Integrating Reliability Engineering with Fault Management to Create Resilient Space Systems

Melissa R. Jones, Kristin A. Fretz, Sanae D. Kubota, and Clayton A. Smith

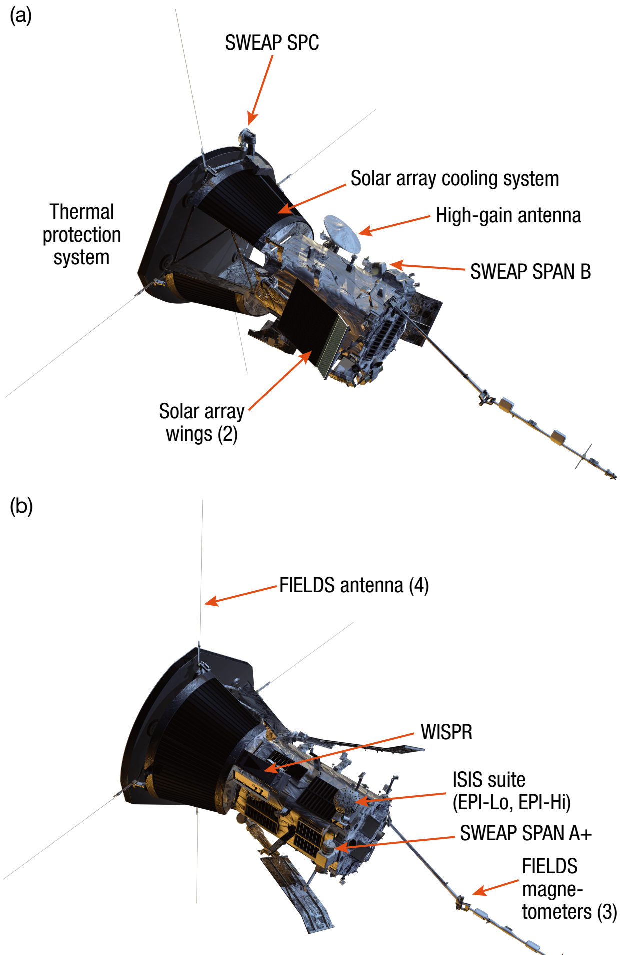
ABSTRACT

The NASA/Johns Hopkins University Applied Physics Laboratory (APL) Parker Solar Probe mission is the first human-built spacecraft to touch the Sun. It launched in August 2018 and began its first solar encounter on 31 October 2018. Parker Solar Probe's instruments analyze the environment inside the Sun's corona as the spacecraft autonomously protects itself from the extreme environment. Because the spacecraft will be unable to contact the ground during many of its encounters, it has to be resilient enough to autonomously detect and correct any issues, such as pointing errors or computer glitches, that might arise. The fault management subsystem is defined as the functional requirements distributed throughout the observatory and ground elements that enable detection, isolation, and recovery from events that upset nominal operations. An expanded failure modes and effects analysis provided input that improved the fault management team's ability to determine failures of concern and to group responses by failure effect. This partnership between the Parker Solar Probe reliability and fault management teams contributed to an observatory that has now repeatedly withstood the rigors of flying through the Sun's corona, proving the resilience of the system.

INTRODUCTION

The space environment is harsh, no matter where a spacecraft travels in it. It features fast-moving debris, charged particles, radiation, extreme heat, extreme cold, and more. When a spacecraft is literally flying through the Sun, and out of communication with Earth while doing so, it needs to not only withstand the environment but also do so on its own and return useful science data back to Earth. This resilience was built into Parker Solar Probe (PSP) with robust design practices and redundancy and through the integration of the reliability and fault management analysis products.

The NASA/APL PSP mission will revolutionize our understanding of the Sun by swooping to within 4 million miles of the Sun's surface. This mission targets the fundamental processes and dynamics that characterize the Sun's corona and outwardly expanding solar wind; additionally, it will be the first mission to fly into the low solar corona (i.e., the Sun's atmosphere), revealing both how the corona is heated and how the solar wind is accelerated. PSP (Fig. 1) faced many engineering challenges because of the intense environment it will encounter in terms of heat and solar radiation, as well as the reaction time required to "safe" the spacecraft. The fault management system is highly autonomous and designed to manage the complex system's robustness as well as fault detection and response in a timely manner. The fault management design relied heavily on the failure modes and effects analysis (FMEA), which uses a systematic approach to determine the effects of each potential failure mode on a particular component/system, the spacecraft, and the mission. Once the potential effects are determined, each failure mode is assigned a severity level commensurate with the potential effects. For the PSP mission, the spacecraft functional FMEA was expanded to include information about whether a failure mode would be detectable by the spacecraft or personnel on the ground, the time frame for detection, and which mitigations, if any, were available to the mission team. The fault management team then used the FMEA to ensure that all faults had been captured, to identify which faults could be detected by the spacecraft, and to build appropriate responses for the spacecraft to take during the mission.


