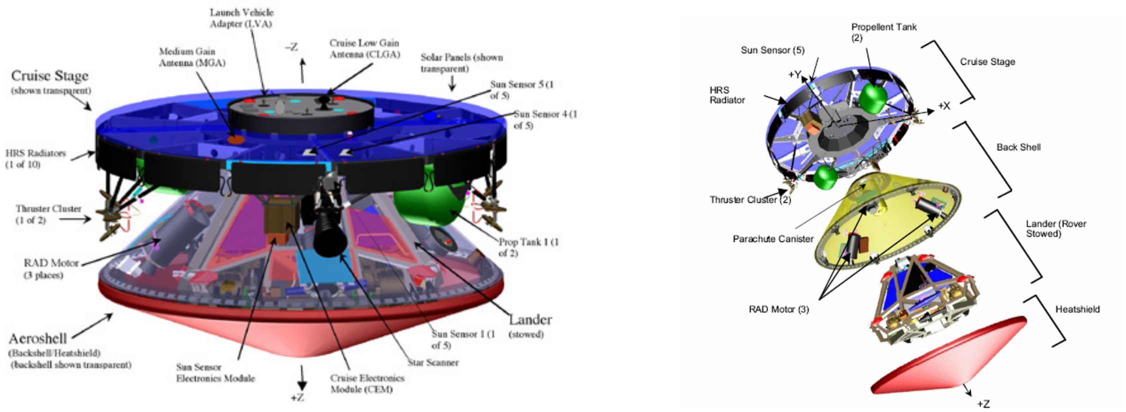


Figure 2-2: Reference cruise stage configuration as used by MER [35]

transit to Mars while the lander is safely housed within the aeroshell. Much of the lander hardware is inaccessible during cruise, so a lot of functionality is also replicated to exist on the cruise stage. Once the spacecraft begins entering the Martian atmosphere, the cruise stage is detached to begin EDL and the lander hardware takes over control.

Our representative high level block diagram of the spacecraft during EDL is represented in Figure 2-3, which includes the cruise stage for context. The lander is fully encased within the backshell and heatshield, with cable umbilicals that connect the lander hardware with those on the backshell or cruise stage. The lander itself can be simplified as a platform atop landing legs. SRL has a propulsion system with reaction control system (RCS) thrusters and supporting cameras and inertial measurement unit (IMU) sensors to provide data to the guidance, navigation, and control system (GNC) to control its path of descent. After landing, it deploys five solar arrays for power production. Much of the flight electronics are housed on the lander platform, including the battery, power control and distribution system, compute elements — which can be considered to be the main computer — and other avionics, thermal control systems, and motor control systems. The lander platform also holds the primary payloads, including the two sample return helicopters (SRH), the sample transfer arm (STA), and the MAV, as well as additional cameras for supporting those payloads and observing lander activities and terrain.

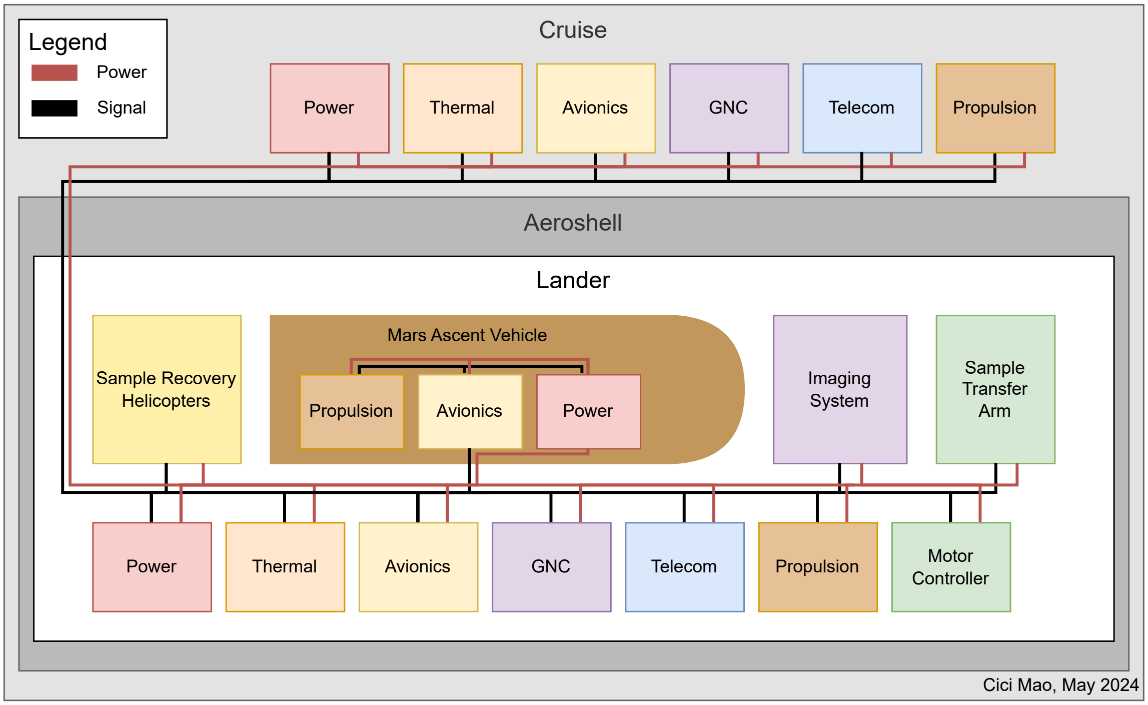


Figure 2-3: Notional Mars lander block diagram, in cruise configuration

2.1.2 MAV Block Diagram

The MAV is the primary payload for SRL, serving as the vehicle for transporting sample tubes into orbit around Mars [48]. It is a two-stage solid propellant rocket with an actively controlled first stage and passively controlled second stage. The MAV payload, called the Orbiting Sample (OS), sits within the MAV payload fairing and holds up to 30 sample tubes. At the end of the mission, the OS will be released from the MAV 2nd stage into Mars orbit for future retrieval.

Before MAV launch is initiated, MAV is housed within SRL, which monitors and maintains its health state. In addition to receiving MAV telemetry, SRL also provides power to charge MAV batteries and thermal control of the solid rocket motors (SRM). After a "point of no return" (PoNR) in the MAV launch sequence, the MAV is cut from SRL and solely reliant on its own systems, as depicted in Fig 2-4. In order for this to work, MAV has multiple batteries within its 1st and 2nd stage, as well as its own flight computers and other associated systems that take over control once the launch sequence begins.

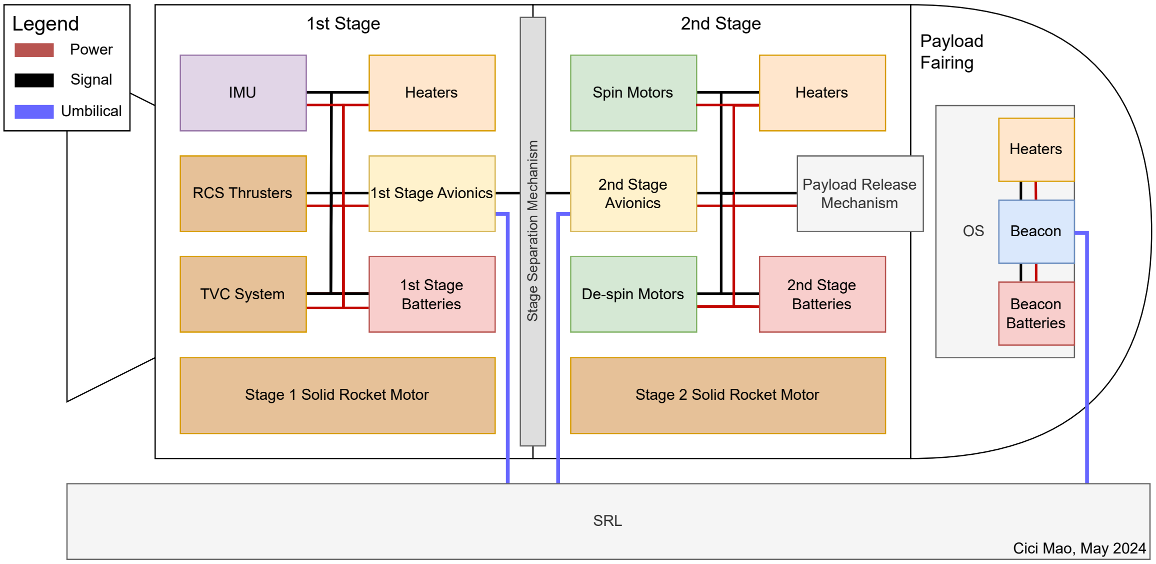


Figure 2-4: Notional MAV block diagram while tethered to SRL

The MAV is composed of a 1st stage solid rocket motor (SRM), interstage, 2nd stage SRM, and payload fairing. Both stages also contain flight avionics, batteries, igniters, and heaters. Active control on MAV's 1st stage is handled by avionics using the inertial measurement unit (IMU), thrust vector control (TVC) system, and reaction control system (RCS) thrusters. The IMU provides orientation data to the guidance, navigation, and control (GNC) software in avionics while the TVC system provides gimballing to the rocket nozzle to control its direction of thrust, and the RCS thrusters provide additional finer control capabilities and stability. These systems on the first stage are used to navigate MAV along a predetermined path to the necessary altitude and trajectory for stage separation and second stage ignition, much like a rocket from Earth launch.

The MAV 2nd stage is similar to the 1st stage, containing flight avionics, batteries, igniters, and heaters. However, unlike the first stage, the 2nd stage is unguided and spin-stable rather than actively controlled. This allows the MAV to save significant mass by not including another TVC and associated avionics, but comes at the cost of no trajectory control within the 2nd stage. The first stage must release the 2nd stage in the correct orientation for its burn, and the 2nd stage requires spin and de-spin motors to spin up and down its angular velocity before and after its flight to achieve spin stability. The 2nd stage also contains a beacon for localization and tracking of the MAV that is used to aid in later OS capture, and controls the mechanism that releases the OS from its payload fairing for orbit insertion.

Critically, due to the significant mass constraints on the MAV, there is very little room for redundancy within the system compared to SRL. While the lander has numerous block redundant hardware elements, including flight computers, power distribution, cameras, radios, etc, the MAV is primarily single string – with only one of each component to save on mass. Lack of redundancy adds risk to the mission since it adds greater chance of single point failures, but that risk must be balanced against engineering requirements.

2.2 Mission ConOps

2.2.1 Entry, Descent & Landing (EDL) ConOps

EDL consists of the rapid-fire sequence of events that take place from the moment the entry vehicle separates from the cruise stage to the moment the lander touches down on Mars. In its entirety, EDL takes approximately just seven minutes to complete - far faster than any telemetry can reach the ground support equipment (GSE) on Earth. During EDL, the entry vehicle is transmitting telemetry back to the ground throughout the entire process, but due to the delay in receiving that telemetry, all the data read by the ground team begins coming in after the spacecraft has already landed. During the landing for M2020, this delay was 11 minutes, but it can be up to 20 minutes depending on the Earth-Mars distance at the time. The EDL process must be carried out completely autonomously by the spacecraft. While JPL has previously demonstrated several iterations of EDL during prior missions, the entire sequence still requires a significant level of focus to ensure mission success.

As shown in Fig 2-5, EDL begins with Cruise Stage separation. As the spacecraft enters the Martian atmosphere at hypersonic velocities, the aeroshell generates intense heat due to air resistance, necessitating a heat shield to withstand the searing temperatures. Following the initial descent, the Heading Alignment Landing Vision System (LVS) Camera (HALCAM) door is ejected and the Enhanced Lander Vision System (ELViS) begins operation, facilitating terrain-relative navigation [15, 21]. Following a period of trajectory corrections, the lander ejects the parachute lid and entry balance mass, deploys the parachute, releases the heatshield, and returns to terrain relative navigation with a second ELViS camera. Once a certain velocity is reached, the backshell separates from the lander, at which point it can fly via its thrusters to reach the final landing site, landing within 60 meters of the targeted location.

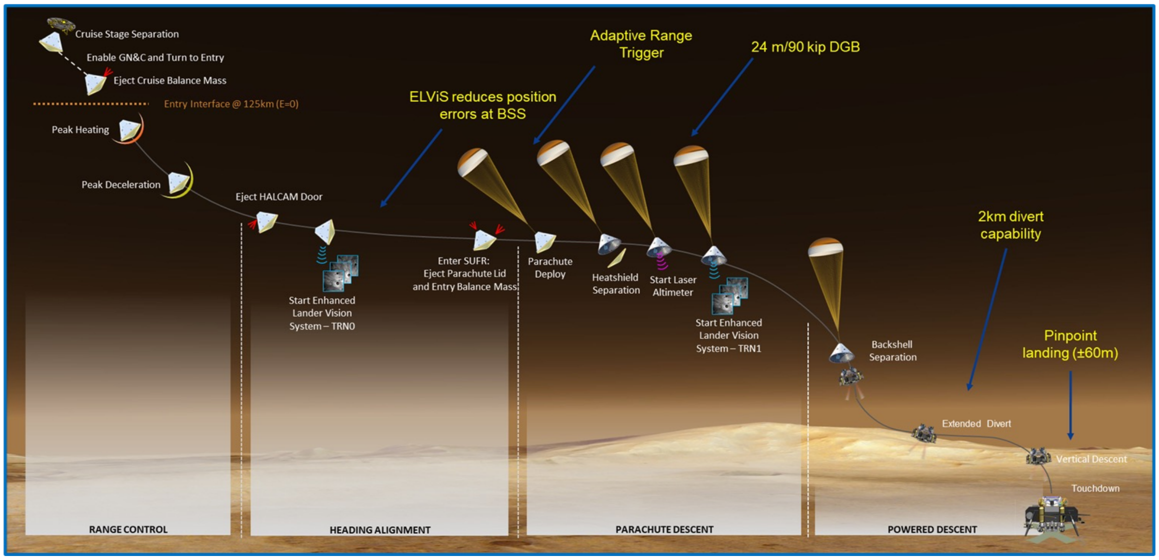


Figure 2-5: SRL EDL flight process [15]

There are many active systems during EDL that all play critical roles, many of which need to work in tandem to successfully land the vehicle. The power system during EDL runs solely off battery power after the cruise stage and its solar panels are ejected – meaning battery health becomes critical to success. The flight computer runs the EDL timeline, including critical event timing, data processing, and commanding. It takes in data from the various landing sensors, such as IMUs, altimeters, cameras, etc to provide sufficient data for landing algorithms to calculate the vehicle's position and determine its path. The landing environment must also be accounted for in modeling, such as time of day or atmospheric conditions like dust factors or air currents. The output of the landing algorithms is used iteratively to command the propulsion system to navigate to and successfully touchdown in the correct landing location.

