Developing a Fault Management Guidebook for NASA's Deep Space Robotic Missions

Lorraine M. Fesq[1], Raquel Weitl Jacome[2]
Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California 91109

NASA designs and builds systems that achieve incredibly ambitious goals, as evidenced by the Curiosity rover traversing on Mars, the highly complex International Space Station orbiting our Earth, and the compelling plans for capturing, retrieving and redirecting an asteroid into a lunar orbit to create a nearby a target to be investigated by astronauts. In order to accomplish these feats, the missions must be imbued with sufficient knowledge and capability not only to realize the goals, but also to identify and respond to off-nominal conditions. Fault Management (FM) is the discipline of establishing how a system will respond to preserve its ability to function even in the presence of faults. In 2012, NASA released a draft FM Handbook in an attempt to coalesce the field by establishing a unified terminology and a common process for designing FM mechanisms. However, FM approaches are very diverse across NASA, especially between the different mission types such as Earth orbiters, launch vehicles, deep space robotic vehicles and human spaceflight missions, and the authors were challenged to capture and represent all of these views. The authors recognized that a necessary precursor step is for each sub-community to codify its FM policies, practices and approaches in individual, focused guidebooks. Then, the sub-communities can look across NASA to better understand the different ways off-nominal conditions are addressed, and to seek commonality or at least an understanding of the multitude of FM approaches. This paper describes the development of the "Deep Space Robotic Fault Management Guidebook," which is intended to be the first of NASA's FM guidebooks. Its purpose is to be a field-guide for FM practitioners working on deep space robotic missions, as well as a planning tool for project managers. Publication of this Deep Space Robotic FM Guidebook is expected in early 2015. The guidebook will be posted on NASA's Engineering Network on the FM Community of Practice website so that it will be available to all NASA projects. Future plans for subsequent guidebooks for the other NASA sub-communities are proposed.

Nomenclature

APL	=	Advanced Physics Laboratory
CDR	=	Critical Design Review
FDIR	=	Fault Detection, Isolation and Response
FM	=	Fault Management
FP	=	Fault Protection
FPP	=	Flight Project Practices
FTA	=	Fault Tree Analysis
HUMS	=	Health and Usage Monitoring
IEEE	=	Institute of Electrical and Electronics Engineers
IVHM	=	Integrated Vehicle Health Management
JPL	=	Jet Propulsion Laboratory
NASA	=	National Aeronautics and Space Administration
NEN	=	NASA Engineering Network
PDR	=	Preliminary Design Review
RM	=	Redundancy Management
SAE	=	Society of Automotive Engineers
SE	=	Systems Engineering
SHM	=	System Health Management
SIR	=	System Integeration Review
V&V	=	Verification & Validation

[1] Chief Technologist, Systems Engineering and Formulation Division, 4800 Oak Grove Drive, Pasadena, CA, AIAA Senior Member.
[2] Fault Protection Engineer, Systems Engineering and Formulation Division, 4800 Oak Grove Drive, Pasadena, CA, AIAA Member.

I. Introduction

In recent years, NASA has been focusing attention on the field of Fault Management - the discipline of establishing how a system will detect and respond to preserve its ability to function even in the presence of faults. NASA held two Workshops in 2008 [ref 1] and 2012 [ref 2] to gather the FM community with the goal of understanding the challenges that face the field, including project cost overruns and schedule slips. A number of recommendations emerged, including the development of a NASA FM Handbook to guide FM practitioners by providing established practices and methodology for designing, testing and operating FM. In 2012, NASA released a draft FM Handbook in an attempt to coalesce the field by establishing a unified terminology and a common process for designing FM mechanisms. The Handbook [ref 3] was distributed to the ten NASA Centers for review. An alarming number of comments, over 1100, were received, which was more than any other document distributed by the NASA Technical Standards Program Office to that date. What this review process had uncovered was how diverse the FM field is.