(a)
SWEAP SPC
Solar array cooling system
High-gain antenna
Thermal protection system
SWEAP SPAN B
Solar array wings (2)
(b)
FIELDS antenna (4)
WISPR
ISIS suite (EPI-Lo, EPI-Hi)
SWEAP SPAN A+
FIELDS magne-tometers (3)

FIELDS	Fields Experiment, consisting of five electric field antennae and three magnetometers
ISIS	Integrated Science Investigation of the Sun instrument suite consisting of the Energetic Particle Instruments (EPI-Lo and EPI-Hi)
SWEAP	Solar Wind Electrons, Alphas, and Protons Investigation consisting of the SPC (Solar Probe Cup) and SPAN Solar Probe Analyzers) sensors
WISPR	Wide-field Imager for Solar Probe

Figure 1. PSP observatory shown from the side that is opposite the direction of travel (a) and from the side that is in the direction of travel (b). (The thermal protection system always faces toward the Sun). Also shown are major spacecraft bus components and all the instruments/instrument suites.

MISSION OVERVIEW[1]

The PSP mission is part of NASA's Living With a Star Program managed by Goddard Space Flight Center. The mission science objectives are as follows:

- Determine the structure and dynamics of the magnetic fields at the sources of the fast and slow solar wind.
- Trace the flow of energy that heats the solar corona and accelerates the solar wind.
- Determine what mechanisms accelerate and transport energetic particles.

The PSP mission launched in August 2018, targeting an orbit nearly in the ecliptic plane at the start of the mission and then making many near-Sun passes at increasingly lower perihelia. The baseline mission of 7 years provides for 24 perihelion passes inside 0.16 AU [equivalent to 35.7 solar radii (R_S)], with 19 passes occurring within 20 R_S of the Sun (see Fig. 2). The first near-Sun pass began 3 months after launch, at a heliocentric distance of 35.7 R_S. Over the next several years, successive Venus gravity-assist maneuvers will gradually lower the perihelion to 8.86 R_S, by far the closest that any space-

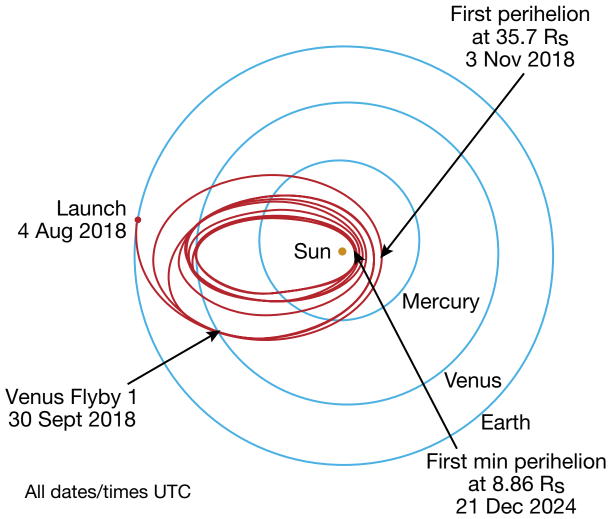

First perihelion at 35.7 Rs 3 Nov 2018
Launch 4 Aug 2018
Sun
Mercury
Venus Flyby 1 30 Sept 2018
Venus
Earth
All dates/times UTC
First min perihelion at 8.86 Rs 21 Dec 2024

Figure 2. PSP mission design overview showing the orbit of the observatory over the course of the mission. Each solar encounter will break all existing records for the closest that a human-made object has approached the Sun while continuing to operate.

craft has ever come to the Sun. PSP will complete its mission with three passes around the Sun at 8.86 R_S (Ref. 2).

The PSP mission is categorized as risk classification B per NPR 8705.4, *Risk Classification for NASA Payloads.*[3] Class B missions are typically fully redundant in their essential spacecraft functions and key instrument measurements. Also, critical single-point failures corresponding to top-level mission requirements are minimized and mitigated with high-reliability parts and dedicated testing in class B missions. These are all approved at the project level.

The unique mission and engineering challenges presented by the intense environment and risk classification necessitate a resilient system. The fault management design provides a means to recover to an operational state, enabling the observatory to collect baseline science measurements inside 0.25 AU.