There is very little room for error during EDL, and every step must succeed for the mission to be able to continue. As a result, fault protection becomes very crucial for EDL, albeit very constrained. A lot of standard FP responses include resetting computers or going into Safe Mode for ground diagnosis, but they aren't viable during EDL as it can result in immediate mission loss. Thus, the EDL fault protection approach focuses on fault *prevention* and mitigation rather than system fault responses.

Much of fault prevention is also encompassed in engineering practices, like designing to safety factors, using best practices, and running an adequate Verification and Validation (V&V) process [26, 29]. This can also include using highly reliable components such as flight tested processors for flight computers, or the release devices used for separation events. However, there are some instances where redundancy and responses can be implemented, though with degraded performance. For example, hot swaps can be attempted between redundant systems – if both are powered on. With the flight computer, hot swapping might still result in the loss of the EDL timeline, so while the option is available, it may take a significant fault to attempt such a response. Sensor fusion can also be attempted if algorithms are able to detect faulty telemetry and adapt to using less sensor data than nominally planned, but the results often are degraded. In these cases though, while degradation of performance is non-ideal, the priority during the EDL phase is to push forward and provide the best chance of the spacecraft landing safely.

2.2.2 MAV Launch ConOps

The primary mission objective of the MAV is to serve as a launch vehicle that will insert the OS into Mars orbit. The process begins with a vertical pneumatic launch of the entire MAV using the Vertically Ejected Controlled Tip-off Release (VECTOR) system, followed by ignition of the first stage. After the first stage's burn and stage separation, the second stage utilizes its pair of side-mounted SRMs to spin up the rocket before the second stage ignites. The second stage then burns until it has reached orbit around Mars, at which point another pair of SRMs de-spin the rocket. Finally, the OS is released into orbit around Mars for capture and return by the Earth Return Orbiter (ERO).

Many of the challenges of the MAV Launch sequence are shared with EDL. Both timelines consist of rapid sequences of events that all must be carried out at the correct time for mission success. They also have the same challenges with communications delay, so both have to be carried out autonomously. The primary difference though, is that while we can calculate when EDL must begin, it cannot be changed or aborted.

The MAV Launch sequence can be aborted and rescheduled, so there is some amount of control over launch conditions and flexibility on mission timeline if issues arise. However, due to the communication delay, there is still a "point-of-no-return" (PoNR) where the ground will no longer have the capability of aborting launch. MAV also has autonomous functions that can trigger an abort if it detects any faults – this system will also have its own PoNR. Past this point, MAV Launch must run autonomously and proceed through completion of its predefined timeline.

Another key challenge posed to designing for MAV Launch is uncertainty. While EDL has a lot of heritage design and past missions to draw data and assumptions from, MAV Launch is a completely new endeavor. Efforts are being made to better model and design for the Martian launch environment – including adapting JPL's EDL modeling tools to simulate Mars launch conditions [1]. However, there is still a lot of uncertainty given the lack of experience launching a vehicle off the surface of Mars, so much of the MAV launch design will be planned ahead of time, with very little autonomous decision making by the vehicle itself – unlike EDL where the lander is able to calculate its own path forward.

In-flight challenges are not the only issues the MAV will have to face – keeping the rocket hardware healthy during the mission is also crucial. SRL is expected to spend about an Earth year on the Martian surface, with MAV launch occurring before the dust storm season begins [48]. During this time, SRL will need to maintain a viable MAV for launch through hundreds of day-night cycles. This includes standard practices of maintaining hardware operational and survival allowable flight temperatures (AFTs), completing checkouts of electronics, and optimizing battery health during charge-discharge cycles. MAV also has unique thermal challenges due to its temperature requirements that have to be balanced against the energy available from SRL during night cycles where solar energy is unavailable [48]. Due to its mass, it's most energy efficient to separate the MAV into 15 heater zones with different minimum AFTs. Platinum resistance thermometers (PRTs) are used in thermal control by SRL and the MAV to properly regulate each zone. Transitioning between survival and operational AFTs for the SRMs must be done gradually and carefully so as to avoid thermal gradients that can result in cracked propellent grains – which would almost guarantee mission failure. On the other hand, the OS cannot be overheated, especially during flight, or it would risk damage to the regolith samples. SRL and MAV work together to monitor and regulate the temperature of the MAV internals to ensure the rocket remains in a safe state for launch.

Thermal considerations are not as significant during MAV flight as they are on the ground, as the short duration of launch to orbit insertion lessens possible environmental impacts. MAV internal insulation helps protect against overheating from impacts of "external aeroheating, plume radiation, SRM nozzle and case thermal soak back" [48]. The MAV also has a set of PRTs during flight for providing temperature telemetry; though these PRTs aren't used in active thermal control, they can provide information about the flight back to the ground for future missions.

2.3 Fault Protection Tools & Approach

This thesis focuses on three main FP analysis tools: Fault Containment Regions (Section 2.3.1), Failure Mode, Effects & Criticality Analysis (Section 2.3.2), and Fault Trees (Section 2.3.3). These tools are used iteratively throughout the design cycle of a system to identify the full set of failure modes and guide future design choices to increase the overall reliability of the mission.

2.3.1 Fault Containment Regions

Fault containment regions (FCRs) are logical sections of a system within which faults can occur, but not propagate beyond [6]. These faults can be both direct, as in physical damage such as short circuits or overheating, and indirect, such as corrupted data or interference. FCRs can be used to describe and facilitate thinking about a system and its high-level interactions, so as to improve its design with respect to fault tolerance.

FCRs can encompass several types of regions. For example, a system with two block-redundant compute elements (CEs) would define each CE as a separate FCR - a fault in one CE would only impact that CE, and would not be allowed to propagate to the other CE, and the mission could continue as planned after swapping to the redundant CE. Likewise, two functionally redundant radio systems would each be drawn as isolated FCRs, as a fault in one should not be allowed to affect the other. Loads on power buses also are contained within their own FCRs, as a fault on a load must not impact the spacecraft bus. Similarly, devices on data buses also will have their own FCRs. FCRs will also isolate non-critical elements, such as engineering cameras, and any equipment that is only conditionally needed, such as electrical system protection devices.

2.3.1.1 FCRs and Redundancy Types

FCR diagrams are visual representations of these fault containment regions in the form of a block diagram. While they look very similar, it encodes specific information on functional areas and redundancy types. For instance, FCRs are useful tools for identifying single string paths in systems, where there is only one possible connection for a function to work.

An example of a single string system would look like (1) in Figure 2-6, where the loss of any component in the path would mean loss of the ability for the processor to command a camera. Each FCR is represented by a rounded-edge rectangle.

Example (2) has two block redundant cameras, and the main processor (MP) can command either camera via the camera control card (CCC). In this case, the loss of a camera would mean swapping to the redundant camera instead of losing the function entirely, but since the MP and CCC are still single string, loss of either of those components would result in loss of the function.

Examples (3) and (4) contain redundant MPs and CCCs. The |X| symbol indicates that the components are cross-strapped, which means that either MP-A or B can communicate with either CCC-A/B, so this system can handle loss of one of either. Example (4) also represents block redundant cameras A or B, drawn in with two parallel lines. In this path, both MPs can command either camera, but each camera is only connected to its associated CCC. Loss of CCC-A would also result in the loss of camera-A, but if that is the only loss in the system, the MPs can still command camera B via CCC-B.

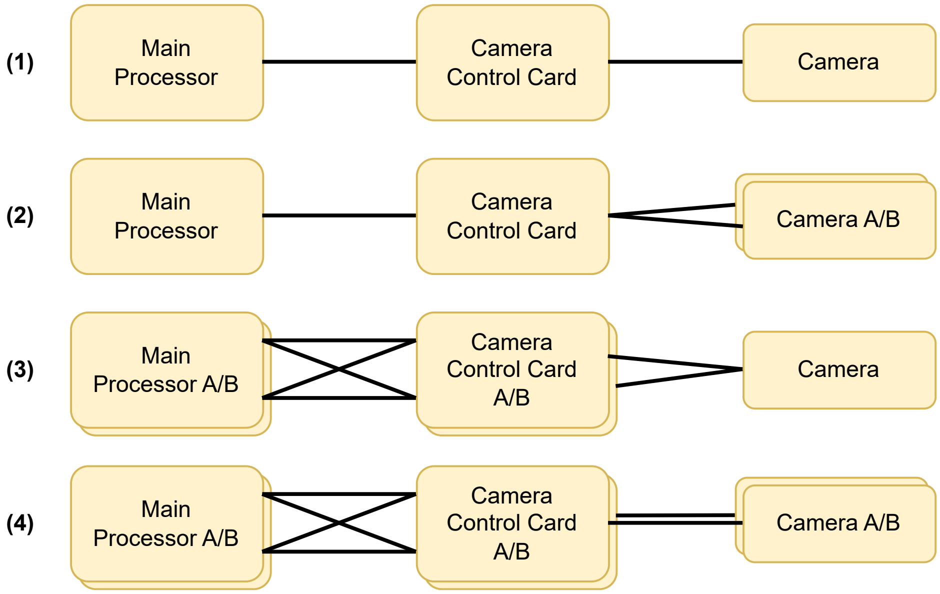


Figure 2-6: Sample FCR demonstrating 1) single string, 2) block redundancy, 3) and 4) cross strapping.

Functional groupings can also be conveyed in FCRs. Figure 2-7, shows an alternative FCR design for a single string MP and CCC with redundant cameras. In this architecture, the CCC doesn't have its own FCR but rather exists within a larger FCR that groups the entire camera system. Cameras A/B each have their own FCR nested within this camera system FCR as a fault in one camera shouldn't impact the other camera, nor should it propagate to the CCC. However, a fault in the CCC necessarily means you lose the ability to command the cameras, so the CCC itself doesn't necessarily require an FCR to limit faults from it to the cameras.

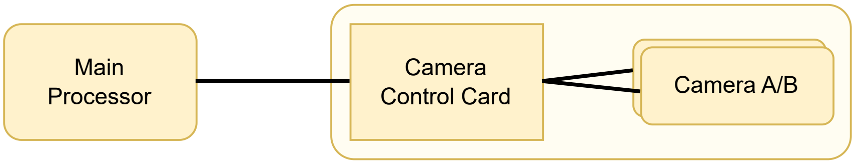


Figure 2-7: Sample FCR with functional group encompassing camera subsystem

It's also important to note that while FCRs often align with hardware block elements, implementing fault propagation boundaries costs resources, so understanding functional groups is beneficial for optimizing FP design. The FCR is complemented and utilized by the FMECA and FTA tools which delve deeper into particular faults and the system level impact of their occurrence.

2.3.2 Failure Mode, Effects & Criticality Analysis

The Failure Mode Effects & Criticality Analysis (FMECA) is a tool used to analyze possible failure modes of a system at its component level, and determine the system and mission impact of the identified faults. Along with the Fault Tree Analysis (FTA) described in Section 2.3.3, the FMECA helps methodologically identify the set of possible failure modes a system can experience and assess their severity. There are also a variety of different types of FMECAs depending on what view is useful for a system analysis. For example, hardware FMECAs are extremely low level, with analysis down to the individual transistors or pins within components. Interface FMECAs primarily focus on the connections between systems at FCR boundaries, assessing how faults can propagate across said boundaries and impact multiple systems. Functional FMECAs, which is the focus of this work, consider the functions that system components provide and analyze failures associated with loss or degradation of that function [11].

The FMECA works by breaking down a system into its constituent parts and assessing each part for all of its possible failure modes. While this work will focus on the system level functional FMECA, it can also be conducted at the subsystem or component level. FMECAs are managed via a table, grouping individual elements by row and attributes of each by column. These columns include:

System and Functional Element: Define what particular functional element of which broader system is being analyzed.

Failure Mode: Particular ways the functional element can fail or is known to fail.

Most Likely Cause: What is the mostly likely reason for the described failure mode to occur?

Local Effect: Within the functional element, what are the observable effects of this failure?

System Effect: How will this failure mode affect the spacecraft system or mission as a whole?

Detection Method: How can the spacecraft or ground control detect a failure?

Compensating Provisions: In the event this failure mode occurs, what are actions that can be taken to address the failure or mitigate its impact?

Preventative Measures: What are actions that can be taken in advance to prevent this failure mode from occurring?

Criticality: Scale of 1-6 indicating the severity of impact this failure mode would have on the overall mission. Examples are shown in Table 2.1.

By conducting this analysis, the FMECA provides a view into the safety critical and high risk areas of a system's design. While not all risks to the system necessarily need to be mitigated against, or even have possible mitigations, it's important to identify these faults to better understand the risk. In particular, FMECA-identified elements with criticality of 5 or 6, also known as single point failures (SPFs), must be carefully considered and managed. If the probability of a particular SPF is sufficiently low, it may simply be within acceptable mission risk; otherwise, it is a critical failure mode to mitigate in design where feasible.

