

# Fault Management Practice: A Roadmap for Improvement

Lorraine M. Fesq<sup>1</sup> and David Oberhettinger<sup>2</sup>

Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, CA 91109-8099

**Autonomous fault management (FM) is critical for deep space and planetary missions where the limited communication opportunities may prevent timely intervention by ground control. Evidence of pervasive architecture, design, and verification/validation problems with NASA FM engineering has been revealed both during technical reviews of spaceflight missions and in flight. These problems include FM design changes required late in the life-cycle, insufficient project insight into the extent of FM testing required, unexpected test results that require resolution, spacecraft operational limitations because certain functions were not tested, and in-flight anomalies and mission failures attributable to fault management. A recent NASA initiative has characterized the FM state-of-practice throughout the spacecraft development community and identified common NASA, DoD, and commercial concerns that can be addressed in the near term through the development of a FM Practitioner’s Handbook and the formation of a FM Working Group. Initial efforts will focus on standardizing FM terminology, establishing engineering processes and tools, and training.**

## I. Introduction

Fault management (FM) is the set of engineering practices that enable an operational system to contain, prevent, detect, isolate, diagnose and respond to conditions that may interfere with nominal operations. FM enables a spacecraft system to detect, isolate, and recover from in-flight events that may hinder nominal mission operations. FM often is identified using different terms, and it is used here to encompass related terms such as Fault Protection, Redundancy Management, Health Management, Fault Detection/Isolation/Recovery (FDIR), and Safing. Autonomous FM is especially critical for deep space and planetary missions where the limited communication opportunities with ground-based operators may prevent timely intervention by ground control. However, increasingly challenging science objectives imposed upon deep space missions are driving new FM requirements and taxing the ability of onboard spacecraft resources and control logic to manage in-flight fault events.

Evidence of pervasive architecture, design, and verification and validation (V&V) problems with NASA FM engineering has been revealed both during technical reviews of spaceflight missions and in-flight. These problems include:

- FM design changes required late in the life-cycle (that often necessitate secondary changes elsewhere in the system),
- Insufficient project insight into the required system-level FM testing, and unexpected test results that require additional, unplanned test time for resolution,
- Spacecraft operational limitations because restrictions are placed on the use of untested functions (in compliance with the “fly-as-you-test” principle).
- Mission failures (e.g., Mars Global Surveyor and Imager for Magnetopause-to-Aurora Global Exploration (IMAGE)) and in-flight anomalies attributed to FM.

In particular, the NASA Science Mission Directorate (SMD), Planetary Science Division (PSD), has experienced a number of technical and programmatic issues related to FM on recent deep space missions. The issues appeared regardless of the organizations involved and occurred in both in-house NASA-developed missions and contractor-developed missions. The resulting schedule impacts jeopardized the missions’ readiness for launch; the launch date

---

<sup>1</sup> Principal Engineer, Engineering Development Office, Systems and Software Division, M/S 301-225, and AIAA Senior Member.

<sup>2</sup> Systems Engineer IV, Office of the Chief Engineer, 301-370, and AIAA Senior Member

for planetary missions often cannot be delayed without a severe impact on the mission outcome. The resulting cost overruns impact NASA's ability to fund other missions.

NASA SMD/PSD commissioned an industry-wide Spacecraft Fault Management Workshop that was held in April 2008 to characterize FM practices, identify trends, and provide a roadmap for improvements. The workshop was very successful in drawing 100 participants from government, industry, and academia, characterizing the state-of-the-practice of FM, distilling specific FM engineering concerns, and generating a roadmap for both near- and long-term NASA actions to address these concerns. The workshop final report<sup>1</sup> published in March 2009 provides 12 sets of findings and recommendations in the areas of requirements definition, design, and test practices for FM. For example, the workshop affirmed the benefits of ingraining FM into the system architecture instead of the more common practice of considering how faults will be handled after the nominal design is in place.

## II. Methodology

The programmatic scope of the workshop focused on deep space and planetary robotic missions since the observed challenges had all occurred on missions of this nature. However, workshop participants recognized that Earth-orbiting (EO) missions and Human Space Flight (HSF) missions also suffered from similar symptoms, although perhaps to a lesser degree, and that there was sufficient overlap in FM architectures and V&V methodologies to warrant strong representation and participation from the EO and HSF communities.

In preparation for the workshop, the workshop organizers conducted a detailed survey of FM practices in the planetary spacecraft development community. The workshop was structured into multiple sessions that included formal presentations on current mission experiences and relevant research. To achieve a better understanding of the issues, the workshop addressed such questions as:

- How may the FM development and system-level testing processes be more predictable from a cost and schedule standpoint?
- What are the system-level design or lifecycle process aspects that drive FM changes late in the lifecycle?
- Are different FM approaches more or less susceptible to these issues?
- Are these issues occurring only on planetary missions or are similar issues happening on Earth-orbiters and/or in the human spaceflight program?