FAULT MANAGEMENT OVERVIEW[4]

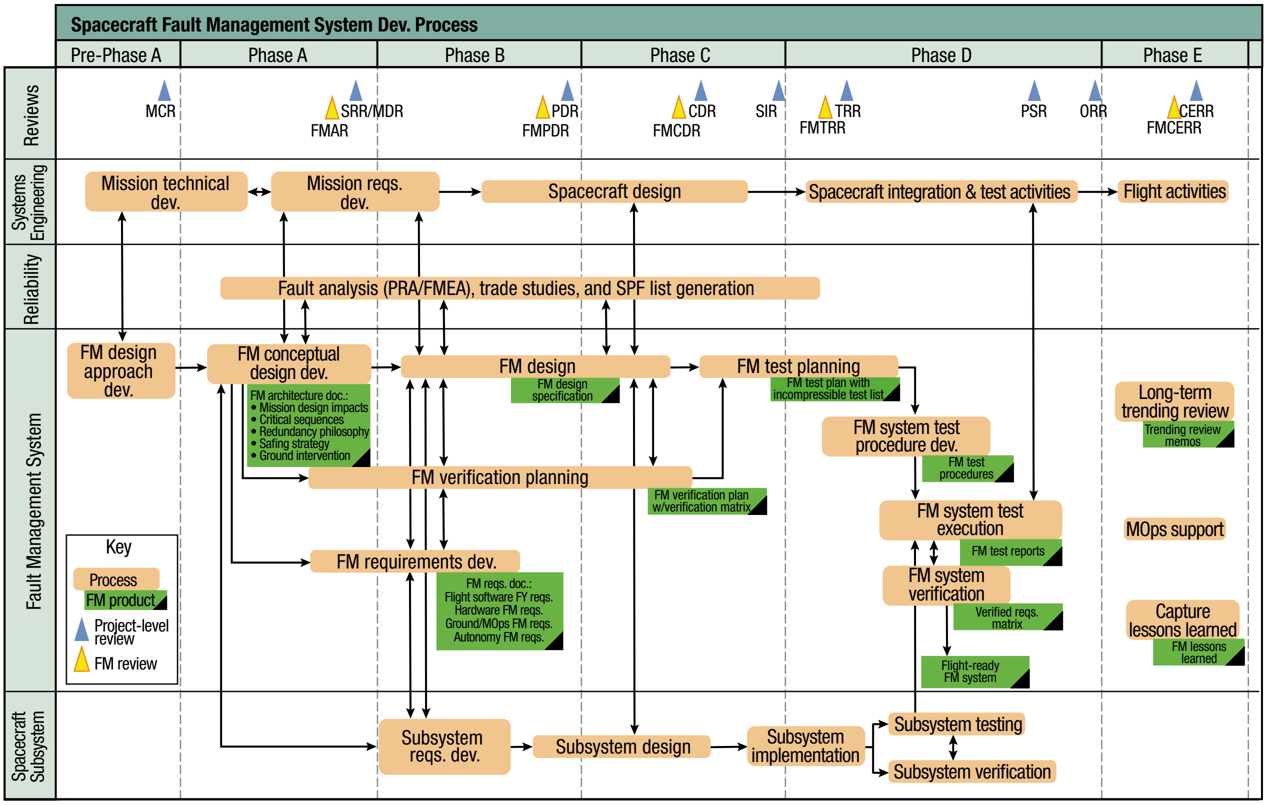
Fault Management Definition/Objectives

Fault management is defined as the functional requirements distributed throughout the observatory and ground elements that enable detection, isolation, and recovery from events that upset nominal operations. The goal of the fault management system is to achieve mission reliability objectives within program resources. Fault management must achieve this goal by balancing project risk and the cost of developing, testing, and operating the fault management system.

Fault Management Process

PSP follows the fault management engineering process documented as a part of the APL Quality Management System. The fault management engineering process is a systematic approach to fault management, with collaboration among systems engineering team members (which includes reliability engineering), subsystem leads, and mission operations team members from phase A through phase E. Figure 3 depicts the high-level engineering process used in the development of the PSP fault management system.

The PSP fault management architecture design is driven by mission requirements for system robustness and fault detection and response. Capturing and understanding key mission design requirements is critical to



CDR	Critical Design Review	FMAR	Fault Management Analysis Review	ORR	Operational Readiness Review	SIR	System Integration Review
CERR	Critical Events Readiness Review	FY	Fiscal Year	PDR	Preliminary Design Review	SRR	System Requirements Review
Dev.	Development	MCR	Mission Concept Review	PRA	Probabilistic Risk Assessment	SPF	Space Power Facility
Doc.	Document	MDR	Mission Definition Review	PSR	Program Status Review	TRR	Test Readiness Review
FM	Fault Management	MOps	Mission Operations	Reqs.	Requirements		

Figure 3. APL fault management engineering process during a mission's design and operational life cycle.