Table 2.1: FMECA Criticality Scale [17]

Criticality	**Description**
6	Complete Loss of Mission (LOM)
5	Major loss or degradation of mission
4	Significant loss or degradation of mission
3	Loss or degradation of system redundancy
2	Limited impact on mission; potential loss of robustness
1	Negligible impact on mission

When used iteratively throughout the design process, the FMECA allows for well-informed fault protection architectures that are able to appropriately address the failure modes the system may see during operations, thus improving the overall reliability of the final design. But on its own, the FMECA's focus on hardware component level faults can miss operational faults, which is addressed in the FTA.

2.3.3 Fault Tree Analysis

A fault tree analysis (FTA) is a tool that generates a tree-like model of a system composed of a set of possible failure paths that stem from a top-level failure event [14]. FTAs are created along with FMECAs to help systematically identify the full set of possible failure modes in a system. Unlike FMECAs that are bottom-up analyses, FTAs are top-down analyses generated by recursively breaking down failure events into their possible causes.

The FTA consists of a top-level failure event (A) that stems from intermediate (C) or basic events (B, D, E), connected by "AND" and "OR" logic gates, as demonstrated in Figure 2-8. In FTAs, "AND" gates imply redundancy, while "OR" gates show multiple paths of causing a single event. The model assumes that basic events do not need to be analyzed further, while each intermediate event will break down further to other intermediate or basic events until you reach a bottom level of solely basic events.

Similar to FMECAs, FTAs can be conducted across varying levels of abstraction depending on the selection of the top-level event and the level of detail in the basic

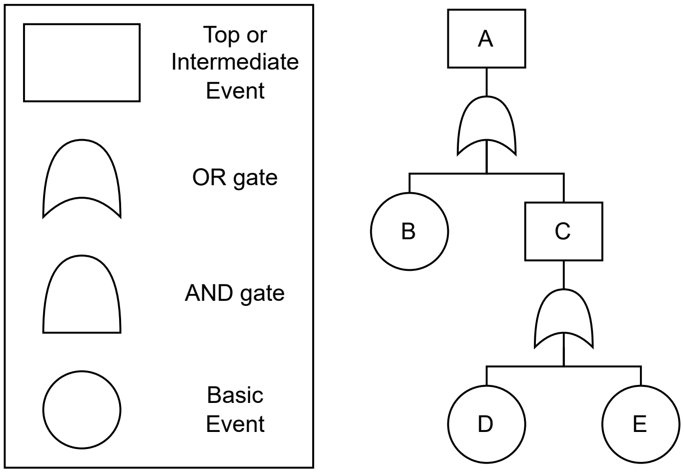


Figure 2-8: Fault tree legend and sample fault tree

events. Rather than using a full mission-level FTA, this work will focus on the top-level events of EDL and MAV launch separately. Coupled with the FMECA and FCRs, these tools will provide insight to the SRL FP implementation and identify areas of risk.

Chapter 3

Fault Protection: Entry, Descent & Landing

Fault Protection for EDL has a few unique challenges that inform the entirety of the EDL architecture. The rapid timeline, often referred to as the "seven minutes of terror" [22], limits possible fault responses, and entirely precludes human intervention. FP for EDL must focus on a combination of preventing faults in the first place and preparing rapid and autonomous responses to fault conditions where possible.

This chapter begins with all three F-Tool analyses for EDL in Section 3.1. Each analysis consists of a visual representation accompanied by exposition on selected features within, and discussion of takeaways from that singular analysis. Section 3.2 then considers the results of all three, discussing how best to approach EDL from a FP perspective within the constraints of the system.

3.1 F-Tools for EDL

3.1.1 Fault Containment Regions (FCR)

A representative FCR diagram shown in Figure 3-1 covers a selection of the high-level systems involved during and immediately after EDL. This shows the fault containment regions of the spacecraft in its initial EDL configuration and the interconnects between major elements. At the start of EDL, the cruise stage is ejected from the rest of the spacecraft, leaving primarily the aeroshell and lander electronics. The solar arrays are stowed within the lander until after touchdown, leaving the spacecraft to run off of battery power. Some elements, such as EDL cameras, get ejected during EDL, but the FCR still includes them, as they are critical during the relevant earlier phases of EDL.

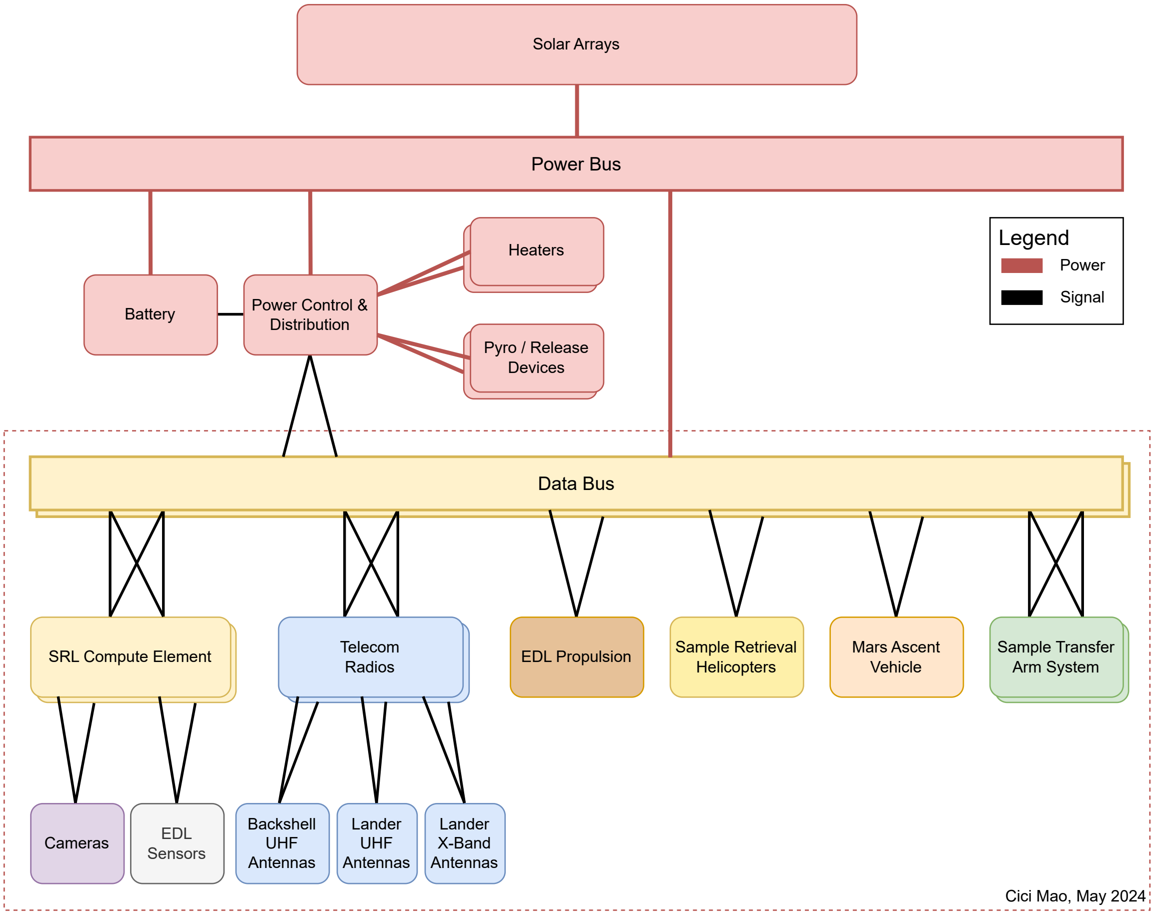


Figure 3-1: Proposed SRL Fault Containment Regions

3.1.1.1 Avionics

The Compute Element (CE) is the main computer for SRL's on-board processing. While certain tasks such as vision processing are delegated to coprocessors, the CE handles the majority of SRL's compute requirements. These functions range from timeline management and operations to telemetry and housekeeping. As the CE is such an important piece of hardware, it is implemented as a pair of redundant radiation hardened processors [31], with a few operating modes available to handle the varying time and power constraints at different points of the mission as discussed in Section 3.2.

Both CEs communicate with almost all digital systems on the lander via a cross-strapped pair of MIL-STD-1553 data busses [9, 31]. This dual redundant interconnect implementation offers significant fault protection advantages, as not only are faults within the buses contained, it also prevents certain faults from spreading between other systems in the spacecraft.

Every connection to the bus goes through a line transceiver, which acts as a fault isolation boundary. If a data bus experiences a short circuit, a stuck-on high voltage, or any other catastrophic failure, the line transceivers protect all attached equipment, thereby protecting the health of the overall system. As devices are attached to both redundant buses, a catastrophic failure to an entire data bus will thus only reduce system redundancy. In this case, the spacecraft can automatically failover to the 2nd data bus and continue operating as otherwise planned, with no impact on operations. Finally, the line transceivers protect the health of the overall system from failures in individual devices. The line transceivers are designed to protect the operation of the bus should any single device fail into a stuck-on a state where it attempts to continuously transmit across the bus, preventing such a failure from impacting the remainder of the system.

3.1.1.2 Telecom

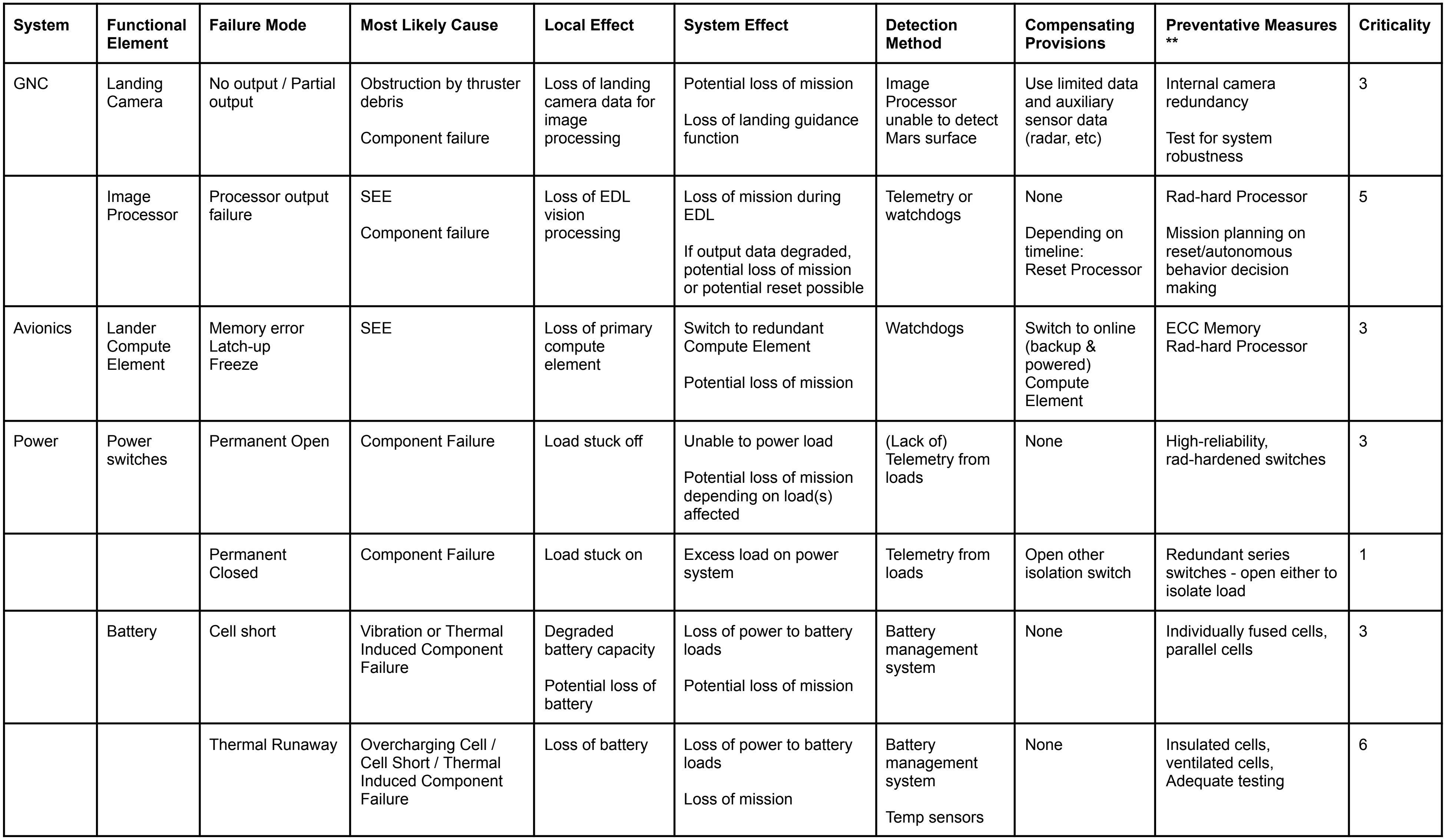
Another critical component of the MSR mission is the communication link between the lander and ground control. SRL has a set of two radios, each of which can drive three antenna systems depending on the phase and status of the mission [44]. During surface operations, ground control relies on telemetry from the lander to plan the sample transfer and launch sequences, and must also reliably transmit these instructions to the lander. This is done primarily via the lander's UHF antennas in conjunction with the Mars Relay Network (MRN). However, the lander also has the capability to communicate directly with the DSN on Earth via an X-Band antenna system, albeit at a significantly reduced data rate. This redundancy allows for degraded mission continuation in the event of a wide variety of failures involving the UHF system (including external failures within the MRN), as opposed to a dual-redundant UHF antenna system which could only handle hardware failures to the radio or antenna itself.

Unlike surface operations, SRL operates in a transmit-only mode during EDL. Since the duration of EDL is shorter than the round trip speed of light from Earth to Mars, there is no advantage in attempting to allow ground control to make real-time adjustments to the landing sequence. SRL only transmits status information for later analysis. While this information is valuable, especially in the event of catastrophic failure during landing, failures in this system during EDL are unlikely to impact the remainder of the mission. As such, SRL has only limited communication redundancy during EDL, in that it relies on a single set of UHF antennas integrated into the backshell to send telemetry to ground control.