The workshop methodology employed five components -- (1) case study presentations, (2) Request for Workshop Input (RFWI), (3) targeted roundtable discussions, (4) invited speakers, and (5) poster presentations. Workshop participants were asked to identify technology issues and process issues that are driving unplanned cost growth and schedule growth in FM systems for unmanned, autonomous spacecraft. In addition, a significant amount of time was spent in three focused discussion sessions that addressed particular aspects of the FM problem. Specifically:

- FM architectures.
- FM verification and validation (V&V).
- FM development practices, processes, and tools.

In soliciting these inputs, the purpose was not to derive a single FM engineering standard, but rather to rise above institutional preferences and evaluate the applicability, strengths, and weaknesses associated with different FM approaches. The results from each of these sessions were presented in terms of "lessons learned," "best practices," and "opportunities for investment." The results from these sessions have been combined in this paper with FM survey responses and information from the presentations of current mission experiences to create a single set of top-level findings and recommendations.

## III. Key Findings & Recommendations

Three general observations can be made from the information offered by the workshop participants:

- 1) The implementation of FM within the software domain is generally similar across NASA, other government agencies, and industry, and it can be characterized as an "alarm-and-response" system; i.e., the software monitors information from various on-board sensors for conditions that are out of specified bounds and responds to violations by sending a sequence of corrective commands. Low-level differences in how alarms

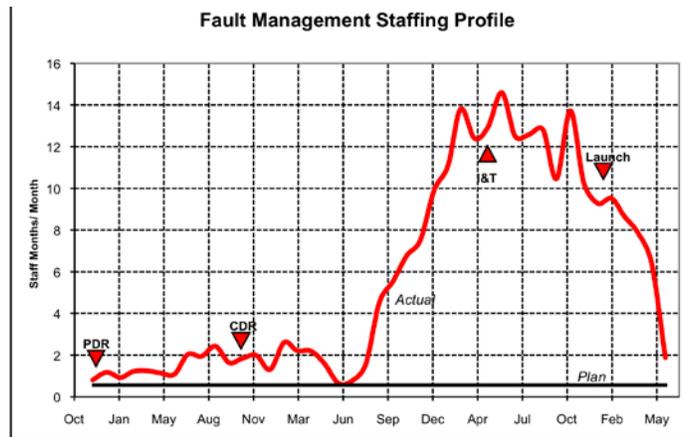
and responses are represented, implemented, and arranged hierarchically, and in the design of responses as single or multi-threaded, represent trade-offs.

- 2) The FM capabilities incorporated into current missions are not limited by the available technology, but rather by flight programs and flight system designs that place insufficient emphasis on FM and by a poorly disciplined approach to FM design and implementation. While advancements in FM technology would be beneficial— e.g., improvements upon rule-based systems may permit the needed scale-up to meet the requirements of future deep-space missions— addressing the systems engineering problems of current-generation programs is an essential prerequisite.
- 3) Established FM designs have provided adequate in-flight performance. FM flaws have not had an adverse impact on mission success, though some errors and false trips have resulted in unnecessary safing events and have prompted FM configuration changes.

The following key findings have been distilled from the frank workshop participant discussions of their experiences in designing and implementing FM on robotic missions:

**FINDING 1 – Unexpected cost and schedule growth during final system integration and test are a result of underestimated V&V complexity combined with late resource availability and staffing.**

Perhaps the single most significant finding is the prevalent lack of consideration that spaceflight projects give to FM in early mission phases, a major contributor to unplanned cost and schedule growth during system development. The large increases between planned labor and actual labor hours in recent missions provide evidence of this poor planning. For example, Figure 1 depicts an actual mission discussed during the workshop that planned for FM staffing at the level of 0.5 Full-Time Equivalent (FTE) engineers throughout the mission. In actuality, FM staffing peaked at more than 14 FTEs during the system-level integration and test (I&T) stage of development. This is reportedly a common occurrence: an initial view of FM as a side responsibility of a single system engineer is replaced by the assignment of a full time engineer as the mission progresses, and it eventually requires an entire team to deal with problems, testing, etc.



**Figure 1 -- Planned vs. Actual Profile for FM staffing from a Case Study mission. This unplanned “bump” in staffing consistently appeared on numerous missions.**

**Recommendation 1a: Allocate FM resources and staffing early, with appropriate schedule, resource scoping, allocation, and prioritizing. Schedule V&V time to capitalize on learning opportunity.**

As space system complexity increases, it is becoming more important to begin FM system design in the very early stages of mission design. FM requirements should be addressed in Pre-Phase A. FM engineers should be involved in proposal development or initial planning. A training period should be provided together with the necessary equipment and tools, prior to ramp-up, and a strong FM lead and team should be active throughout spacecraft development. V&V is a critical process that cannot be an afterthought for a project simply because it occurs late in the development cycle. V&V planning should not be overly optimistic: the project schedule and budget must allow for finding and fixing anomalies. In addition, all projects should have an incompressible test list of fault scenarios.