Fault Management (FM) is the discipline of establishing how a system will respond to preserve its ability to function even in the presence of faults. FM is an integral part of NASA's Systems Engineering process since timely and effective detection and mitigation of off-nominal conditions can make the difference between mission success and mission failure. FM approaches are highly dependent on mission characteristics such as

- The light time delay between the ground system and the space asset – for many deep-space missions, the light time often is longer than the time-to-criticality for many faults, so more fault handling mechanisms are engineered into the spacecraft;
- Whether humans are available to intervene – in human spaceflight missions, crews in space can work with operators on the ground to resolve many anomalies; and
- If a "safe" mode is a viable option – for critical events such as orbit insertions and landings, the option rarely exists to stop the activity and wait for ground operators to determine the problem and then transmit recovery commands; the opportunity to accomplish the event will have been lost in that time. However, for many earth-orbiting satellites, the environment is relatively known and stable, making "safe" mode a straightforward, practical choice.

Because of these different mission characteristics, FM approaches are very diverse across the different mission types and elements of space systems, such as

- Deep space robotic missions
- Earth orbiting robotic missions
- Earth orbiting human spaceflight missions
- Launch vehicles
- Ground/launch systems
- Control centers (mission systems)
- Aeronautics
- Deep Space Human Spaceflight (under development)

In fact, even the name "Fault Management" is not used consistently across the Agency. Other terms used to capture the essence of this field include System Health Management (SHM), Fault Protection (FP), Integrated Vehicle Health Management (IVHM), Fault Detection, Isolation and Response (FDIR), Redundancy Management (RM), Autonomy, Integrated Hazard and Aborts Analyses, and Health and Usage Monitoring (HUMS). The authors of the NASA FM Handbook were challenged to capture and represent all of the views from the communities that work within each of the different mission types and elements.

The attempt to coalesce the FM field through the development of a NASA-wide Handbook had exposed and highlighted the varied FM views, approaches and practices across the agency. In fact, comments against the Handbook were varied and diverse even within each of the sub-communities that work within the different mission types and elements listed above. The authors of the FM Handbook recognized that a necessary precursor step to writing an Agency-wide handbook is for each sub-community to codify its FM policies, practices and approaches in individual, focused guidebooks. Then, the sub-communities can look across NASA to better understand the different ways off-nominal conditions are addressed, and to seek commonality or at least an understanding of the multitude of FM approaches. This paper describes the development of the "Deep Space Robotic Fault Management Guidebook," which is believed to be the first of NASA's FM guidebooks. Its purpose is to be a field-guide for FM

practitioners working on deep space robotic missions, as well as a planning tool for project managers. This guidebook will become a chapter of the NASA FM Handbook, and will be a demonstrator of the future organization of the handbook, with one chapter dedicated to each mission type/element.

II. Overview of the Guidebook

The motivation to develop the Deep Space Robotic Fault Management Guidebook is two-fold. First, as mentioned in the previous section, the distribution of the NASA FM Handbook to all of the Centers uncovered discrepancies across the Agency, even within a particular community of FM practitioners. Second, the NASA FM Workshops exposed the circumstatnce that the set of institutional guidance for this discipline at many of the Center is incomplete. For example, currently at JPL, institutional documents provide definitions of what FM is and its role on a project. However, there is no formal guidance on how to design the FM portion of a system. This lack of design guidance leads to a number of challenges. For example, lack of a formal process can lead to ad hoc implementations resulting from a project's culture or FM designs that are derived from the heritage knowledge of individuals rather than a careful inspection of key mission characteristics. Also, sub-allocation of FM capabilities between the flight system and the ground system, and among the spacecraft subsystems can be uncoordinated if not explicitly managed, resulting in a lack of flow-down and integration direction. Finally, a composite of approaches are sometimes implemented, instead of a top-down architected approach. This leads to difficulties in understanding, behavioral conflicts, integration problems, and challenges to verifying and validating the FM portion of the system. These challenges lead to added incidental complexity, higher costs and increased schedules, especially during the integration and test phase of a mission.