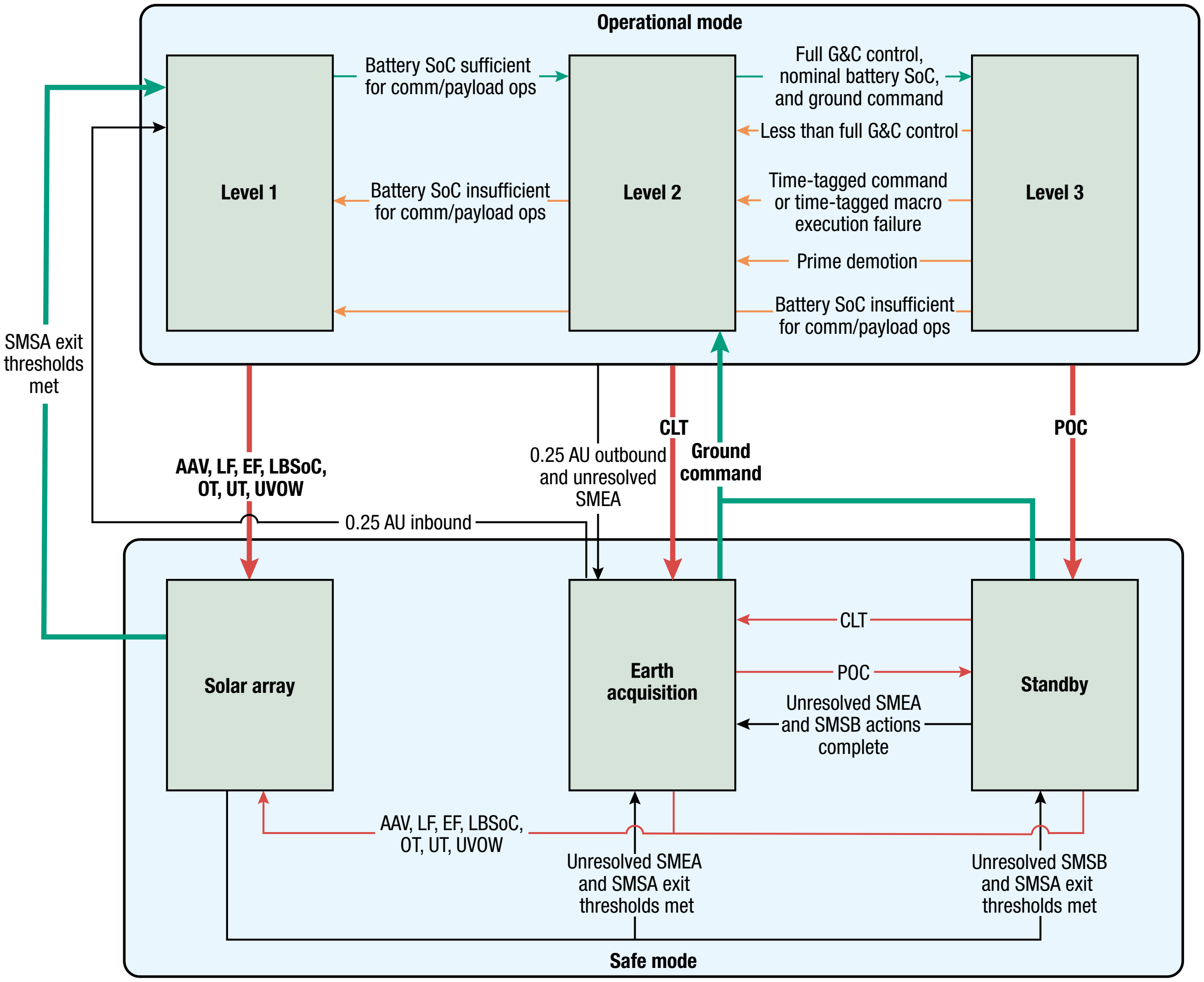
successfully developing the fault management system because it focuses the engineering team on the unique challenges of the mission. The PSP fault management architecture also focuses on redundancy management, the modes and safing concept, the ground intervention concept, and critical sequences, as guided by the fault management engineering process.

Reliability analyses play an important role in the development of the fault management system by identifying potential faults and failures and analyzing the impact of cross-cutting faults and failures on the planned protection schemes in a comprehensive framework. The reliability analyses are used in an iterative manner to ensure that the quantity and impact of potential faults are minimized and that the fault management design is complete, as well as to enable system efficiency in design and fault response.