**Recommendation 1b: Establish hardware / software / “sequences” / operations function allocations within an architecture early to minimize downstream testing complexity.**

Hardware, software, on-board sequences and operations procedures provide different levels of isolation, reliability and flexibility to a design. If the allocation of FM functions among these elements, including tradeoffs between hardware, software, and operational provisions selected to protect the system, is not established early in the

project lifecycle, FM will receive late or changed requirements resulting in non-optimal architectural elements, and testing opportunities will be pushed downstream.

***Recommendation 1c: Engrain FM into the system architecture. FM should be “dyed into the design” rather than “painted on.”***

Integrating the management of faults into the baseline design reduces the complexity of the overall design and permits the design of generic protections that can remedy large classes of faults. Also, responses can be developed in such a way as to reduce coupling to other elements of the FM architectures, reducing the complexity of system test efforts.

**FINDING 2 – Responsibility for FM currently is diffused throughout multiple organizations; unclear ownership leads to gaps, overlap, and inconsistencies in FM design, implementation, and validation.**

The lack of a clearly defined relationship between the Systems Engineering and the Safety and Mission Assurance (SMA) organizations has caused difficulties in FM design, implementation, and validation on spaceflight projects. In developing the mission fault set, NASA centers tend to utilize failure analyses and mission assurance analyses drawn from the SMA disciplines, as well as subsystem engineer interviews. Industry practitioners more commonly use heritage fault sets updated with subsystem interviews to converge on a fault set, with some use of failure modes and effects analyses when they are available. In all cases, interaction with subsystem engineers and mission assurance is paramount to assessing how a system can fail and defining the failure modes against which the system FM design will protect.

***Recommendation 2a: Establish clear roles and responsibilities for FM engineering.***

Clear roles and responsibilities need to be defined between the Engineering and the SMA organizations with regard to defining FM scenarios, identifying faults, and determining risk levels associated with identified faults. In particular, mission assurance should have a larger role in FM design. One organization stressed that an integrated product team environment can provide a sound approach to ensure that a system-level perspective is enforced, that all of the elements are brought together in the process, and that component-level and system-level behavior is properly characterized, tested, and stressed on the ground.

***Recommendation 2b: Establish a process to train personnel to be FM engineers and establish or foster dedicated education programs in FM.***

Even though deep-space missions tend to be unique, the FM knowledge base and lessons learned could best be retained by using the same personnel on multiple missions. The current generation of FM engineers is typically drawn from Attitude Control Subsystem/Guidance, Navigation and Control (ACS/GNC), or I&T organizations. Anecdotal information at the workshop indicated that these engineers are generally forced to learn on the job without formal training dedicated to the FM domain. NASA should advocate for the creation of an FM academic/engineering discipline.

**FINDING 3 – There is a lack of standard terminology for FM systems that causes problems in reviews and discussions, particularly when multiple organizations partner on a project.**

Various organizations across NASA, other government agencies, and industry use different terminology and different ways to represent a FM architecture. Terminology differences are so deep that there are even significant differences in the definitions of the terms used to describe the prevention and treatment of faults-- fault management, fault protection, fault avoidance, redundancy management, or FDRIR (fault detection, response, isolation, and recovery). Table 1 provides a sample list of terms that are frequently used in the FM field, but lack common definitions.

**Table 1 -- List of terms currently having multiple definitions when used within the FM field**

Anomaly	Diagnosis	Failure
Fault	Fault management	Fault protection
Fault recovery	Fault tolerant	FDIR

Fault isolation	Redundancy management	Error
-----------------	-----------------------	-------

Terminology differences can happen even within a single organization. Reportedly, one major spacecraft anomaly was partially caused by project members using similar terminology with slightly different definitions, leading to misunderstanding and design errors.

***Recommendation 3: Standardize FM terminology to avoid confusion and to provide a common vocabulary that can be used to design, implement, and review FM systems.***

NASA should take a lead role in establishing a standard FM terminology and a well-defined set of metrics for FM characterization. Lacking a standard terminology, it will be difficult to avoid miscommunication and confusion during the design process and reviews, evolve FM into a discipline, or address the other findings in this paper. Hence, Recommendation 3 should likely be the first to be addressed by NASA as a prerequisite for other advancements in the FM state-of-practice. This standardization will also require the involvement of a broad spectrum of the FM community in order to achieve overall consensus and acceptance.