Recently, the FM community has recognized this lack of guidance, and there has been significant movement in the field to methodize how to design FM. In particular,

- JHU/APL developed a process description for fault protection titled QY3-660, "Fault Management Engineering Process"
- The Society of Automotive Engineers (SAE) developed a book/standard titled "IVHM: Perspectives on an Emerging Field"
- IEEE is developing a "Prognostics and Health Management Standard"
- Aerospace Corporation developed two guidelines for Earth-orbiting spacecraft:
    - Aerospace Report No. TOR-2009(8591)-14, "Effective Fault Management Guidelines, 5 June 2009"
    - Aerospace Report No. TOR-2012(1302)-13, "Proposed Satellite System Safe Mode Standard," August 1, 2012 (Draft)

The purpose of the Deep Space Robotic FM Guidebook is two-fold. The Guidebook is designed to be a field-guide for FM practitioners and systems engineers on NASA deep space robotic missions to provide them with a structured approach to designing, building, testing and operating the FM portion of a space system. It also is intended to provide guidance as a planning tool, enabling managers to set expectations of cost, schedule and deliverables at major project milestones. This Guidebook is related to, and should be used alongside of other NASA documents, particularly the NASA Systems Engineering Handbook [ref 4]. The systems engineering functions and project lifecycle defined in the SE Handbook were used to define and organize the tasks in the Deep Space Robotic FM Guidebook. In addition, the FM functions identified in the Guidebook are defined in context of NASA's systems engineering engine. Other related documents that should be used in conjunction with the Guidebook are the NASA FM Handbook, the NASA 2008 and 2012 FM Workshop reports, and institutional/Center practices such as JPL's Design Principles [ref?] and Flight Project Practices [ref?].

III. Details of the Guidebook

The Deep Space Robotic FM Guidebook captures the tasks needed to be performed to define and implement the FM portion of a space system. These tasks are overlaid onto the NASA defined Mission Phases. The Guidebook provides details needed to perform each FM task, such as inputs and documents needed, step-by-step directions and pointers, as well as expected/required deliverables associated with that task. The format of the Guidebook includes:

- A top-level FM process that uses the Systems Engineering (SE) engine defined in NASA's SE Handbook to define the high-level organization of FM activities for a project;

- A layout of activities for each mission phase that identifies the FM tasks to be performed in each phase and the relationships between the tasks (i.e., required inputs, expected outputs, and and the products resulting from each FM task). These tasks are organized in swim lanes aligned with the relevant SE functions as defined in NASA's SE Handbook such as Requirements Definition, Technical Solution Definition and Design Realization;
- Detailed descriptions for each task elaborating the definition, the objective, the detailed steps needed to accomplish the task, metrics for achieving the task, schedule, and expected deliverable(s).

III.A Top-Level FM process

Starting at the highest level of detail, Figure 1 shows the FM Process Flow and allows the FM engineer to understand the general flow of work required throughout each mission phase. The high-level Process Flow provides the big picture of the FM activity on a project, and sets the expectations for FM conceptual design, architecture definition, V&V planning, etc. Major milestones and key decision points are provided at the top, and serve as the driving force for scheduling and completion of major activities.