PSP Fault Management Design

The PSP mission design accommodates at least three orbits with a minimum perihelion distance of less than 10 R_s from the center of the Sun. The following key requirements drive the fault management design:

- The mission shall ensure that the observatory is protected from the Sun at solar distances less than 0.7 AU (with the exception of the thermal protection system, solar array wings, solar limb sensors, FIELDS instrument electrical field antennae, and SWEAP instrument solar particle cup).


Operational mode
Level 1
Battery SoC sufficient for comm/payload ops
Level 2
Full G&C control, nominal battery SoC, and ground command
Level 3
Less than full G&C control
Battery SoC insufficient for comm/payload ops
Time-tagged command or time-tagged macro execution failure
Prime demotion
Battery SoC insufficient for comm/payload ops
SMSA exit thresholds met
AAV, LF, EF, LBSoC, OT, UT, UVOW
0.25 AU inbound
0.25 AU outbound and unresolved SMEA
CLT
Ground command
POC
Solar array
Earth acquisition
Standby
CLT
POC
Unresolved SMEA and SMSB actions complete
AAV, LF, EF, LBSoC, OT, UT, UVOW
Unresolved SMEA and SMSA exit thresholds met
Unresolved SMSB and SMSA exit thresholds met
Safe mode

AAV	Aphelion attitude violation	G&C	Guidance and control	OT	Over temperature	SMSB	Safe mode—standby
CLT	Command loss timer	LBSoC	Low battery state of charge	POC	Processor overcycling	SoC	State of charge
Comm	Communications	LF	Low flux	SMEA	Safe mode—Earth acquisition	UT	Under temperature
EF	Excessive flux	Ops	Operations	SMSA	Safe mode—solar array	UVOW	Umbra violation: orange warning

Figure 4. PSP spacecraft modes: this multitiered approach to fault management allows the spacecraft to continue taking measurements during a solar encounter when local faults have occurred and keeps the observatory safe until it can communicate with the ground in the case of a critical fault condition. The resilient spacecraft autonomously transitions from one level or mode to another.

- The mission shall be designed such that the observatory is capable of autonomously detecting and safing itself in response to a critical fault.
- The mission shall provide a means to recover to an operational state from critical faults.

As a result, PSP is a redundant observatory designed to maintain continuity of attitude, solar array wing angle, and cooling system control and to have a strong autonomous fault detection and response system. The fault management design provides a means to recover to an operational state, enabling the observatory to collect baseline science measurements inside 0.25 AU.

PSP fault management uses a layered approach to protect the mission, with faults categorized by severity and responses executed at two redundant levels. Two spacecraft modes are used by the PSP fault management system: (*i*) operational and (*ii*) safe. PSP implements three operational levels within the operational mode and three separate safe modes, as shown in Fig. 4. These spacecraft modes define groupings of observatory functions and states to facilitate design and spacecraft operations. The spacecraft modes also provide a common vocabulary and simplify communications between operations and the design teams. Finally, the definition of modes provides a structured framework for developing flight software, autonomy rules, and operational procedures.

Faults that are identified and isolated to a particular subsystem are referred to as local faults. The fault management system is designed to implement a simple process with minimized impact to the observatory in response to local faults; for these, the observatory remains in operational mode. All subsystems are required to supply sufficient housekeeping telemetry to allow for detection of faults.

Critical scenarios are planned mission events (critical sequences) or unanticipated faults that create conditions that require a timely response to preserve the mission (critical faults). Critical sequences are sequences of events that must be executed within a specified time to ensure mission success. Critical faults are persistent, are not identified in advance or diagnosed in flight, could be attributed to one or more subsystems, and pose an immediate risk to mission success. They create a condition in which there is a time-critical threat to spacecraft thermal, power, communication, or command and data handling (C&DH) capability.

PSP has one critical sequence, the post-separation sequence, that is critical to prevent a low battery state of charge and includes the following: separation detection, guidance and control/propulsion/telecom activation, nulling tip-off rates, solar array release, slew to radiators 1 and 4 warm-up attitude, solar array deploy to warm-up angles, initial cooling system activation, and slew to aphelion pointing for battery recharge.

PSP has nine critical fault conditions. These conditions are grouped according to the safe mode type in which they would result.

- Power and thermal critical fault conditions that result in demotion to safe mode—solar array include the following:
  - Aphelion attitude violation
  - Umbra violation: orange warning
  - Under temperature
  - Over temperature
  - Low flux
  - Excessive flux
  - Low battery state of charge
- The C&DH critical fault condition of processor overcycling results in demotion to safe mode—standby.
- The communication critical fault condition of an expired command loss timer results in demotion to safe mode—Earth acquisition.

FAILURE MODES AND EFFECTS ANALYSIS

The FMEA is a systematic approach for identifying potential failures in a system, where “failure modes” refers to the ways in which something might fail and “effects analysis” refers to studying the consequences of those failures. MIL-STD-1629A[5] is used as a guide to establish the set of questions asked in a typical FMEA.