**FINDING 4 – There is insufficient formality in the documentation of FM designs and architectures, as well as a lack of principles to guide the FM processes.**

FM systems have become so complex that it has become very difficult to visualize all the monitors, responses, and locations where FM functions are implemented, and to visualize how a change in a monitor, response, or parameter will affect the rest of the system. This poses a special challenge for system engineers who are often charged with designing and implementing the monitors and responses, but who are not software specialists. The inability of FM developers to describe or formally document the complex FM architecture and concept of operation translates into ineffective project reviews and poor coordination of FM with other subsystems. Such unstructured representation and knowledge transfer of the FM requirements and design is a major cost driver for FM design and test. In addition, almost all respondents to the RFWI identified technical reviews as key milestones, but most also reported that additional reviews were helpful to address topics of specific interest.

***Recommendation 4a: Identify representation techniques to improve the design, implementation, and review of FM systems.***

Effective documentation of the FM system design would be a boon throughout the project lifecycle. Such documentation should clearly show how the FM architecture meets institutional and Agency guidelines for FM systems, provide justification for FM design decisions, and address the allocation of functionality between hardware, flight software, ground software, and operations. Development of a process or tool that links FM conceptual design, requirements generation/decomposition, design, development, I&T, and operation would result in major savings and risk reduction for spaceflight projects. In addition, descriptive visualization tools are needed to graphically depict FM design and behavior (and telemetry activity) in accessible terms so that reviewers, testers, and operators can understand the system design and response.

***Recommendation 4b: Formulate a set of design principles to aid in FM design.***

Many lessons have been learned on recent missions that would benefit future FM designers. However, these lessons are not easily captured or transferred to other engineers. Consequently, the FM community is witnessing the reoccurrence of similar problems across missions. The case studies presented at the workshop identified a FM design principles, based on lessons learned, that apply across the industry and should be used as guidelines on future missions. For example:

- FM should include features that will protect the spacecraft from known risks, even where no fault has been specifically identified for the flight system. This is because known failure modes may not be fully understood, and unexpected situations can occur.
- Characterization of unknown faults (and methods of recovery from them) should be included in safing recovery procedures. The procedures must be properly planned, tested, and practiced for rapid execution, where necessary.
- Treat autonomous changes to redundant systems with caution. It is often preferable to operate a primary system with a minor flaw rather than switch to a redundant backup system that may exhibit worse performance.

- Although a high level of complexity is inherent in the FM of deep-space missions, the simplest FM design is often the best. Look for opportunities to apply simplifying assumptions to extremely complex FM problems. (See Recommendation #7.)

**FINDING 5 – Metrics have not been established to evaluate FM systems or measure the progress of FM system development.**

Consistent with the lack of standard FM processes, engineering roles, and terminology, there is a lack of standard metrics for evaluating the appropriateness of different canonical FM approaches to meeting specific mission requirements and for tracking progress of FM development, test, and integration. It became apparent during the workshop that variations in FM requirements across mission classes-- manned, deep-space, landed, and Earth-orbiting—obviates deriving a single optimal design solution. Currently, the only metrics in common use by participants are staffing levels (see Finding 1) and “rule counts” in those architectures that support rules. These metrics do not relate fundamental FM requirements or design parameters to estimates of mission cost and complexity, and they cannot serve as an effective basis for improvement and maturation of engineering processes.

***Recommendation 5a: Identify FM as a standard element of the system development process.***

FM is not typically regarded as an engineering discipline distinct from GNC, propulsion, communications, etc., and its cost and schedule impact can get lost in early program planning. Recognizing FM engineering as a separate and distinct element of the system development process, and as an area of evaluation for competitive mission proposals, would highlight its importance. This recognition should include highlighting FM in the program structure (e.g., dedicated Work Breakdown Structure [WBS] elements), and the use of generally accepted measures of risk, complexity, and performance.

***Recommendation 5b: Establish metrics that will allow proposal evaluators and project teams to assess the relevance, merits, and progress of a particular FM approach.***

A comprehensive suite of FM metrics should encompass risk, complexity, and performance. (The “complexity” metric is essential to assessing the level of V&V effort needed.) Performance could be further broken down to include “functional” measures, such as diagnostic coverage of the fault space, timing responsiveness of the fault responses, and determinism, and “non-functional” measures such as testability, usability, and maintainability. Features that promote these properties should be inherent in FM architectures. Performance measures and progress metrics (e.g., FM test progress) need to be specified for the key figures of merit, and reported during reviews and at major milestones of FM architecture development. Table 2 shows an example process specification that identifies FM tasks for each mission phase, along with suggested tools to perform these tasks.