3.1.1.3 Propulsion

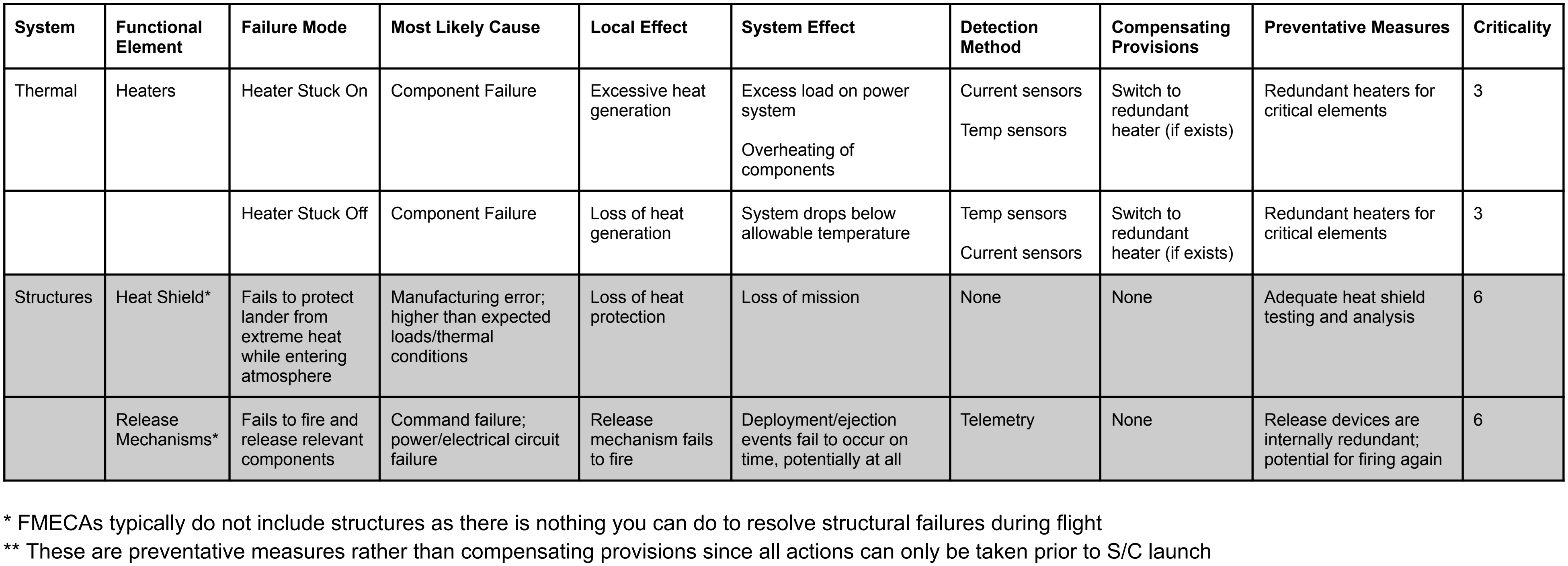
Not all systems can have redundant options built in. Although these systems are generally engineered to contain faults, internal faults may still cause catastrophic failure. Despite being designed to not directly damage the remainder of the lander, generally allowing the avionics systems to report failures to ground control and possibly remediate the issues, failures in these systems can still indirectly jeopardize the remainder of the lander. For instance, the landing propulsion system is far too heavy to have any redundant backups. Consequently, a failure in this system would result in the lander impacting Mars at high velocity, thus destroying the remainder of the lander. The impact of potential failure modes like these need to be analyzed separately from the FCR, using tools such as FMECA and FTA. Only some failure modes can be mitigated with redundancy, those that remain need to be designed against failure with high reliability. The FMECA and FTA can help determine relative criticality of these systems to help prioritize reliability appropriately amidst engineering trade-offs.

Table 3.1: Proposed EDL Failure Mode, Effects & Criticality Analysis (FMECA)



System	Functional Element	Failure Mode	Most Likely Cause	Local Effect	System Effect	Detection Method	Compensating Provisions	Preventative Measures **	Criticality
GNC	Landing Camera	No output / Partial output	Obstruction by thruster debris Component failure	Loss of landing camera data for image processing	Potential loss of mission Loss of landing guidance function	Image Processor unable to detect Mars surface	Use limited data and auxiliary sensor data (radar, etc)	Internal camera redundancy Test for system robustness	3
	Image Processor	Processor output failure	SEE Component failure	Loss of EDL vision processing	Loss of mission during EDL If output data degraded, potential loss of mission or potential reset possible	Telemetry or watchdogs	None Depending on timeline: Reset Processor	Rad-hard Processor Mission planning on reset/autonomous behavior decision making	5
Avionics	Lander Compute Element	Memory error Latch-up Freeze	SEE	Loss of primary compute element	Switch to redundant Compute Element Potential loss of mission	Watchdogs	Switch to online (backup & powered) Compute Element	ECC Memory Rad-hard Processor	3
Power	Power switches	Permanent Open	Component Failure	Load stuck off	Unable to power load Potential loss of mission depending on load(s) affected	(Lack of) Telemetry from loads	None	High-reliability, rad-hardened switches	3
		Permanent Closed	Component Failure	Load stuck on	Excess load on power system	Telemetry from loads	Open other isolation switch	Redundant series switches - open either to isolate load	1
	Battery	Cell short	Vibration or Thermal Induced Component Failure	Degraded battery capacity Potential loss of battery	Loss of power to battery loads Potential loss of mission	Battery management system	None	Individually fused cells, parallel cells	3
		Thermal Runaway	Overcharging Cell / Cell Short / Thermal Induced Component Failure	Loss of battery	Loss of power to battery loads Loss of mission	Battery management system Temp sensors	None	Insulated cells, ventilated cells, Adequate testing	6

Table 3.1: (Cont.) Proposed EDL Failure Mode, Effects & Criticality Analysis (FMECA)



System	Functional Element	Failure Mode	Most Likely Cause	Local Effect	System Effect	Detection Method	Compensating Provisions	Preventative Measures	Criticality
Thermal	Heaters	Heater Stuck On	Component Failure	Excessive heat generation	Excess load on power system Overheating of components	Current sensors Temp sensors	Switch to redundant heater (if exists)	Redundant heaters for critical elements	3
		Heater Stuck Off	Component Failure	Loss of heat generation	System drops below allowable temperature	Temp sensors Current sensors	Switch to redundant heater (if exists)	Redundant heaters for critical elements	3
Structures	Heat Shield*	Fails to protect lander from extreme heat while entering atmosphere	Manufacturing error; higher than expected loads/thermal conditions	Loss of heat protection	Loss of mission	None	None	Adequate heat shield testing and analysis	6
	Release Mechanisms*	Fails to fire and release relevant components	Command failure; power/electrical circuit failure	Release mechanism fails to fire	Deployment/ejection events fail to occur on time, potentially at all	Telemetry	None	Release devices are internally redundant; potential for firing again	6

* FMECAs typically do not include structures as there is nothing you can do to resolve structural failures during flight

** These are preventative measures rather than compensating provisions since all actions can only be taken prior to S/C launch

3.1.2 Failure Mode, Effects & Criticality Analysis (FMECA)

The representative FMECA shown in Table 3.1 partially analyzes a selection of the high-level systems involved during EDL. A full FMECA would be far more detailed and thorough, and there would likely be additional FMECAs analyzing individual modules down to a board or component level instead of staying this general. However, we can still gain valuable information from high level functionality by looking at major components on the spacecraft and analyzing a select few common or likely failures for different areas across the system. Further analysis would find more specific causes than can be derived from the current level of analysis, but would also require more detailed documentation on the system design that is not yet available.

3.1.2.1 Power Switches

The FMECA in Table 3.1 analyzes the power distribution system's switches as a single element, and shows how they have failure modes with varying criticality. A power switch failing open ("off") or closed ("on") is likely caused by some component failure (which could likely be identified by a FMECA focused on the switch itself). Both of these failures can be detected via various means, including measuring the voltage of the switched circuit or otherwise detecting that the load is still powered on.

This, however, is the extent of the similarities. A switch stuck **closed** will leave some element of the system powered on, possibly increasing the power draw of the system. However, as most power distribution systems switch both the high and low side of the circuit [5], the load can still be powered down by opening the other side. Furthermore, many loads can go into low power modes while still powered on. As such, this particular failure mode is unlikely to cause significant impact to the operation of the mission and is identified as a level 1 criticality.

A switch stuck permanently **open** can have a much larger impact on the system. While the exact impact on the broader system depends on what the particular switch is powering, this failure is likely to completely disable a single subsystem powered by said switch. Without specifically building in redundancy to the power switch, there is little that can be done to remedy a stuck-open fault. A switch powering a critical non-redundant system could likely earn a criticality of 5-6. However, as many systems involved in the lander have redundant counterparts, a stuck-open switch will generally result in a loss of redundancy, and thus this generic case is assigned a criticality of 3.

3.1.2.2 Batteries

Battery failures tend to spell loss of mission (LOM), especially during EDL when there is no power available from solar arrays. If a battery overheats and experiences thermal runaway, the mission will soon be lost (criticality 6) with no hope for recovery. Not only will the battery cease providing power to the remainder of the system (meaning everything will shut down), a failure like this one could end up literally burning the remainder of the spacecraft due to the intense heat generated.

While a complete battery failure cannot be compensated for or recovered from without significant design changes (such as a redundant battery), certain internal failures can be mitigated to prevent LOM. For example, batteries can be designed such that cell shorts can be isolated to one section of the battery rather than propagating through, resulting in decreased capacity but not necessarily LOM. These types of failures would be best investigated in a battery-focused FMECA due to the complexity within this system on its own.

3.1.2.3 GNC Image Processor

The GNC Image Processor is used to perform real-time terrain relative navigation during the descent and landing stages of EDL. This feature is necessary for precise landing site control, as it provides the only source of map-relative location. Losing the image processor will cause a local effect of a loss of EDL vision processing, and thus a system level effect of up to LOM. As one of the most likely causes of failure is a Single Event Effect (SEE) due to ionizing radiation [40], one of the most significant preventative measures is that the entire image processor is built from Rad-Hard components such as the RAD750 processor and RTAX2000S FPGA used in M2020

[47]. As the lander can still attempt to land without the image processor, but with degraded probability of success, this failure is assigned a level 5 criticality.

3.1.2.4 Structures

Structural elements and mechanisms are typically not included in spacecraft FMECAs. Simply put, any structural element failure will almost certainly lead to mission failure (criticality 6), as there is no way to repair or swap out these elements after launch. As hinted in this analysis, there is only room for one heat shield, and a failed release mechanism often can't simply be re-tried, as the critical time to release has already passed. Instead, structural elements and mechanisms must be carefully designed and tested to ensure they will meet mission requirements with appropriate margins and high reliability.

3.1.3 Fault Tree Analysis (FTA)

The EDL Fault Tree Analysis in Figure 3-2 is a representative example of how one can construct an FTA. This FTA starts with the top-level failure event of EDL, namely EDL Fault: Failure to land in target Mars landing location. This is then broken into two broad intermediate events - Failure to safely land on the surface (i.e. crash landing), and GNC failure (for soft landings, but in the wrong location). Each of these are then further subdivided until the bottom layer which is made of exclusively Basic Events.

As this FTA shows, the vast majority of the Basic Events chain directly through OR gates to the top level event, meaning any single one of these root failure modes would directly cause mission failure.

However, there is one AND gate in this FTA, joining the failure of the primary and backup Compute Elements. This shows that either CE can fail without directly causing LOM, as their redundancy prevents a single failure from propagating. Unfortunately, both CEs share "Power system failure" as a common basic event, meaning that particular failure could take both CEs offline simultaneously. This hints at a nu-

Figure 3-2: Proposed EDL Fault Tree Analysis (FTA)