Benefits of the FMEA

The FMEA process can provide many benefits to a design program. It can be used to analyze both hardware and software failures, and it provides a basis for identifying root causes of failure and developing effective corrective actions. It can be used in the discovery of single points of failure within a system. It facilitates investigation of design alternatives at all stages of the design. It can provide input to or verification/validation of other analyses such as a probabilistic risk assessment.

Limitations of the FMEA

An FMEA has a limited scope in that only a single item (function, box, component, piece part, etc.) is typically analyzed at a time. This makes the analysis blind to failures that happen in combination, either through a common cause or through independent means. The FMEA also only looks at failures through a “worst-case” lens. As each item is traced through each potential failure mode and the effects that failure might have on the item, the local system, and the mission, each time the worst-case effect is considered. This can some-times be off-putting to the design engineers, but it is a worthwhile exercise.

PSP FMEA

For the PSP mission, an additional question was asked in this base set of questions: Is there an effect that can lead to umbra violation (i.e., impingement of direct solar radiation on the unprotected portions of the spacecraft)? How? Figure 5 describes the columns in the PSP base FMEA. The severity categories used are described in Table 1.

A Microsoft Excel spreadsheet was used to capture the PSP FMEA. Each subsystem and instrument had its own worksheet that followed the basic format described above. In addition, the ground system and selected portions of the ground support equipment were analyzed, although those portions did not include the expanded FMEA sections.

FMEA ID	Name	Function	Failure Mode/Limit/ Constraint	Possible Causes	Phase	Effect				Severity
						Local	Next Higher	Mission	Umbra Violation	

FMEA ID	Unique ID for each failure mode
Name	Hardware or software element name
Function	Function the element performs
Failure Mode/ Limit/Constraint	Specific failure mode (i.e., sensor failure, software error, electronic part failure)
Possible Causes	Credible causes for failure (e.g., radiation upset on field-programmable gate array)
Phase	Operational phase (launch, commissioning, cruise, encounter)
Effects	Effects of the failures at various levels
Local	Effect on the failed element
Next Higher	Effect of failed element on subsystem/instrument
Mission	Effect of failed element on mission
Umbra Violation	Is there an effect that can lead to umbra violation? How?
Severity	Rating of severity should failure occur

Figure 5. Standard FMEA template that has been modified for PSP's unique mission circumstances. This base FMEA is described in MIL-STD-1629A.

USE OF AN EXPANDED FMEA FOR PSP[6]

A three-step iterative fault analysis and response planning process was used in developing the PSP fault management system. First, the FMEA was used to identify failure modes and analyze their effects. The FMEA was then expanded and used for preliminary response planning. Second, a top-down analysis called the effects and failure mode analysis was performed from the effects to examine completeness in the list of causes, and the response plans were further developed. Third, the response plans were shaped based on the symptoms expected to be available in telemetry. These were then linked with lower-level hardware and software requirements to achieve the planned response and linked back to each FMEA line item to ensure completeness.

Expanded FMEA

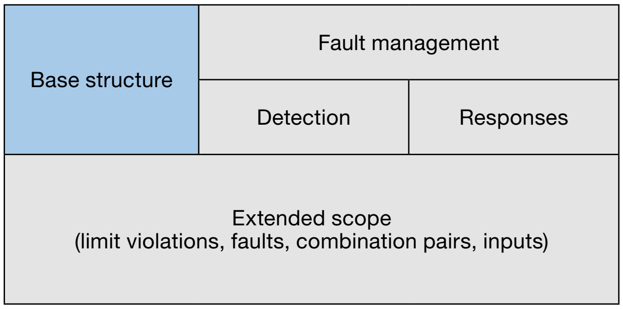
For the PSP mission, the FMEA was expanded in several ways. Columns were added that primarily addressed questions pertinent to the design of the fault management subsystem. These included questions pertaining to the detection of failures/faults and to the responses to

Table 1. Severity categories

Category	Severity	Description
1	Catastrophic	Failure modes that could result in serious injury, loss of life, or loss of spacecraft
1R		Failure modes of identical or equivalent redundant hardware or software elements that could result in category 1 effects if all failed
1S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to category 1 consequences
2	Critical	Failure modes that could result in loss of three or more mission objectives
2R		Failure modes of identical or equivalent redundant hardware or software that could result in category 2 effects if all failed
2S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to category 2 consequences
3	Significant	Failure modes that could cause loss to any mission objectives
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

those failures/faults (either by engineers/operators on the ground or through the spacecraft's autonomous systems).