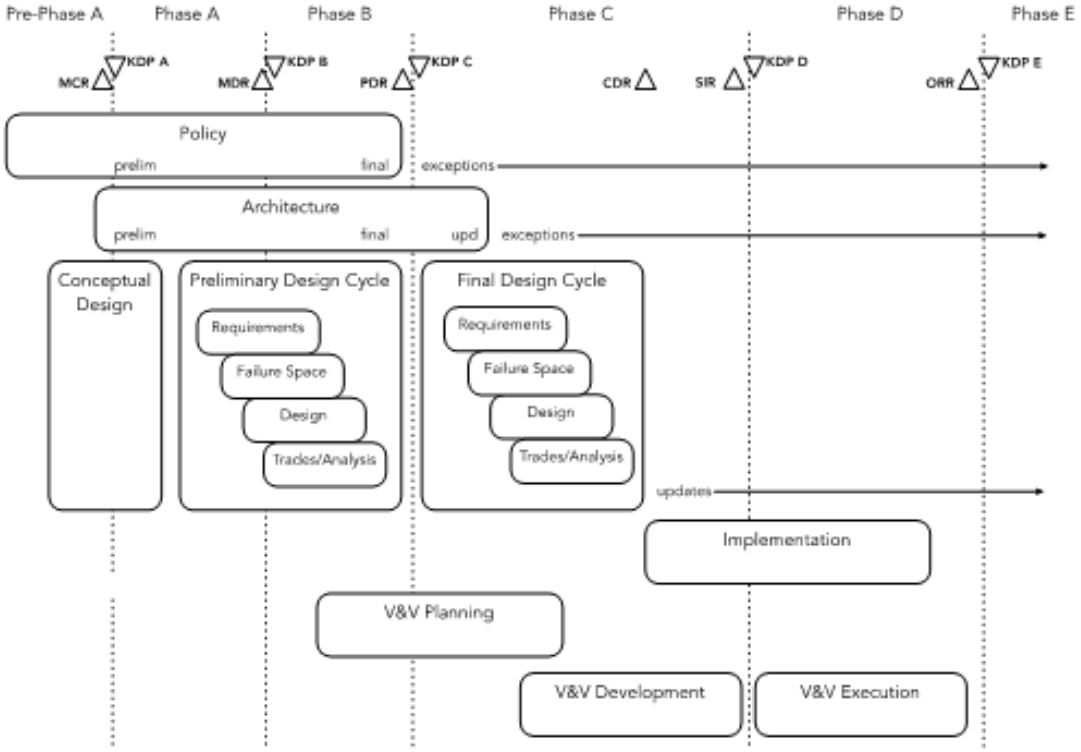

Figure 1 – Fault Management Process Flow

III.B High-Level FM flows

At the next level of detail, the Guidebook expands each Phase into a separate graphical representation we call the Phase "Spider Diagram," as seen in Figure 2. A Spider Diagram is defined for every phase, and represents all FM tasks to be completed within that phase. The Spider Diagarm identifies all applicable input documents and deliverables for each FM task. These diagrams distinguish between intermal FM versus external products, including deliverables that may be needed by other Systems Engineers, as well as identifying any deliverables that are required for major reviews such as PDR, CDR, SIR, etc. These diagrams enable the FM engineer to become aquainted with how the tasks depend on one another, how the products will be used, and when the products are

required within the framework of the Mission Phase Milestones. The Spider Diagrams organize the various tasks and products into NASA SE topic "swim-lanes" – Technical Assessment, Technical Plannning, Requirements Definition, Technical Solution Definition, Design Realization, and Evaluation Process.

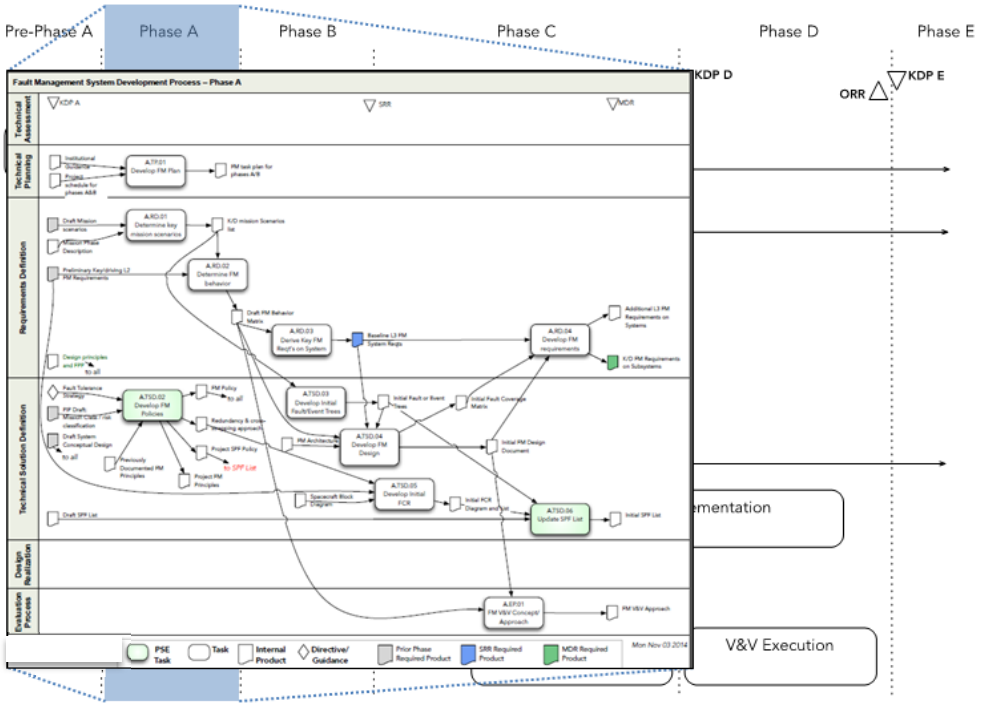

Figure 2 – Phase A "Spider Diagram"