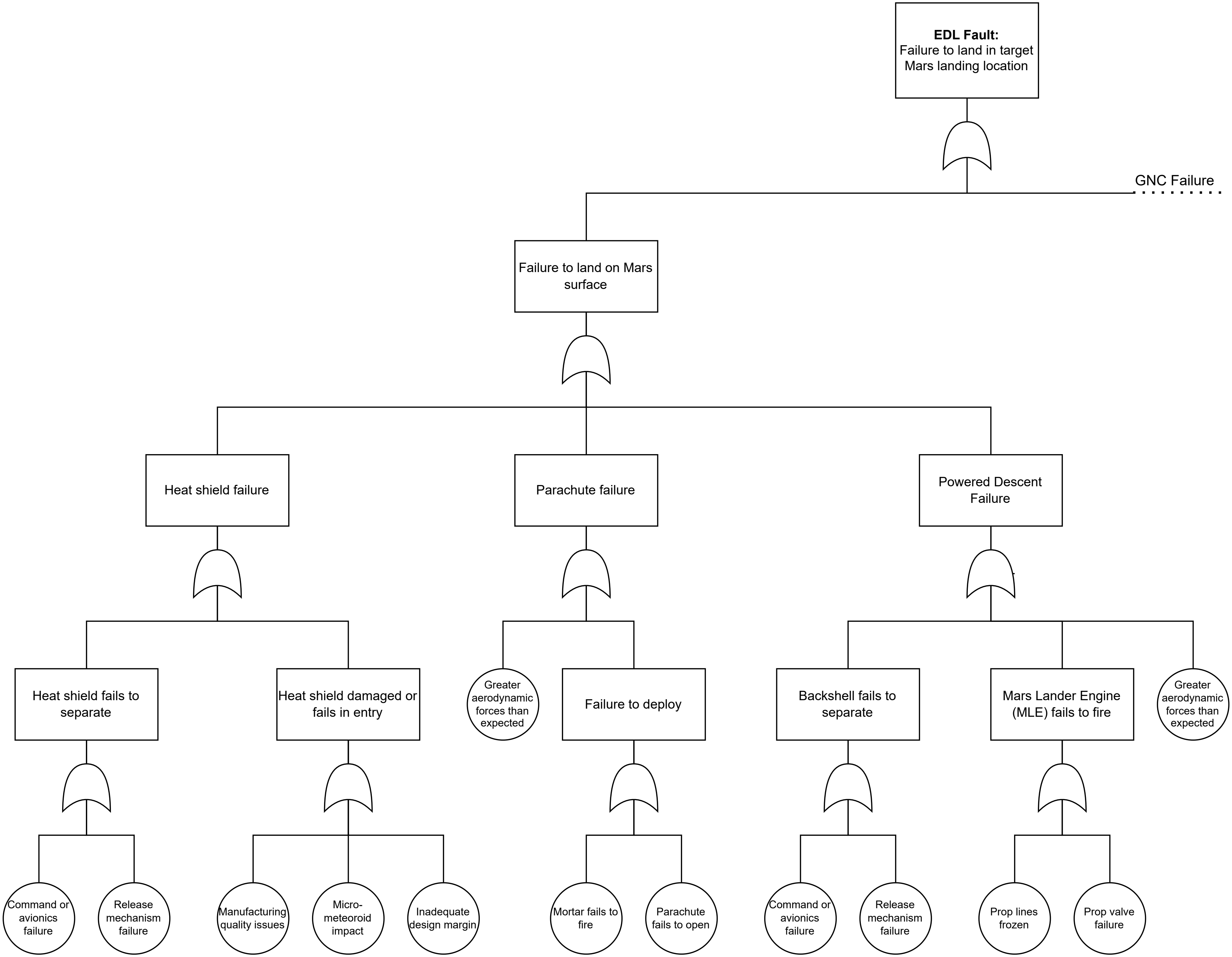
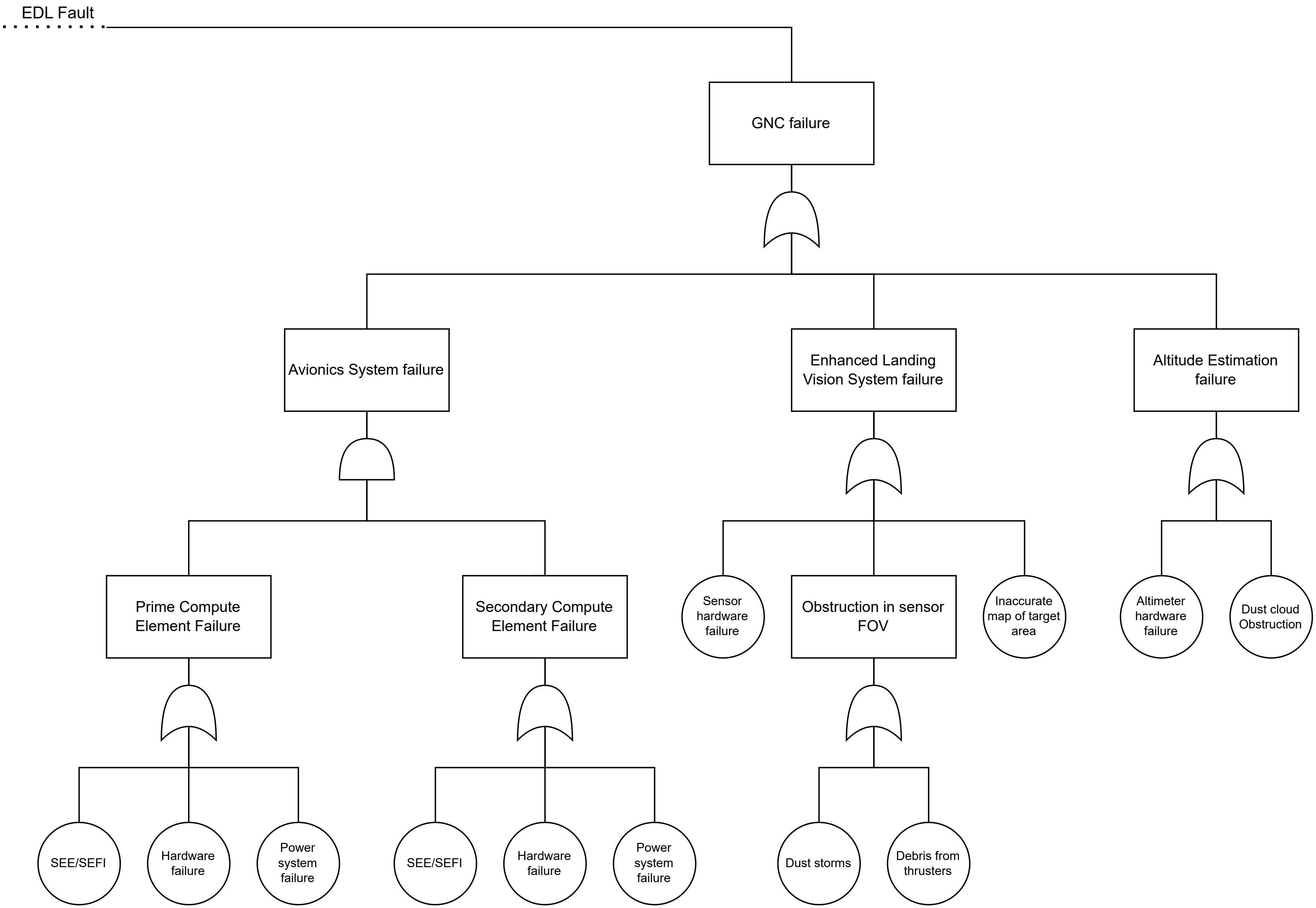

EDL Fault:
Failure to land in target Mars landing location
GNC Failure
Failure to land on Mars surface
Heat shield failure
Parachute failure
Powered Descent Failure
Heat shield fails to separate
Heat shield damaged or fails in entry
Greater aerodynamic forces than expected
Failure to deploy
Backshell fails to separate
Mars Lander Engine (MLE) fails to fire
Greater aerodynamic forces than expected
Command or avionics failure
Release mechanism failure
Manufacturing quality issues
Micro-meteoroid impact
Inadequate design margin
Mortar fails to fire
Parachute fails to open
Command or avionics failure
Release mechanism failure
Prop lines frozen
Prop valve failure

Figure 3-2: (Cont.) Proposed EDL Fault Tree Analysis (FTA)



anced limitation of FTAs: when basic events are correlated (or are the same event), faults can propagate through multiple branches of the tree where otherwise not expected. The FCR analysis can then be used to help understand which basic events are independent, and which may influence each other.

3.2 FP Approach to EDL

The proposed general approach to EDL involves including as much active redundancy available as possible while simultaneously disabling responses to almost all faults [24]. These FP responses are turned off because there is no mitigating or resolving action that can be taken. Smaller faults such as heater or temperature sensor errors are recorded and then ignored, to be dealt with after landing. Larger issues such as undervoltage errors or shorted circuits may cause loss of mission if left unresolved, but simultaneously the only available actions to repair (such as powering off loads, power cycling systems, etc.) will all guarantee loss of mission. In these cases, the only hope for mission success is that the reading of the error was itself an error, and the system is still actually healthy.

There are limited cases where fault protection systems can still recover from errors during EDL. One example can be found in the CEs, as initially demonstrated by the Curiosity mission [26]. Both CEs are kept powered on during EDL to enable a rapid fault response. In nominal conditions, the "prime" CE is the only CE to issue commands during EDL. However, the "online" (backup) CE runs a stripped down version of the EDL software, named "Second Chance". It continuously shadows the timeline execution and sensor data available on the bus, running the same navigation control loops as the prime CE. In the event an error is detected within the prime CE, the backup can take over instantly.

As a point of comparison, only one CE is enabled at a time during surface operations. Persistent faults in the active CE can generally be mitigated by power cycling or switching to the backup. This isn't an option during EDL, as it would take too long to boot the backup and redetermine position and attitude.

In this vein, there are also slight differences between EDL Approach vs. EDL itself – during Cruise the system begins transitioning to EDL Approach which performs checkouts and sets up the system for entering EDL. Faults during EDL Approach are treated with more urgency than during typical Cruise, but the ground can often still intervene depending on the duration until EDL begins.

During M2020, CE SEFIs during Cruise were resolved with a full reset, but during EDL Approach and EDL, they had to create a decision tree so they could react to how they'd handle resetting and in which cases they would, or just switch to the backup computer and go single string [10].

The other form of FP that can be used during EDL can be found in the design of the GNC algorithms used to control the process. For example, the attitude and position estimation algorithms can be designed to be tolerant to certain sensor faults, using sensor fusion to operate despite degraded sensor data. Unfortunately this can only go so far, as sensor fusion relies on accurate models of the spacecraft and its environment, and can only handle limited input degradation before it will fail entirely.

Given these constraints, the majority of EDL FP comes in the form of prevention rather than reaction. Certain classes of faults can be predicted and engineered around to reduce or eliminate the chance of disruption. However, this requires additional resources, be it engineered margin or redundant systems. These come with inherent tradeoffs, and must be designed in relation to the broader system in order to maximize reliability in the context of the acceptable risk posture while meeting all other requirements.

Chapter 4

Fault Protection: MAV Launch

MAV launch will be the first of its kind, which in and of itself is a major challenge when designing fault protection. One of the most important steps in designing a FP system is understanding the difference between normal and abnormal, but this is inherently challenging for a first-of-its-kind mission such as this one. Significant effort is required to model and predict the launch environment, such as by adapting tools originally designed for EDL simulations [1]. The MAV is also extremely mass constrained, meaning all systems must be designed with tight margins and little room for error. It will live in the harsh Martian environment, enduring significant thermal cycles that must be continuously monitored and managed. And finally, the MAV launch process will be complete before any telemetry can reach Earth, meaning the entire flight must be completely autonomous once initiated.

This chapter primarily analyzes the MAV from the moment it is launched by VECTOR through the release of the OS into orbit around Mars, though it also includes some pre-launch FP related opportunities.

4.1 F-Tools for MAV

4.1.1 Fault Containment Regions (FCR)

A representative FCR diagram shown in Figure 4-1 covers the high-level systems in the MAV. This shows the fault containment regions of the spacecraft at the beginning of the launch process. The dashed boxes both represent functional groups, and show how stages separate as the MAV launches to orbit, ending with only the payload fairing orbiting Mars. Within each stage is a set of batteries that power said stage, and there is no power sharing available across stages. The batteries therefore cannot have their own fault containment region - any fault within them will immediately directly affect the remainder of that stage.

As the MAV is extremely mass-constrained, it has no internal redundancy at all. This results in a flat FCR diagram, showing the relative fragility of the system. Note that while there are multiple heaters, they are attached to different portions of the MAV and as such are not redundant [48]. Also known as a single string design, a failure in any of these FCRs will likely lead to LOM, and worse, loss of the entire MSR campaign. Because the MAV requires a high number of sequences of events to occur exactly as designed to insert the OS into the correct orbit, the lack of hardware redundancy also adds risk to each event, as any single failure is unlikely to be able to be compensated by other hardware elements. However, it is still important to define and consider the fault containment regions [6], as they can help engineers analyze the system at a systems level, helping to identify opportunities to reduce the impact of faults and improve resiliency as well as reassess if each single-string element is truly appropriate for the MAV design. The faults specific to particular hardware elements will be assessed in conjunction with the FMECA.

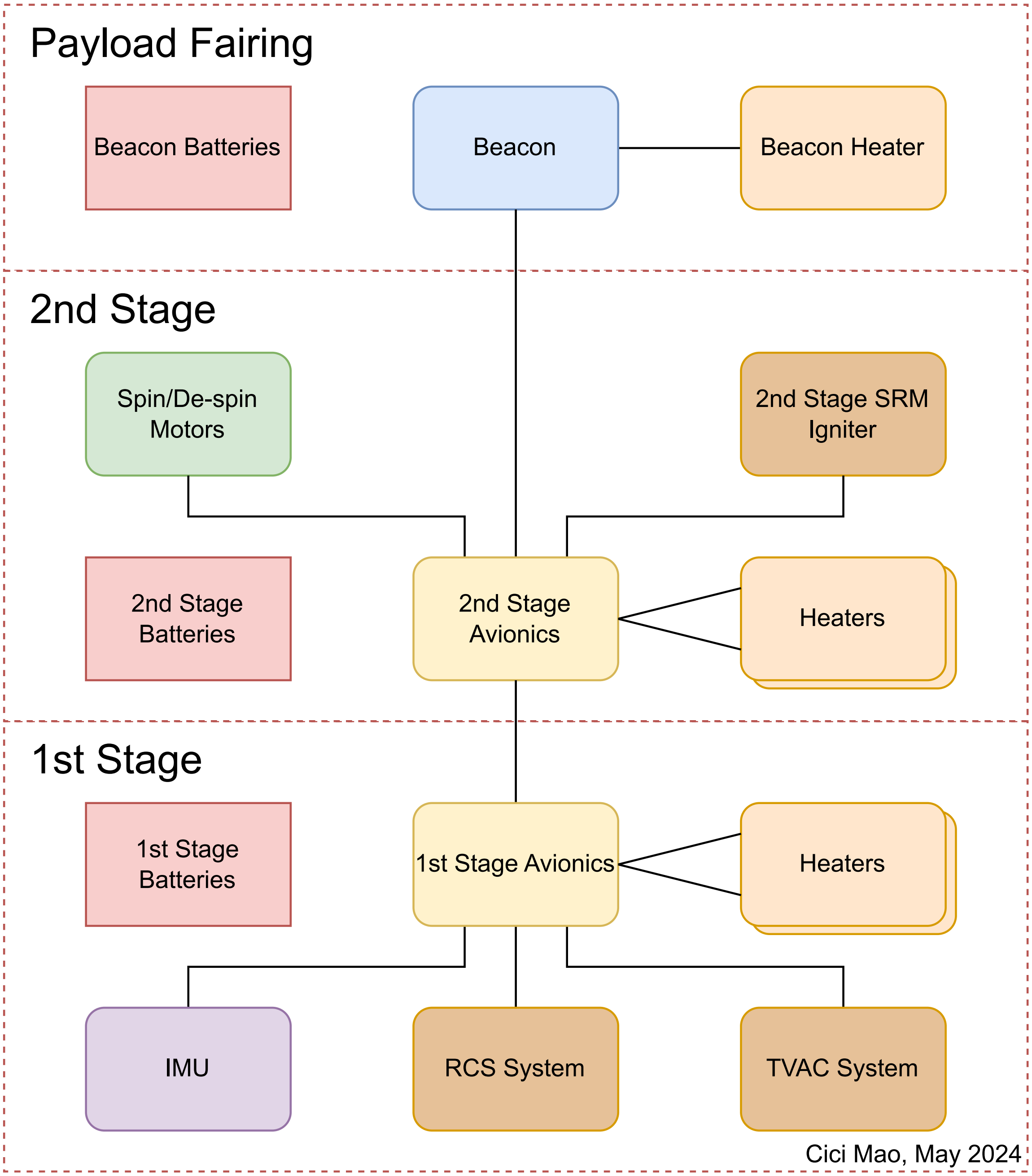


Figure 4-1: Proposed MAV Fault Containment Regions

4.1.2 Failure Mode, Effects & Criticality Analysis (FMECA)

The representative FMECA shown in Table 4.1 analyzes a selection of the high-level systems involved during MAV launch. As with EDL's FMECA, a full analysis would be far more detailed and thorough, but would require design details that are not publicly available.