Additionally, the scope of the analysis was extended in that the analysts also looked at what would occur if an item failed to receive its expected inputs (e.g., power, timing pulse, information from another component/system, etc.). In very limited cases, the analysts also examined the effects to the system if two components failed in combination. Figure 6 shows the expanded FMEA structure. The questions asked in the detection portion of the extended FMEA are described in Fig. 7.



Base structure

Fault management

Detection

Responses

Extended scope
(limit violations, faults, combination pairs, inputs)

Figure 6. PSP expanded FMEA structure.

Each item in the FMEA was analyzed to determine whether that particular failure mode or fault was managed. If the fault management subsystem was specifically monitoring for that exact failure mode, then it was considered active. If the failure mode could be detected but was not specifically being monitored for, it was considered passive, and in some cases, there was no management and the risk was accepted. Then the design team was asked whether the fault in question could be observed at all, and if so, how. After determining which system would detect the observable faults, the exact telemetry necessary for observation was determined along with the telemetry path and the time it would take to detect that particular failure or fault.

Next, the design team looked at what the responses would be given the detected faults that had been identified. The questions asked in the response section of the expanded FMEA are described in Fig. 8.

For each FMEA line item, the response level was determined—whether the response would be at the local (component) level or at the system (or instrument) level. In some cases, there was no response avail-

Type of Fault Management	Detection					
	Observable	How Observed?	Telemetry for Diagnosis	Telemetry Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)

Type of Fault Management	Active, passive, none
Observable	Yes/no
How Observed?	How is the fault observed (narrative)? Who observes the fault (hardware, flight software, autonomy, ground)?
Telemetry for Diagnosis	Telemetry needed for diagnosis of fault
Telemetry Path for Diagnosis	Where does the telemetry come from? Who is it sent to/through?
Time to Detect (Local)	Time to detect locally
Time to Detect (System)	Time to detect at system level

Figure 7. PSP expanded FMEA detection legend. These cells captured whether a fault could be detected and, if so, how and how quickly.

Response									
Response Level	Desired Local Response	Allocation of Local Response	Time to Fix Locally	Time to Transmit Signal	Desired Spacecraft Response	Allocation of System Response	Time to Fix System	Time to Transmit Signal	Ground Response/ Contingency

Response Level	Local, system, instrument, or, none
Desired Local Response	Narrative description of desired action taken locally at subsystem/instrument level
Allocation of Local Response	Who responds locally? Hardware, flight software, autonomy, ground
Time to Transmit Signal	How long does it take before local response begins?
Time to Fix Locally	Time to fix for local response
Desired Spacecraft Response	Narrative description of desired action taken at system level
Allocation of Spacecraft Response	Who responds locally? Hardware, flight software, autonomy, ground
Time to Transmit Signal	How long does it take before system response begins?
Time to Fix System	Time to fix for system response
Ground Response/ Contingency	Ground response needed (narrative); ideas for steps in contingency plans

Figure 8. PSP expanded FMEA response legend. These cells captured how the observatory would respond to a fault (via subsystem response, fault management response, or if the ground would need to be involved) and how long it would take for the response to occur. This section also provided a mechanism for the subsystem design leads to communicate their desired spacecraft responses to the fault management team.

able. For those failures or faults for which a response was available, it was then determined who would respond at the local or system level, how they would respond, and how much time that response would take. In cases where engineers on the ground were required for successful response, the required contingency steps were captured as well.

Effects and Failure Modes Analysis

Once the expanded FMEA was completed, it was inverted such that it was sorted by effect so that for each effect, the list of potential causes (failure modes) was listed. This turnaround of the FMEA product was termed the effects and failure modes analysis. This analysis allowed the fault management team to determine the most effective corrective actions to the manifested effects, given the variety of causes. The methodical FMEA approach also gave confidence that all of the potential high-level response causes were captured.

Response Plans

The third step in this fault management and response planning process was to create corrective response plans based on the telemetry available to the spacecraft at the time of the various faults or failures. For completeness, these individual responses were then mapped back to individual FMEA line items.

This fault response approach is designed to implement a simple process with minimized impact to the observatory in the detection and response to less severe and isolated (local) faults. This response will allow the observatory to remain in operational mode if a local fault occurs.

The fault response approach also enables all subsystems of the observatory (power, communication, C&DH, and thermal) to remain safe in the event of critical fault conditions through a system-wide response to protect against “unknown unknowns.” This response will cause the observatory to demote to safe mode if a critical fault condition occurs.