III.C Task Desciptions

Each task identified on a Spider Diagram is further expanded into a more detailed outline to convey precisely what is expected and how it should be executed. These task descriptions include details such as a description of the task, the task objective, when the task is expected to be performed within the project milestone framework, required inputs needed to accomplish the task, detailed step-by-step instructions to perform the task, and the expected deliverables.

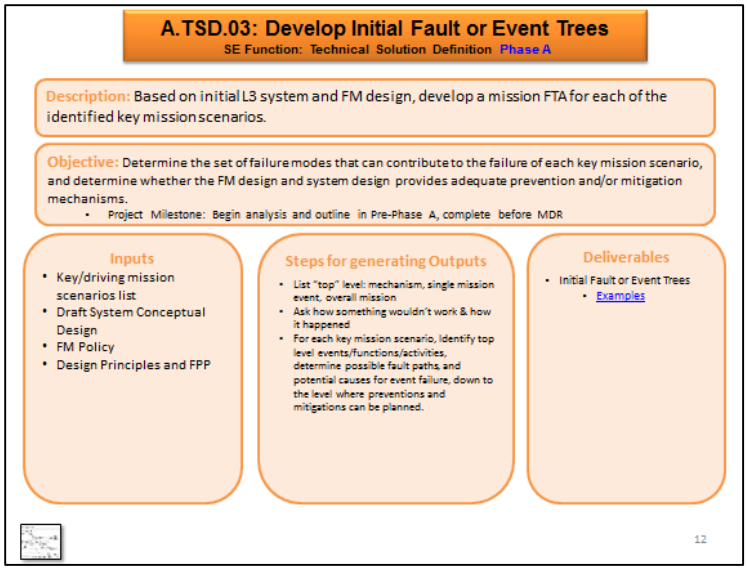

Figure 3 – Example Task – Develop Initial Fault or Event Trees

Shown in Figure 3 is the task description for "Develop Initial Fault or Event Trees" containing all the necessary information needed for developing initial FTAs. The description answers the question - "What is this task?" For our Initial Fault Trees, it describes the task as developing a Mission FTA for each identified Mission Scenario. The next entry in the Task Outline is the Objective – "Why are we completing this task?" Each task carried out by an FM

engineer over the course of the project lifetime should have a purpose for the project; wasted effort equates not only to wasted time, but also wasted money. The objective gives value to the task at hand as well as listing any applicable project milestones and schedule constraints. This task describes the objective as "determining the set of failure modes that can contribute to the failure of each key mission scenario" as well as "determining whether the FM design and system design provides "adequate prevention and/or mitigation mechanisms." Listed in the Inputs block are the documents and products required to perform this task – in this example, those products include the Key/Driving mission scenarios list, Draft System Conceptual Design, the project's FM Policy as well as Design Principles and FPPs. The "Steps for generation Outputs" box answers the "How do we complete this task?" question and details all the nuances that the FM engineer will need to remember when working through this task. This will help to promote consistency across the Deep Space Robotic community by describing what the process is for producing each FM task. Lastly any deliverables associated with this task are listed, as well as hyperlinks to example artifacts or sample templates showing how the deliverable could be expressed. These examples allow a FM engineer to see an example of the task from a different mission/project. All of the task defined in the guidebook have this same level of detail, and provide an FM engineer with the necessary guidance and tools needed to perform the FM activities and fufill the FM responsibilities.