4.1.2.1 Batteries

As with EDL, battery failures in the MAV tend to cause LOM (criticality 6). One of their more likely failure modes is going under their designed voltage, which itself would be likely if the batteries are too cold. As the batteries are the sole power source for each stage, any failure would immediately disable all electronics in that stage and thus cause LOM.

Battery concerns within MAV are particularly focused on battery health within the thermal environment because the lander maintains temperatures just above the lower survivable limits of each of MAV's systems while stowed. Faults within that thermal regulation system could impact the MAV's battery health, potentially degrading performance below the minimum acceptable levels.

The MAV batteries have no failure detection mechanisms or compensating provisions available should a fault occur, as there is no mass available for any of these. While each stage's independent batteries potentially have excess energy available due to sizing for worst-case operations, sharing power between them adds an unacceptable amount of mass in the form of wires [48], and is thus not an option. As such, the only option is to minimize the chance of failure. This will involve managing the MAV batteries' state of charge via an umbilical from the lander and maintaining safe thermal conditions throughout the mission.

4.1.2.2 OS Beacon

The OS's beacon is a relatively simple device that sends a constant tone depending on the phase of the launch. The most likely cause of failure is component or battery

Table 4.1: Proposed MAV Failure Mode, Effects & Criticality Analysis (FMECA)

System	Functional Element	Failure Mode	Most Likely Cause	Local Effect	System Effect	Detection Method	Compensating Provisions	Preventative Measures	Criticality
Avionics	Compute Element	Freeze	SEE Component Failure	No control over MAV guidance or sequencing	Loss of mission	None	None	High-reliability rad-hard processor	6
Telecom	Beacon	No signal transmitted	Component Failure	No signal transmitted	Unable to track MAV during ascent and orbit insertion of OS	Lack of signal	Ground can attempt to detect OS (high-albedo) with cameras	None	4
Power	Battery	Undervoltage	MAV is too cold Waited too long to take off	Loss of power	Loss of mission	None	None	Battery testing under expected thermal conditions, maintain charge from lander before launch	6
GNC	Spin-Up / Spin-Down Motors	Fails to ignite	Component Failure	No rotational thrust from motors	2nd stage unstable Loss of mission	Telemetry	None	Testing under comparable launch conditions	6
Propulsion	Thrust Vector Controller	Stuck	Component Failure	No thrust vector control	1st stage uncontrollable Loss of mission	IMU	None	Testing under comparable launch conditions	6
Thermal	Heaters	Heater Stuck On	Power Switch Component Failure	Excessive heat generation	Excess load on power system Overheating of components	Temp sensors Current sensors	None	Redundant switches	2
		Heater Stuck Off	Component Failure	Loss of heat generation	System drops below allowable temperature	Temp sensors Current sensors	Rely on neighboring heaters	Overlapping heater zones	5
Structures	Stage Separation Mechanism	Uneven release	Component Failure	2nd stage angular procession	OS orbit insertion outside requirements Potential loss of mission	Telemetry	Spin up 2nd stage quickly to minimize angular error	Testing under comparable launch conditions	5
	Motor Casing	Structural Failure	Exceeded expected loads due to launch environment conditions	Motor casing fails	Loss of mission	None	None	Motor static fires under comparable launch conditions	6

failure, as there isn't much else that can impact its operation. Once enabled, the beacon is required to transmit for 25 days, allowing the MRN to determine the OS's orbital parameters for later capture by the CCRS. While a failure here wouldn't directly impact the MAV's mission of launching the OS into orbit around Mars, it would likely have significant impacts on the broader MSR campaign. This is also a notable exception to the battery failure modes discussed above - while an OS battery failure would certainly prevent the OS's beacon from transmitting, this can still be potentially mitigated in the same way as any other beacon failure.

There is a backup plan available, should there be issues determining orbit from the beacon. The OS will be designed with a high albedo (the outer shell will be bright, white, and reflective) so that it can be spotted by the CCRS's cameras to aid in final alignment for capture [34]. This high albedo can potentially enable other members of the MRN to spot the OS and determine its orbit optically. However, this contingency has no guarantee of success and requires significant additional resources to be allocated to the OS recovery effort, so an OS beacon failure significantly degrades the overall mission and is considered to be a criticality level 4 event.

4.1.2.3 Heaters

The MAV has several temperature sensitive components that must be both kept within their survival Allowable Flight Temperature (AFT) range throughout the mission, and slowly brought to their operational AFT shortly before the MAV launch. This requirement is managed through the use of a set of heaters integrated into various zones in the MAV. However, if one of these **heaters** were to get stuck in the **off** state, unable to provide heat most likely due to a component failure, then the connected section of the MAV would risk dropping below its AFT. This can be detected with temperature or current sensors, but currently there are no immediate solutions to such an issue. One potential solution is to increase the temperature of neighboring zones using their still operational heaters, and hope that this is sufficient to keep the MAV alive. However, this isn't guaranteed to work, and could cause the MAV to underperform during launch, making such a failure a level 5 criticality.

In the unlikely event that any of these **heaters** are stuck **on**, there would be excessive heat generation for some components within the MAV and excess load on the power system. Due to the extremely low ambient temperatures, the excess heat is unlikely to be an issue, unless it heats a section so fast as to damage it, though this particular failure mode can be mitigated by limiting the heater's maximum power. The slightly larger concern is the excess power load on the system, as this will limit power available to the remainder of the lander. This may force some operational adjustments to stay within the power budget, but will have relatively limited impact on the mission, and is thus assigned a criticality of 2. Fortunately, due to redundancies in the power supply switching system (as discussed in Section 3.1.2.1), this failure mode is extremely unlikely to occur.

4.1.3 Fault Tree Analysis (FTA)

The representative MAV FTA in Figure 4-2 considers failure modes that could prevent the OS from reaching the intended orbit. This is broken into three broad intermediate events - failure to initiate launch, failure in VECTOR launch of MAV, and Ascent Vehicle failure. As this FTA is made of entirely OR gates, any single event will cause the top level failure condition.

However, that doesn't mean every event causes loss of mission. Any failure to initiate launch that occurs before the point of no return will disrupt that particular launch attempt, but will likely also abort the remainder of the launch and trigger a safe mode state. This will provide ground control an opportunity to hopefully remedy the situation before attempting the launch again.

One failure condition found in this FTA but initially overlooked by the FMECA occurs within the stage separation mechanism. Stage separation errors account for around 22% of all US launch vehicle failures [13], and are of particular concern to the MAV. While a structural failure in the separation mechanism would certainly result in LOM, there are also more nuanced issues found here. In particular, if the release has a large tipoff rate, and thus significant second stage angular procession, the lack of guidance on the second stage could result in significant stage 2 orbital insertion

Figure 4-2: Proposed MAV Fault Tree Analysis (FTA)

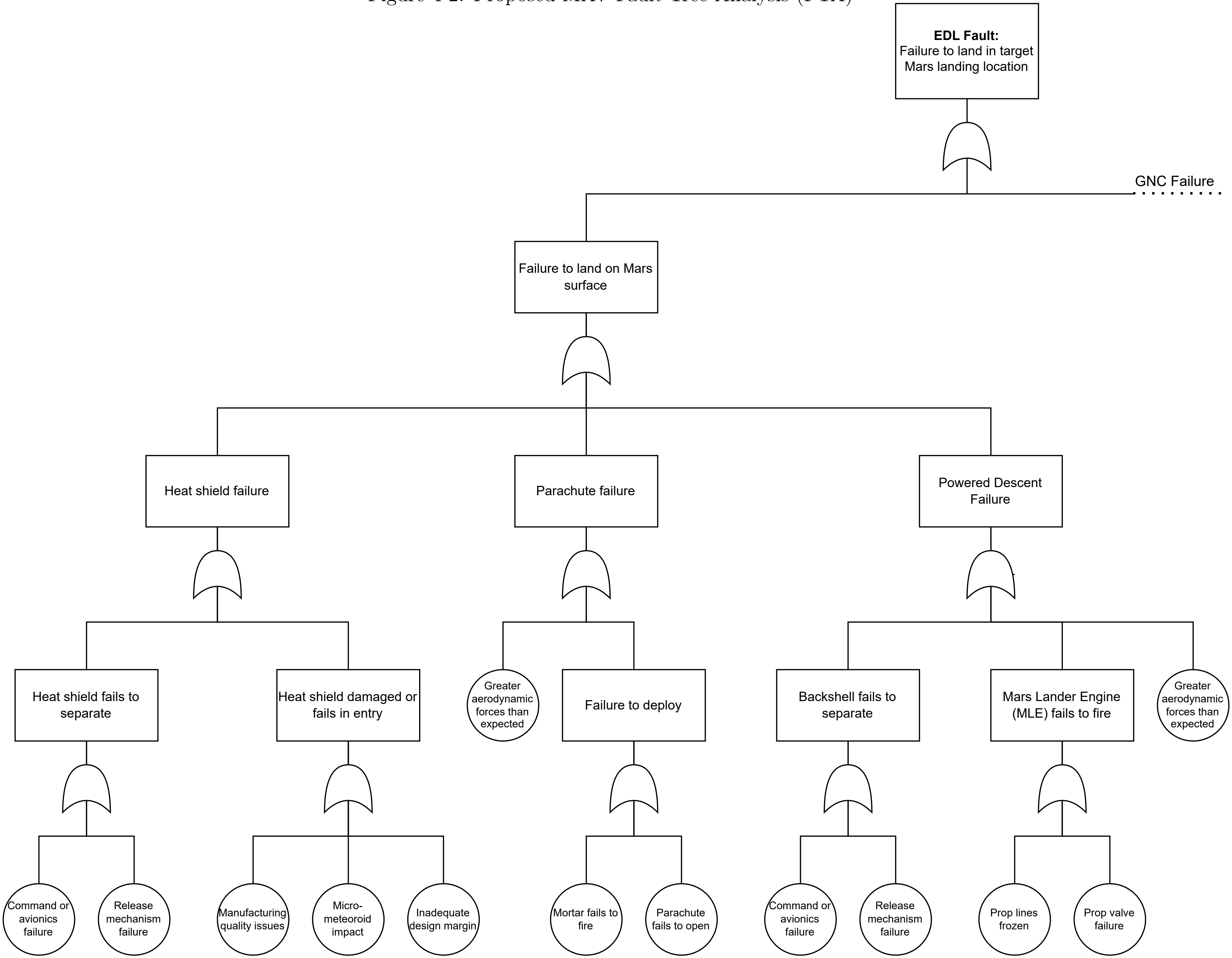
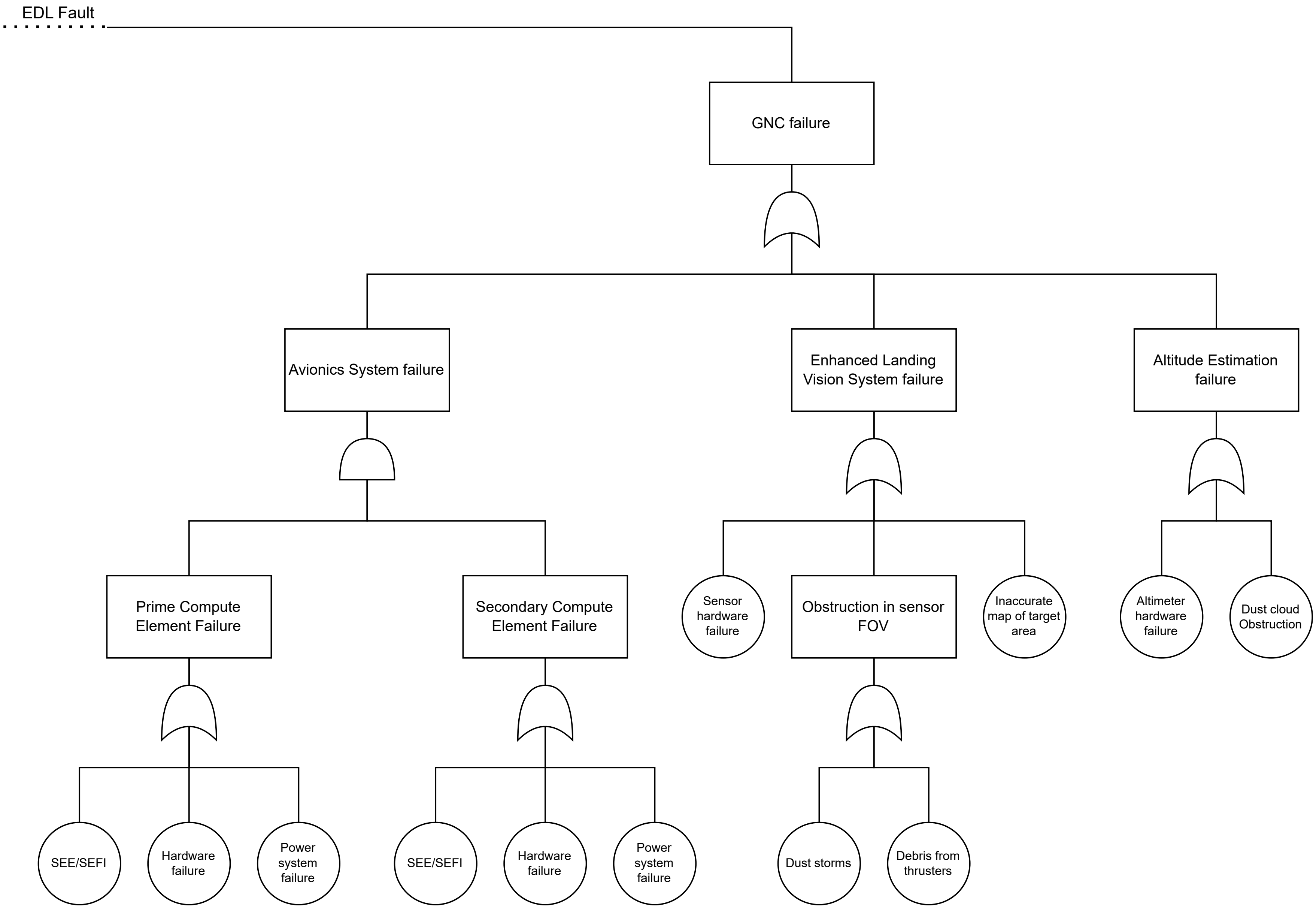