CONCLUSION

Developing a FMEA is a useful process for any design campaign. By expanding the breadth and the scope of the FMEA, the PSP reliability team provided additional support to the fault management team. The expanded FMEA provided the basis for the effects and failure mode analysis, which grouped the similar effects and traced them back to their potential causes. This new product was used in shaping the fault management responses to faults and failures within the spacecraft and gave the team confidence that all potential failure modes had been captured. All of this worked together to increase PSP mission resilience, which was shown during PSP’s first encounter with the Sun in November 2018 and will continue to be shown over the course of the next 7 years and at least 23 more solar encounters.

REFERENCES

[1] Kinnison, J., Lockwood, M. K., Fox, N., Conde, R., and Driesman, A., “Solar Probe Plus: A Mission to Touch the Sun,” in *Proc. 2013 IEEE Aerospace Conf.*, Big Sky, MT, pp. 1–11 (2013).

[2] Guo, Y., McAdams, J., Ozimek, M., and Shyong, W.-J., “Solar Probe Plus Mission Design Overview and Mission Profile,” in *24th International Symp. on Space Flight Dynamics (ISSFD)*, Laurel, MD (2014).

[3] National Aeronautics and Space Administration, Office of Safety and Mission Assurance, *Risk Classifications for NASA Payloads*, 3rd Rev. (NPR 8705.4) (2 Oct 2014).

[4] Fretz, K., Kirby, K., Marsh, D., and Stratton, J., “Overview of Radiation Belt Storm Probes Fault Management System,” in *Proc. 2013 IEEE Aerospace Conf.*, Big Sky, MT, pp. 1–12 (2013).

[5] *Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*, MIL-STD-1629A, U.S. Department of Defense, Washington, DC (24 Nov 1980), https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=37027.

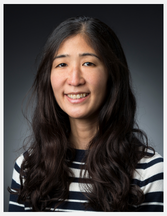
[6] Smith, C., “Evolving Interactions Between Reliability and Fault Management Processes,” *Proc. Trilateral Safety and Mission Assurance Conf. (TRISMAC)*, Frascati, Italy (2015).

Melissa R. Jones, Space Exploration Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Melissa Jones has performed reliability analyses on a number of NASA spacecraft in her nearly 20-year professional career. These include the International Space Station, the MESSENGER propulsion system (which is now a landmark on Mercury), STEREO, the Van Allen Probes, PSP, and the Europa Clipper. She has also spent time as a lead flight controller for the New Horizons mission to Pluto and beyond. She has bachelor’s and master’s degrees in aerospace engineering from the University of Maryland at College Park. At other times in her career, she has been a robotics engineer for a company that designed and built simulators for minimally invasive medical procedures and a project coordinator for a humanitarian organization working in the Middle East. In her spare time, she homeschools her three children. Her e-mail address is melissa.r.jones@jhuapl.edu.

Kristin A. Fretz, Space Exploration Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Kristin Fretz has worked in APL’s Space Exploration Sector since 2000. She has more than 15 years of engineering experience on a variety of NASA space programs, serving in reliability, fault management, and systems engineering roles. Currently, she is the Van Allen Probes mission system engineer and previously worked as the fault management and reliability lead engineer. Kristin has also supported fault management and payload systems engineering on PSP and worked as the reliability lead on the New Horizons and MESSENGER programs. She received bachelor’s degrees in mathematics and health and exercise science from Wake Forest University in 1998, an M.S. in reliability engineering from the University of Maryland in 2000, and a Ph.D. in reliability engineering from the University of Maryland in 2006. Her e-mail address is kristin.fretz@jhuapl.edu.



Sanae D. Kubota, Space Exploration Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Sanae Kubota is the fault management lead engineer and deputy spacecraft systems engineer for the PSP mission. She has 18 years of engineering experience working with numerous NASA spacecraft projects. Her experience includes systems engineering for the International Lunar Network and its Earth-based landing algorithm test vehicle, reliability analyses for the International Space Station, and system safety engineering for the MESSENGER and New Horizons spacecraft. She received a B.S. in mechanical engineering and an M.S. in computer science from the Johns Hopkins University. Her e-mail address is sanae.kubota@jhuapl.edu.

Clayton A. Smith, Space Exploration Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Clayton Smith is a member of the Principal Professional Staff at APL and has more than 30 years of experience analyzing systems from risk, reliability, and safety perspectives. These systems included NASA and DoD missions, payloads, ground communication systems, air traffic control systems, and missile systems. He is developing approaches to assess intentional threats against space assets using probabilistic risk analysis and game theory techniques. He created and managed NASA's International Space Station Program probabilistic risk assessment specifically geared toward quantifying the safety risk during operations. Clayton is currently the reliability engineering lead for APL's PSP mission. He received a B.S. in aerospace engineering, an M.S. in engineering management, and a Ph.D. in reliability engineering all from the University of Maryland. His e-mail address is clay.smith@jhuapl.edu.