**Table 2 -- Sample FM process specification**

<b>Mission Phase</b>	<b>Focus</b>	<b>Tools</b>
Conceptual Design (Pre-A)	<ul style="list-style-type: none"> <li>• Understand Critical Risks &amp; Mitigation Costs</li> </ul>	<ul style="list-style-type: none"> <li>• Qualitative/Quantitative Risk Analysis</li> </ul>
Preliminary Analysis (A)	<ul style="list-style-type: none"> <li>• Preliminary Quantitative Risk Assessment</li> <li>• Architecture Trades</li> <li>• Cost Estimation</li> </ul>	<ul style="list-style-type: none"> <li>• FM Complexity Analysis</li> <li>• FM Costing</li> </ul>
Definition (B)	<ul style="list-style-type: none"> <li>• Probabilistic Risk Assessment</li> <li>• Preliminary FMEA</li> <li>• System &amp; Subsystem Requirements Development</li> <li>• Testbed Plan</li> </ul>	<ul style="list-style-type: none"> <li>• PRA &amp; FMEA Support</li> <li>• Test Planning</li> </ul>
Design/Development (C/D)	<ul style="list-style-type: none"> <li>• Formal Behavior Specification</li> <li>• Verification &amp; Validation</li> <li>• Operations Training</li> </ul>	<ul style="list-style-type: none"> <li>• Logic Verification</li> <li>• Simulation</li> <li>• HIL Testbeds</li> </ul>
Operations (E)	<ul style="list-style-type: none"> <li>• Contingency Response</li> <li>• Degraded Operations</li> </ul>	<ul style="list-style-type: none"> <li>• Telemetry Analysis</li> <li>• Plan Generation</li> <li>• Operations Interface</li> <li>• Simulation &amp; Testbeds</li> </ul>

**FINDING 6a – Practices, processes, and tools for FM have not kept pace with the increasing complexity of mission requirements and with more capable spacecraft systems.**

To take advantage of improvements in processor, sensor, and mechanism capabilities, spacecraft designers are using increasingly complex designs containing more subsystems with increasingly complex interfaces and embedded software. The increased complexity exponentially increases the number of potential system fault scenarios, but FM engineers lack the tools to determine the level of complexity that represents an unacceptable level of risk.

**FINDING 6b - Indications of potential spacecraft anomalies exist in test data, but are not always observed or not adjudicated.**

Reviewing the large quantity of data following a test anomaly often reveals indications of the problem that were not identified during the test because (1) the pass criteria of the test were met, (2) inadequate analysis time was allocated, (3) the test set was not comprehensive, or (4) schedule and budget pressures forced the test program forward. In-flight problems indicated by telemetry may also be missed until the anomaly occurs because the system performed in an unexpected manner, but still passed the official pass/fail criteria.

***Recommendation 6a: Design for testability: architectures should enable post-launch and post-test diagnosis.***

In test programs and in telemetry definitions, an alert should proceed from unexpected performance and early indicators of problems, instead of waiting until the thresholds for a given monitor are passed. Architectures that enable rapid diagnosis can stave off or provide quick recovery from in-flight faults, and during I&T the FM test data can aid in post-test analysis and troubleshooting.

***Recommendation 6b: Examine all observed, unexpected behavior.***

Workshop participants agreed that every anomaly or problem revealed during the V&V process should be fully addressed and resolved before launch to avoid occurrence in flight. It is necessary to investigate all anomalies during a test program and in flight, regardless of whether pass/fail criteria have been met. Because it is not possible to test all possible scenarios for complex systems, test programs should evaluate performance against a defined “behavior envelope” that envelopes a regime that is known to be safe.

***Recommendation 6c: Implement continuous process improvement for FM lifecycle.***

The V&V process, by nature, is a learning experience that should evolve throughout its duration. Lessons that are learned during the V&V process should be used to update and improve the procedures for the remainder of testing. Clear pass/fail criteria, and proper tools to assess test results, should be established to assure that questionable performance is not accepted.

***Recommendation 6d: Catalog and integrate existing FM analysis and development tools to identify capability gaps in the current generation of tools and to facilitate technology development to address these gaps.***

The workshop identified many FM tools in current use, but found that they are not integrated or coordinated in terms of functionality, or even terminology. For example, traditional analysis tools like Failure Mode and Effects Analysis (FMEA) are not directly linked with system design tools and architectures. Linkage through common or integrated tools will facilitate communications and help eliminate unnecessary sources of error in the system development process.

Certain capability gaps are evident in the current generation of tools. During concept and requirements development, for example, tools for quantitative complexity analysis and complexity/risk tradeoff would be particularly valuable. These tools should be linked with costing tools to enable early, high-level decisions in cost/risk, hardware/software, and human/system trade spaces. Better tools for system behavioral modeling during early development were also cited as a current capability gap.