EDL Fault:
Failure to land in target Mars landing location
GNC Failure
Failure to land on Mars surface
Heat shield failure
Parachute failure
Powered Descent Failure
Heat shield fails to separate
Heat shield damaged or fails in entry
Greater aerodynamic forces than expected
Failure to deploy
Backshell fails to separate
Mars Lander Engine (MLE) fails to fire
Greater aerodynamic forces than expected
Command or avionics failure
Release mechanism failure
Manufacturing quality issues
Micro-meteoroid impact
Inadequate design margin
Mortar fails to fire
Parachute fails to open
Command or avionics failure
Release mechanism failure
Prop lines frozen
Prop valve failure

Figure 4-2: (Cont.) Proposed MAV Fault Tree Analysis (FTA)



inaccuracy [3, 48, 49].

4.2 FP Approach to MAV Launch

Any approach to FP for MAV Launch will be constrained by several competing factors. One of the most constraining is the extremely limited mass available for the MAV, as this precludes almost any active FP responses and creates a massive challenge to include any form of redundancy. But there are other constraints also in play, such as the brevity of the launch (approximately 20 minutes from land to final orbit [48]) and general uncertainty in performing a novel launch from Mars. These combine to yield requirements forcing the launch to be autonomous, with no capacity for ground control intervention in the event of any abnormalities. As such, the delivered MAV for launch from Earth must be as thoroughly tested in flight-like conditions as possible to demonstrate likely success.

4.2.1 Pre-MAV Launch

There are many FP options available before the MAV launches. While this phase is generally out of scope for this thesis, it is worth mentioning some of the impact it can have on the MAV.

One of the most critical pre-flight activities is MAV thermal management. The lander will go through several extreme thermal cycles, from the relatively warm Earth prior to the launch to mars, to the cold vacuum of space, brief extreme heat during EDL, and then daily cool to extremely cold and back cycles on Mars. Some of this is mitigated by designing the MAV to handle the cold temperatures on Mars, while the remainder is managed with active heating inside the lander's igloo enclosure. However, the current design has no FP for failures in these heaters. To improve overall reliability, these heaters should be designed with some form of redundancy, either by validating the use of neighboring heaters' overlapping zones as a backup plan, or by directly including redundant heaters within the igloo. As heaters tend to be extremely low mass, this will likely be a low cost method of improving the overall mission reliability and fault tolerance by ensuring the MAV survives at least until it is ready to launch.

There are some additional opportunities for active FP during system checkouts before the launch. In the event of a detected abnormality, FP can intervene and put the entire lander and MAV in a safe state, giving ground control an opportunity to attempt to repair any issues found in the system. Likewise, ground control can choose to delay the launch based on external factors, such as waiting for a Martian dust storm to settle down. This is true up until the point of no return (PoNR) after which neither ground control nor automated FP systems can abort the flight. Once certain systems are activated, such as VECTOR launching the MAV or the thermal battery's ignition, the flight must go on. And it is starting at this point that the remainder of the MAV analysis in this thesis begins.

4.2.2 MAV Design Validation

As there are no FP opportunities after the PoNR, the MAV must be meticulously designed to reduce the risk and impact of faults wherever possible. While the MAV is a relatively simple system (at least as compared to the remainder of the MSR campaign), there are still several challenges to validating the design. Primarily, it is impossible to test in situ, and no one test can perfectly replicate all aspects of the Martian launch environment. Instead, many tests with overlapping sets of varying scope will be used to help ensure comprehensive coverage.

The validation campaign will likely include mechanical tests such as thermal cycling to ensure all components will survive in the igloo, shake tables to simulate vibrations experienced during launch and EDL, software simulation and hardware in the loop testing for electrical components, and even terrestrial test launches. For example, in order to investigate the MAV's second stage flight characteristics and stage separation technique, JPL is planning a sounding rocket based test launch from Wallops Flight Facility to achieve conditions similar to those that will be seen on Mars [3].

Beyond this, there isn't much more that can be done. The reality is that MSR is pushing the limits of modern technology, and the MAV in particular has no room to grow. It is a single-string system that is critical to the overall campaign, and as such the very real chance of failure is a major risk. However, some level of risk must be accepted in order to make the mission possible at all [25]. As in all parts of this campaign, engineers must carefully consider the risk posture when making design trades in order to maximize the likelihood of mission success.

Chapter 5

Summary & Future Work

Mars Sample Return is attempting to retrieve samples of Martian regolith collected by the M2020 Rover and return them to Earth via a rocket launched from the surface of Mars. This unprecedented mission will not only allow for advanced terrestrial analysis of the Martian environment, but will also be an informative baseline for future two-way outer space exploration. SRL's currently proposed EDL and MAV Launch phases are two of the most critical, but also operationally challenging, portions of the mission. Fault protection analyses and techniques are imperative in order to ensure the reliability of each phase and maximize the overall chance of mission success.

5.1 Fault Protection

All engineering decisions come with tradeoffs, including those related to FP. For example, increasing redundancy costs mass, which could be allocated to other objectives such as additional scientific instruments. But without FP, there is a greater chance that a mission will fail and recover no scientific value at all. Tradeoffs involving the allocation of resources, both hardware and budget, to fault protection and prevention can be informed via the FP analysis tools discussed in this thesis.

FMECAs are a useful tool to determine the relative priority, and thus allocation of resources to FP, for all possible faults in a system. As defined in this thesis, FMECAs are first a brainstorming tool to list all possible faults. From there, by thinking about how said faults could occur and what their impacts on the system could be, a criticality score can be assigned, and planned compensating provisions can be enumerated. This forces designers to think about how to compensate for failures in advance, while simultaneously helping guide efforts to focus on the higher priority events. The results of the FMECA can also be utilized for troubleshooting of anomalies. While the FMECA identifies the end response the spacecraft will take, the fault set's list of likely causes coupled with spacecraft telemetry can allow operators to deduce the root cause of anomalies and formulate solutions to mitigate future occurrences.

FTAs are primarily used as a brainstorming tool, to make sure engineers have considered all possible failure cases during the design phase. A good FTA can also be used in the event of a failure to attempt to determine the root cause. By removing branches that are known to have not failed, the FTA will show the paths of the only possible causes of failure. These can be further investigated and pruned until the final root cause is understood.

Generating and analyzing FCRs assists engineers in understanding the failure propagation behavior of a spacecraft. This can be used to assess the effectiveness in the fault containment strategies, and determine the most crucial locations for additional isolation mechanisms and the most effective ways to improve redundancy. However, given that implementing fault containment adds additional complexity to hardware, FCRs also help inform engineers of functional groupings of elements within a spacecraft system – i.e. a sensor is paired to the processor reading it – so that fault containment isn't over-imposed.

5.1.1 Combining F-Tools

Much as the F-Tools can support the engineering process, they also complement each other. FMECAs and FTAs are both failure-oriented brainstorming tools, but they approach the problem from opposite directions. FMECAs attempt to answer the question "what are all of the ways this component can fail?" for every component in the system, and then attempt to reason about the impacts from there. FTAs are instead based on a central failure condition, typically something along the lines of "mission failure". This is then recursively broken down into every possible way that condition can be triggered, until the events described are so basic they cannot be further subdivided. As these are fundamentally different ways of brainstorming, they can often find different sets of failure conditions. In the event of discrepancies between the FMECA and FTA, both can be iteratively updated until a comprehensive set of failure modes is found.

For example, the original MAV FMECA in this thesis didn't consider the stage separation mechanism at all, as structural failures are typically ignored in FMECAs. However, the FTA found a failure case where the stage separation mechanism could release unevenly, causing problems for the unguided 2nd stage. This was then added to the FMECA, to further consider how to compensate or prevent this condition from causing orbital insertion failure. As such, the various FP tools are able to be used in conjunction to formulate a more comprehensive set of faults than each may necessarily identify independently.

5.1.2 MSR FP

As applied to MSR, the F-Tools reveal several similarities and also significant differences between EDL and MAV Launch. Both must be autonomous due to the rapid pace and long distance to Earth, and once started neither can be aborted or delayed. Typical FP systems will revert spacecraft to a safe mode in the event of detected errors, and MSR will likely use this technique during many portions of the campaign. But this is not an option while flying through Mars' atmosphere, and this creates several challenges in designing EDL and MAV to be fault resistant. In the end, all FP responses for these phases must be meticulously pre-planned. In the many cases where no responses are possible, the chance of error can be minimized but the remaining risk of failure must be accepted.

Amongst the differences between EDL and MAV, one of the starkest is the fact that JPL has performed EDL several times before. Effectively detecting faults requires accurate models of the spacecraft and its environment, such that the spacecraft can discern the difference between nominal and off-nominal behavior. As JPL has landed on Mars several times, they have a fairly detailed understanding of EDL, and can effectively test future spacecraft in representative environments. MAV will be much trickier, as it has never been attempted before, and has limited data available on what to expect during the launch. MAV also has much stricter limits on mass budget, and as such has tight margins and no capacity for redundancy.

While most of MAV's FP limitations are the same or more limiting than those discussed for EDL, MAV Launch has one redeeming quality - it can be aborted and reattempted (in some circumstances) *before* the launch is initiated. In contrast, EDL must begin at the instant the lander arrives at Mars, with no ability to delay for any issues that may crop up at the last second.

5.2 Future Opportunities

The F-Tools discussed in this thesis are useful well beyond the current iteration SRL's EDL and MAV Launch. Future missions, the remainder of MSR, even future iterations of EDL and MAV that may be redesigned, will all need to consider FP as a core component of the design effort to maximize reliability without overly compromising other objectives. This applies across the board, from phases with similar fundamental time and mass constraints to those that can be continuously monitored and managed by ground control. The F-Tools will continue to be a useful source of engineering feedback for this purpose.

Beyond the F-Tools, there are several other FP-related tools available to use. Success Trees, the inverse of Fault Trees which analyze everything that must go *right* for mission success, are a viable replacement for FTAs in single-string missions, such as the MAV. It can be easier to reason through a relatively constrained list of everything that must successfully happen than it is to enumerate every possible thing that could go wrong; and doing so is just as useful when prioritizing FP and design efforts.

System-Theoretic Accident Model and Processes (STAMP) framework analyses offer an entirely different perspective on FP. Instead of considering faults from a component failure perspective, STAMP considers that failures can still occur in complex systems despite every individual component operating as designed [28]. A common example of such a failure would be software bugs, where in the vast majority of non-SEE faults, the code runs exactly as it's designed. However, the code may not have covered a particular edge case, and thus fails. In the case of the Hakuto-R Mission 1 Lander, which did not experience a software fault, the lander failed to touchdown after its FSW mistakenly marked its altimeter as sick after detecting a large spike in altitude caused by the lander flying over a crater edge. The lander's parent company, ispace, failed to consider that a change in their landing site, which originally did not contain craters, would have necessitated an updated FP software model [19, 20].

5.3 EDL & MAV FP Opportunities

EDL and MAV Launch both have limited FP opportunities available due to the nature of the event sequences. However, EDL is continued to be developed and optimized for future missions, with greater capabilities added from early Mars landings through the Perseverance rover. The addition of sensor fusion algorithms and "Second Chance" demonstrate a desire to increase reliability and performance for a process with significant past heritage.