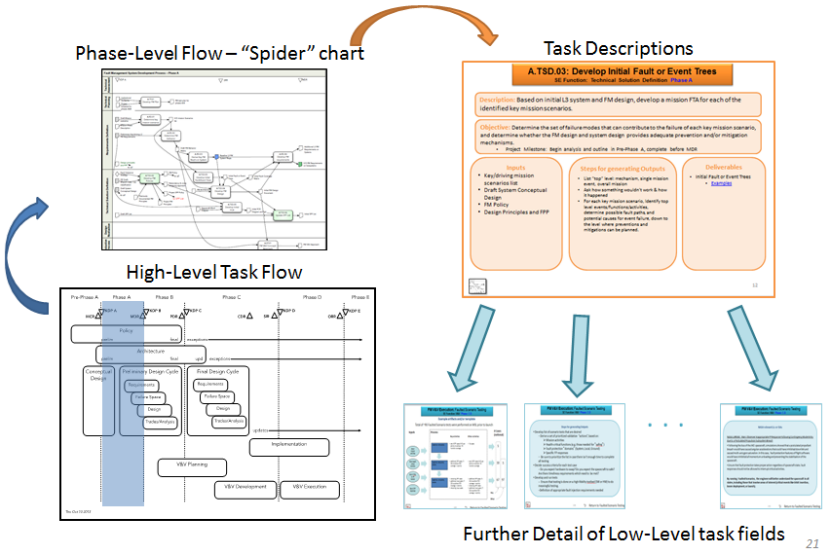

Figure 4 – Guidebook Navigation

The current format of the Guidebook is compiled into a PowerPoint Presentation with navigable hyperlinks enabling the reader to move through the document by choosing the level of detail desired. Figure 4 shows how the reader can gain more detail of each task by entering levels of greater detail. There are plans to also migrate the Guidebook into a hosted wiki format in addition to this exportable PowerPoint Presentation. Once completed, the wiki-based guidebook will be posted on the NASA Engineering Network (NEN) FM Community of Practice website (https://nen.nasa.gov/web/faultmanagement/home), where it will be accessible to all of NASA.

IV. Summary and Future Plans

This paper describes the development of the "Deep Space Robotic Fault Management Guidebook," a field-guide for FM practitioners and managers working on NASA's deep space, uncrewed missions. FM approaches are very diverse across NASA, especially between the different mission types such as Earth orbiters, deep space robotic vehicles and human spaceflight missions. In recent years, NASA has recognized this diversity, as well as a seemingly *ad hoc* approach to designing how faults are handled. The deep space robotic community has been codifying its FM policies, practices and approaches to provide guidance on how to design, develop, test and operate FM for this type of mission. The guidebook contains process information throughout a project's lifecycle, such as FM tasks to be performed and expected deliverables to be produced at major project milestones. It also includes example FM products from projects, as well as templates for deliverables.

The Deep Space Robotic FM Guidebook will be posted on the NASA Engineering Network (NEN) FM Community of Practice website where it will be accessible to NASA community. Future plans are to "socialize" the

format of the guidebook with communities of other mission types in order to encourage the development of FM Guidebooks for all of the mission types and elements. In the nearterm, this collection of guidebooks would be included as chapters of the FM Handbook so that all viewpoints are represented. Once each community has codified its approach to FM, only then we can look across the mission types to better understand the different ways off-nominal conditions are addressed across NASA, to identify similarities and differences, seek commonality or at least an understanding of the multitude of FM approaches, and ultimately to coalesce the FM field, as directed by the NASA Chief Engineer.

Acknowledgments

The work described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract with the National Aeronautics and Space Administration. The authors are grateful to many people, without whose support and contributions, this paper could not be written: John Day, Magdy Bareh, Tracy Nielson, Gene Lee, Mary Lam, Molly Bittner, Jeffery Nunes, Bharat Chudasama, Chi Lin, Danielle Marsh, Julie Wertz and Kristen Fretz.

References

[1]Fesq, L., Cancro, G. Jones, C., Ingham, M., Leitner, J., McDougal, J., Newhouse, M., Rice, E., Watson, D., Wertz, J., NASA White Paper Report: "Spacecraft

[2]Fesq L., Fretz, K., Newhouse, M., NASA White Paper: "Report on the 2012 NASA Spacecraft Fault Management Workshop for the Science Mission Directorate, Planetary Sciences Division," February 2013.

[3]Fesq, L. (ed.). "Fault Management Handbook." NASA Technical Handbook, NASA-HDBK-1002, Second Draft, 2 April 2012.

[4] NASA Systems Engineering Handbook.