**FINDING 7 – The impact of mission-level requirements on FM architecture complexity and V&V is not fully recognized.**

Having a single FM architecture address differing or conflicting requirements produces a complexity that may cause unexpected problems for missions. Although requirements for a fail-operational FM strategy, ground-in-the-loop response time, and protection of resources are major FM design drivers, the most stringent complexity driver appears to be a project requirement for single fault-tolerance. This requirement drives the design of a fully redundant

flight system and an FM system that is capable of monitoring and managing that redundancy, and managing the increased number of fault cases that must be handled. Three missions that had significant trouble with complexity reported problems with interactions between fault monitors or responses. Three other architectures had explicit provisions to de-conflict FM responses with other on-board activities. In a rule-based architecture, the number of possible on-board response interactions increases as the square of the number of fault monitors and responses.

Missions that require autonomous recovery of time-critical events (or have strict availability requirements) tend to drive the project to a complex “fail-operational” strategy, instead of adopting a less demanding “fail-safe” approach. For example, ion propulsion requires a continuous thrust that, if interrupted for too long, might interfere with navigation. Similarly, thermal control, power production, or the protection of an instrument might impose tight pointing constraints, making reduced pointing modes impractical for vehicle safing.

The clearest driver for fail-operational designs is the need to complete a mission critical event. Six of the missions that provided input identified at least one event that required most of the system to fail operational. For interplanetary missions, encounters commonly come with some critical component, usually a timed event like an orbit insertion or deployment when non-completion could cause a loss of science or the mission. Missions with hours-long communications delays are wholly dependent on autonomy to intervene if critical events encounter a fault. Functions that are necessary to completing these activities must be recovered in a timely manner to keep the spacecraft safe and to meet mission objectives.

***Recommendation 7: Review and understand the impacts of mission-level requirements on FM complexity. FM designers should not suffer in silence, but should assess and elevate impacts to the appropriate levels of management.***

When defining mission requirements, projects should give strong consideration to the impacts on FM V&V. Critical behaviors should be implemented as simply as possible, making them easier to characterize and execute more reliably. One approach to limiting complexity is to implement “dead-end” logic. If there is an appropriate end state for every response behavior, the emergent behaviors of the system are much easier to predict and significantly more stable. One project discussed during the workshop benefitted in-flight from dead-end logic when a repeating response would likely have been a risk to the mission.

**FINDING 8a – FM architectures often contain complexity beyond what is defined by project-specific definitions of faults and required fault tolerance.**

As a consequence of the intricacies and capabilities of FM, FM systems often are required to protect and manage on-board resources. Management of critical resources such as consumables, power, and redundant assemblies activated to avoid conflicts, often place non-trivial restrictions on the response to failures and increase FM complexity. FM engineers should press projects to limit FM system complexity to only those FM functions needed to address the faults and fault tolerance specified by the project.

**FINDING 8b – Increased FM architecture complexity leads to increased challenges during I&T and mission operations.**

Increased FM capabilities and complex operations drive increased potential for faults and increased complexity during I&T. At higher levels of integration, FM systems tend to have emergent behaviors that are difficult to predict, complicating V&V. Even slight variations in initial conditions may result in different system behaviors that (1) are difficult to test and (2) lead to many operational constraints that restrict operations. Also, some FM architectures (e.g., rule-based systems) may be difficult to scale up without introducing significant verification issues.

FM systems that are flexible and configurable are beneficial in that they permit in-flight modification, but they can significantly add to testing complexity. The many optional configurations of a flexible system translate to many test cases that need to be run. The flexible FM system, which may utilize commendable parameters in place of compiled code, must also be tested for sensitivity to the timing of faults, as the timing can affect response paths. The inability to exhaustively test a flexible system has led to operational restrictions and adjustments on multiple missions, with one mission electing to restrict operations to only those states that had been tested.

***Recommendation 8: Assess the appropriateness of the FM architecture with respect to the scale and complexity of the mission and the scope of the autonomy functions to be implemented within the architecture.***

One of the root causes of failure to prevent flight system anomalies is the complexity level of the FM system. FM designers must be aware of the consequences of complexity as it is introduced and make deliberate decisions

when introducing features that might increase system complexity—such as configurability. Good engineering judgment needs to be used in system design, and the configurability of the system should not be an excuse to delay design decisions or provide loose implementations. Projects need to define a strong architecture and desired behaviors for FM systems early and keep a consistent approach throughout design and test. The overlapping concerns of resource management and FM suggest that both should be addressed in a single architecture.

**FINDING 9 – FM architecture development is subject to changing priorities toward cost and risk over the course of system development.**

While flight projects place an early emphasis on flight system cost, as evinced by FM task staffing at 1 person or less, the project priority late in the project lifecycle switches to risk, forcing the FM architecture and staffing levels to evolve to accommodate newly discovered risks. The workshop discussed one project that originally was designed with a high tolerance for risk, but eventually proceeded to launch with a “must succeed” posture that created additional stress on the FM strategy.