While MAV Launch doesn't have the same amount of heritage and experience that EDL can use to draw from, there are opportunities to seek additional reliability within the MAV. While mass is a major concern for the MAV, and consequently the SRL wet mass at Earth launch, additional redundancy should not be immediately turned aside. Critically, given the short duration of the MAV Launch itself, significant focus must be given to maintaining the MAV hardware in good health prior to its Mars launch date for the highest chance of success. For instance, for critical elements like thermal that maintains the propellent grain health of the MAV motors, the benefit of adding redundant heating elements likely exceeds the risk of adding mass due to the small form factor of heater patches. Additionally, it will be worth studying how operationally on Mars, there may be methods of mitigating hardware degradation to single-string components on MAV so as to limit any degradation from the Mars environment prior to launch. As of 2024, the MAV, and SRL as a whole, is undergoing additional industry study requests for formulating a lighter launch vehicle. Certainly, there is much work to be done in evaluating the risk posture of the MAV by NASA managers in comparison to its cost and mass budgets.

Though the MAV will be a small demonstration of an orbital launch from another planet, the MAV will directly contribute to bringing Mars regolith samples back to Earth for analysis into the search for evidence of life in the solar system. MSR itself is listed as a top priority in the 2023 Planetary Science and Astrobiology Decadal Survey, affirming the importance of this sample return. Additionally, the MAV will be an important proving ground for collecting flight dynamics data on Mars and paving the way for future space exploration between Earth and Mars, including the potential transport of resources and eventually people.

Bibliography

[1] Joel Benito, Connor Noyes, Robert Shotwell, Ashley Karp, Barry Nakazono, Gurkirpal Singh, Hunjoo Kim, Mark Schoenenberger, Ashley Korzun, Marcus Lobbia, and Erich Brandeau. Hybrid propulsion Mars Ascent Vehicle concept flight performance analysis. In *2017 IEEE Aerospace Conference*, pages 1–13, 2017. doi:10.1109/AERO.2017.7943964.

[2] Ed Benowitz. The Curiosity Mars Rover's fault protection engine. In *2014 IEEE International Conference on Space Mission Challenges for Information Technology*, pages 62–66, 2014. doi:10.1109/SMC-IT.2014.16.

[3] William W Benson, Michael Fritzinger, Justin Costley, Brian Tibbetts, Brent Edwards, and Tim Kibbey. Mars Ascent Vehicle flight test mission design, analysis, and instrumentation. In *45th Rocky Mountain AAS Guidance, Navigation and Control Conference*, number 23-171 in AAS, 2023.

[4] Aliza Chasan. NASA hears Voyager 2 "heartbeat" after losing communication with spacecraft [online]. Aug 2023. URL: https://www.cbsnews.com/news/nasa-loses-communication-voyager-2-spacecraft-antenna-accident-earth/.

[5] Qi Chen, Zhigang Liu, Xiaofeng Zhang, and Liying Zhu. *Spacecraft Power System Technologies.* Springer, 2020.

[6] John Day and Michel Ingham. Fault management at JPL: Past, present and future. Technical report, Jet Propulsion Laboratory, California Institute of Technology, Oct 2011. URL: https://indico.esa.int/event/62/contributions/2808/attachments/2356/2717/0905_-_fault-management-at-jpl_Presentation.pdf.

[7] Samalis Santini De León, Allen Chen, David W. Way, and Paul Brugarolas. Assessment of the robustness of the Mars 2020 terminal descent sensor in the event of beam failure. In *2020 IEEE Aerospace Conference*, pages 1–10, 2020. doi:10.1109/AERO47225.2020.9172281.

[8] What Is the Decadal Survey? [online]. The Planetary Society. URL: https://www.planetary.org/space-policy/what-is-the-decadal-survey [cited 2023-08-30].

[9] Department Of Defense, MIL-STD-1553. *DIGITAL TIME DIVISION COMMAND/RESPONSE MULTIPLEX DATA BUS*, 2018.

[10] Gregory F. Dubos, Mallory Lefland, Magdy Bareh, and Keith Comeaux. Single event functional interrupts during the cruise and edl phases of the mars 2020 mission. In *2022 IEEE Aerospace Conference (AERO)*, pages 13–25, 2022. doi:10.1109/AERO53065.2022.9843756.

[11] Roland J Duphily and Air Force Space Command. Space vehicle failure modes, effects, and criticality analysis (fmeca) guide. *Space Missile Syst. Center, El Segundo, CA, USA, Aerosp. Rep. No. TOR-2009 (8591)-13*, 2009. URL: `https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/TOR2009-8591-13.pdf`.

[12] Jeff Foust. NASA to look for new options to carry out Mars Sample Return program [online]. April 2024. URL: `https://spacenews.com/nasa-to-look-for-new-options-to-carry-out-mars-sample-return-program/` [cited 2024-05-01].

[13] Susie Go, Scott L Lawrence, Donovan L Mathias, and Ryann Powell. Mission success of us launch vehicle flights from a propulsion stage-based perspective: 1980-2015. Technical report, NASA, 2017. URL: `https://ntrs.nasa.gov/citations/20170009844`.

[14] B. E. Goldberg, K. Everhart, R. Stevens, N. Babbitt, P. Clemens, and L. Stout. System engineering "toolbox" for design-oriented engineers. NASA Reference Publication 1358, NASA, 1994.

[15] Jeff Gramling, Michael Meyer, and Richard Cook. Space studies board Mars Sample Return (msr) [online]. June 2023. URL: `https://www.nationalacademies.org/documents/embed/link/LF2255DA3DD1C41C0A42D3BEF0989ACAECE3053A6A9B/file/D22CACD7F23488540A73C493389C7257D440500FC0C7` [cited 2024-05-01].

[16] Jeffrey Gramling and Michael Meyer. Mars Sample Return. Technical report, NASA Committee on Astrobiology and Planetary Sciences, Irvine, CA, September 2022. URL: `https://ntrs.nasa.gov/citations/20220014347`.

[17] Project Reliability Group. Jet Propulsion Laboratory reliability analyses handbook. Technical report, JPL, July 1990.

[18] Pamela Hoffman, Tomasso Rivillini, Eric Slimko, Neilesh Dahya, Anthony Agajanian, Jennifer Knight, Anita Sengupta, Benjamin Thoma, Richard Webster, John Gallon, and Michael Gradziel. Preliminary design of the cruise, entry, descent, and landing mechanical subsystem for MSL. In *2007 IEEE Aerospace Conference*, pages 1–18, 2007. `doi:10.1109/AERO.2007.352826`.

[19] ispace announces results of the HAKUTO-R mission 1 lunar landing [online]. May 2023. URL: `https://ispace-inc.com/news-en/?p=4691` [cited 2023-09-04].

[20] Status update on ispace HAKUTO-R mission 1 lunar lander [online]. April 2023. URL: `https://ispace-inc.com/news-en/?p=4655` [cited 2023-09-04].

[21] Andrew E. Johnson, Yang Cheng, Nikolas Trawny, James F. Montgomery, Steven Schroeder, Johnny Chang, Daniel Clouse, Seth Aaron, and Swati Mohan. Implementation of a map relative localization system for planetary land-

ing. *Journal of Guidance, Control, and Dynamics*, 46(4):618–637, 2023. doi:10.2514/1.G006780.

[22] 7 minutes to Mars: NASA's Perseverance rover attempts most dangerous landing yet [online]. URL: https://www.jpl.nasa.gov/videos/7-minutes-to-mars-nasas-perseverance-rover-attempts-most-dangerous-landing-yet [cited 2024-05-04].

[23] JPL. Mars 2020: Perseverance rover [online]. URL: https://www.jpl.nasa.gov/missions/mars-2020-perseverance-rover/ [cited 2024-05-01].

[24] JPL. Fault protection: Lesson learned #772. Technical report, NASA, February 1999. URL: https://llis.nasa.gov/lesson/772.

[25] JPL. Mitigating the risk of single string spacecraft architecture. Technical report, NASA, April 2006. URL: https://llis.nasa.gov/lesson/1743.

[26] Richard P. Kornfeld, Ravi Prakash, Ann S. Devereaux, Martin E. Greco, Corey C. Harmon, and Devin M. Kipp. Verification and validation of the Mars Science Laboratory/Curiosity rover entry, descent, and landing system. *Journal of Spacecraft and Rockets*, 51(4):1251–1269, 2014. doi:10.2514/1.A32680.

[27] Mallory Lefland and Aaron Stehura. Mars 2020 entry, descent, and landing system software implementation. In *2022 IEEE Aerospace Conference (AERO)*, pages 1–13, 2022. doi:10.1109/AERO53065.2022.9843575.

[28] Nancy Leveson, Mirna Daouk, Nicolas Dulac, and Karen Marais. Applying STAMP in accident analysis. In *NASA Conference Publication*, pages 177–198. NASA; 1998, 2003.

[29] Landano Matthew. Design, verification/validation and operations principles for flight systems. JPL Guideline D-17868, JPL, 2001.

[30] Richard Mattingly and Lisa May. Mars Sample Return as a campaign. In *2011 Aerospace Conference*, pages 1–13, 2011. doi:10.1109/AERO.2011.5747287.

[31] M McHenry, N Abcouwer, J Biesiadecki, J Chang, TD Sesto, A Johnson, T Litwin, M Maimone, J Morrison, R Rieber, et al. Mars 2020 autonomous rover navigation. *AAS*, 2020.

[32] Heather Monaghan. What is the deep space network? [online]. March 2020. URL: https://www.nasa.gov/directorates/somd/space-communications-navigation-program/what-is-the-deep-space-network/ [cited 2024-05-01].

[33] Brian Muirhead, Austin Nicholas, Chad Edwards, Jeffrey Umland, Sanjay Vijendran, and Richard Zurek. Mars sample return campaign concept architecture. *Bulletin of the AAS*, 53, 03 2021. doi:10.3847/25c2cfeb.a57d10a4.

[34] Brian Muirhead, Austin K Nicholas, Chad Edwards, Jeffrey Umland, Sanjay Vijendran, and Richard Zurek. Mars Sample Return campaign concept architecture. *Bulletin of the American Astronomical Society*, 53(4):311, 2021.

[35] Cruise configuration - NASA Mars [online]. URL: `https://mars.nasa.gov/mer/mission/spacecraft/cruise-configuration/` [cited 2023-09-04].

[36] Mars Sample Return program update (april 15, 2024) [online]. April 2024. URL: `https://www.youtube.com/watch?v=5PA1qhzkSlA` [cited 2024-05-01].

[37] Mars Sample Return [online]. URL: `https://mars.nasa.gov/msr/` [cited 2023-09-04].

[38] Mars Sample Return: Sample Retrieval Lander [online]. URL: `https://science.nasa.gov/mission/mars-sample-return/sample-retrieval-lander/` [cited 2024-05-01].

[39] Adam Nelessen, Chloe Sackier, Ian Clark, Paul Brugarolas, Gregorio Villar, Allen Chen, Aaron Stehura, Richard Otero, Erisa Stilley, David Way, Karl Edquist, Swati Mohan, Cj Giovingo, and Mallory Lefland. Mars 2020 entry, descent, and landing system overview. In *2019 IEEE Aerospace Conference*, pages 1–20, 2019. `doi:10.1109/AERO.2019.8742167`.

[40] Eugene Normand. Single-event effects in avionics. *IEEE Transactions on nuclear science*, 43(2):461–474, 1996.

[41] Ravi Prakash, P. Dan Burkhart, Allen Chen, Keith A. Comeaux, Carl S. Guernsey, Devin M. Kipp, Leila V. Lorenzoni, Gavin F. Mendeck, Richard W. Powell, Tommaso P. Rivellini, A. Miguel San Martin, Steven W. Sell, Adam D. Steltzner, and David W. Way. Mars Science Laboratory entry, descent, and landing system overview. In *2008 IEEE Aerospace Conference*, pages 1–18, 2008. `doi:10.1109/AERO.2008.4526283`.

[42] H. Price, K. Cramer, S. Doudrick, W. Lee, J. Matijevic, S. Weinstein, T. Lam-Trong, O. Marsal, and R. Mitcheltree. Mars sample return spacecraft systems architecture. In *2000 IEEE Aerospace Conference. Proceedings (Cat. No.00TH8484)*, volume 7, pages 357–375 vol.7, 2000. `doi:10.1109/AERO.2000.879302`.

[43] Arturo Rankin, Mark Maimone, Jeffrey Biesiadecki, Nikunj Patel, Dan Levine, and Olivier Toupet. Driving Curiosity: Mars rover mobility trends during the first seven years. In *2020 IEEE Aerospace Conference*, pages 1–19, 2020. `doi:10.1109/AERO47225.2020.9172469`.

[44] MSL – EDL communications overview [online]. URL: `https://spaceflight101.com/msl/msl-edl-communications` [cited 2024-05-01].

[45] A. Steltzner, D. Kipp, A. Chen, D. Burkhart, C. Guernsey, G. Mendeck, R. Mitcheltree, R. Powell, T. Rivellini, M. San Martin, and D. Way. Mars Science Laboratory entry, descent, and landing system. In *2006 IEEE Aerospace Conference*, pages 15 pp.–, 2006. doi:10.1109/AERO.2006.1655796.

[46] David Stephenson. Mars Ascent Vehicle - concept development. *38th AIAA/ASME/SAE/ASEE Joint Propulsion Conference &amp; Exhibit*, 2002. doi:10.2514/6.2002-4318.

[47] Nikolas Trawny, Andrew E. Johnson, Erik S. Bailey, Gabrielle Massone, Mark Reid, Timothy P. Setterfield, Yang Cheng, Glenn Sellar, and Jose Soto. The enhanced lander vision system for Mars sample retrieval lander entry descent and landing. *AIAA SCITECH 2024 Forum*, 2024. URL: https://arc.aiaa.org/doi/abs/10.2514/6.2024-0314, doi:10.2514/6.2024-0314.

[48] Darius Yaghoubi and Shawn Maynor. Integrated Design Results for the MSR SRC Mars Ascent Vehicle. In *2022 IEEE Aerospace Conference (AERO)*, pages 1–20, 2022. doi:10.1109/AERO53065.2022.9843749.

[49] Darius F Yaghoubi. Emerging technologies for Mars exploration: Mars ascent vehicle. In *AIAA Next Gen Technical Symposium, Pre-Event Tech Talk*, 2020.