Many organizations reportedly responded to the changing priorities by introducing flexibility for late additions into their architectures. Other organizations preferred to focus on developing more “inherent” robustness in their architecture early in the program. Some advocated combinations of both adding robustness features and flexibility if used sparingly. Regardless, all projects are helped by a tougher stance at the project level that evaluates overall risk against the cost that will be incurred during I&T due to late changes. However, an inability to characterize this “incurred” cost hampers project managers from making well-informed decisions.

***Recommendation 9: Define and establish risk tolerance as a mission-level requirement.***

The workshop consensus on this issue is that (1) an early and clearly defined risk posture helps guide FM design, and (2) consistency throughout the project is necessary to avoid friction and to formulate the best FM system for the project. Agreeing upon and carefully defining the level of risk tolerance early in the project lifecycle will help define the scope of testing and reduce the stress experienced during I&T. But project managers must develop and maintain a consistent risk posture over the project lifecycle, or fully appreciate implication to the FM design integrity and I&T schedule if the posture changes. Establishing a clear relationship between risk posture and I&T cost will provide project staff, mission managers, and reviewers with a better understanding of the consequences of risk decisions.

**FINDING 10a – The bulk of existing FM systems (e.g., mission-specific monitors and responses) is not inheritable. Heritage, similarity, and inheritance assumptions tend to underestimate budgeting for necessary V&V activities and review milestones.**

A recurring assumption that heritage flight systems will require less testing is a major reason why FM labor is commonly under-budgeted for flight projects. However, a new spacecraft with legacy software cannot be assumed to perform the same as a previous spacecraft, due to differences in timing and other minor system differences, and an extensive test program remains the norm.

In addition, the claim of FM heritage in the proposal or planning stages is often false or exaggerated. Because those FM systems classified as heritage or “re-use” may only require peer-review-- not a full design review—it is tempting to view them as heritage even when major adaptations may be required to meet the requirements of the new mission.

**FINDING 10b – Current FM systems do not support significant re-use.**

Many organizations employ engine-based or table-driven FM system designs to facilitate software re-use. However, the core of the FM functionality is not in the re-usable engine-based code, but rather in the mission-specific alarms and responses that are designed and inserted into this code. It was clear from the workshop discussions that an inability to re-use any significant portion of the mission-specific design or implementation is a common problem across NASA, other government agencies, and industry. The lack of re-use may be attributable to the one-of-a-kind types of missions pursued by NASA, and to the cultural differences and variations in FM philosophy between partnering organizations within the aerospace industry.

***Recommendation 10: During the proposal evaluation phase, examine claims of FM inheritance to assess the impacts of mission differences.***

Logical patterns should exist within a mission’s FM system that are applicable to future missions. Consider development of FM re-use concepts, potentially similar to software patterns or objects. However, the V&V engineer

and project manager should carefully examine all of the components, the environment, and the modes of operation before exploiting heritage assumptions to an effort to reduce the level of V&V. Use extreme caution when attempting or assessing claims of FM system re-use.

**FINDING 11 – Inadequate testbed resources is a significant schedule driver during V&V.**

Testbed resources for FM integration and test are often inadequate, and a number of workshop participants indicated that the shortfall is particularly problematic in the later stages of system development. Often, the I&T of FM logic must wait until all other aspects of system hardware and software are in place. Resources for early checkout of FM logic prior to or in addition to full-scale spacecraft testbeds would be extremely desirable.

***Recommendation 11: Develop high-fidelity simulations and hardware testbeds to comprehensively exercise the FM system prior to spacecraft-level testing.***

A crucial element of the FM V&V process, testbed resources and simulation fidelity must be adequate to perform pre-flight testing. Workshop recommendations related to testbeds included:

- 1) Testbeds must be kept current with changes to the flight vehicle. While use of testbeds developed for similar vehicles is prudent, they must be made compatible with the key parameters of the new vehicle.
- 2) The fidelity of each testbed and simulation and the specific fault cases to be tested should be clearly defined on the basis of mission phase, not globally for the mission.
- 3) Stress testing is important and should be a required part of the V&V program. Stress testing in flight-like scenarios can help to ensure system robustness and mitigate risk in single-string architectures.
- 4) Design validation should be performed independently from the designers to capture any inherent flaws or systemic errors. Such independence is necessary to avoid a repeat of flawed logic, or erroneous analysis or assumptions.
- 5) Evaluate FM test suite quality by assessing test coverage across subsystems and mission phases. No single mission phase or subsystem is sufficient to characterize system FM.
- 6) Always consider operations when defining the I&T environment and flow to ensure that the testing limits are necessary and sufficient to cover the environment to which the vehicle will be exposed in space. Early involvement of operations personnel in V&V is necessary to assure that stress levels are appropriately defined.
- 7) Assume that failures will occur in FM testing, and assure that the test plans include recovery procedures. This will ensure that anomalies and failures are appropriately adjudicated during testing.

**FINDING 12 – Organizations have different and sometimes conflicting institutional goals and risk postures that drive designs, architectures, and V&V plans in different directions, causing friction between customers and contractors.**

There are factors that drive FM architecture decisions and designs that vary between organizations and are not explicitly documented or taken into account in the development process. These factors may include institutional fears, heritage principles, heritage architectures, and high-level requirements for an FM response time in resuming normal mission operations. This may cause conflicts where there is shared design responsibility, and the lack of traceability to design principles prevents application of lessons learned to the next mission.

The conflicts typically arise from the organizations' different approaches to risk. The workshop participants discussed projects where a differing interpretation of a single fault tolerance policy caused friction between the contractor and NASA during FM system implementation. For example, the contractor planned to protect against the most probable failures, while the NASA approach was to design for all possible failures. For V&V, NASA tends to devote more resources to system level testing than industry might expect, performing extensive scenario testing for more rigorous validation of the system design. The different risk postures may be manifested in review findings, which may impose unexpected FM requirements on projects. These conflicts were most prevalent in areas of the design where organizations with differing approaches attempted to share design responsibility.

***Recommendation 12: Collect and coordinate FM assumptions, drivers, and implementation decisions into a single location that is available across NASA and industry. Utilize this information to establish/foster dedicated FM education programs.***

To provide a more complete view of the trade space and to enable more educated decisions for future projects, NASA and industry would benefit from establishment of a repository of requirements, driving factors, and implementation decisions for use by future FM architects. From this background information, an established vocabulary, suggested representation approaches, and a list of design principles utilized on prior missions could be derived. Each principle should be presented with an associated rationale statement, consequences (pro and con) of adopting the principle, and example implementations of this principle on past missions. This information would provide a basis for training material for educating future FM engineers. (See Recommendation #2b.)

#### **IV. Plans for Future Work**

NASA was successful in assembling a set of 100 FM professionals from across government and industry willing to share FM success factors and lessons learned, despite the need to safeguard proprietary information. Now, NASA is moving forward with a plan to implement the Workshop Recommendations through multiple avenues – see Figure 2.

First, NASA will develop an Agency-wide FM Handbook to help future programs by standardizing FM terminology, providing common representation techniques for expressing FM architectures and designs, and capturing FM design guidelines. Establishment of a shared lexicon and common practices within an engineering discipline is typically aided or enforced by the existence of engineering standards or handbooks. These documents define for the discipline the basic elements that do not change from organization to organization or from project to project. Those elements that do change are usually relegated to organization-specific or project-specific plans and procedures. Federal policy<sup>2</sup> mandates the use of industry standards instead of developing equivalent government (e.g., NASA) standards where the existing industry standards are adequate.

However, no NASA or industry standards or handbooks exist that would serve to provide a common base for interoperability, capture lessons learned and new technology, and facilitate engineering excellence in the field of FM engineering. Preparation of a NASA FM engineering handbook has been initiated, and will document an agreed upon lexicon and a set of design principles, and describe representation techniques that can be used on future missions to capture and review FM architectures and designs.

Second, concurrent with work on a handbook will be the establishment of a NASA Fault Management Working Group. The NASA Chief Engineer has endorsed plans to create a Fault Management Working Group (FMWG) within his Office to lead follow-on activities directly impacting future projects. NASA Center representatives will be chartered to explore areas of agreement or common interest and advance the state of FM practice. Improved mutual understanding of the different FM philosophies would be particularly beneficial for programs like Constellation, where systems designed by different NASA Centers and contractors must be interoperable. The FMWG's charter will be to provide projects with the ability to develop effective FM systems, for NASA spacecraft to manage faults, and for the FM community to collaborate effectively. Activities will include identifying FM metrics to enable cost and risk estimations, establishing a process to train personnel and fostering education programs to generate a pipeline of future FM engineers. The FMWG will work with the Software Working Group and the Systems Engineering Working Group to coordinate activities and identify issues that cross disciplines.

Third, although the focus of this NASA initiative has been on FM for unmanned missions, especially deep-space missions, FM is also an issue for human spaceflight programs managed by the NASA Exploration Systems Mission Directorate (ESMD). ESMD recognized that the FM issues captured during Workshop are not SMD-specific. The Constellation Chief Architect chartered a Fault Management Assessment and Advisory Team to assess and advise the Program on FM designs, V&V approaches, processes and organization. The NASA/Caltech Jet Propulsion Laboratory has been leading this work to characterize the FM engineering practices in use by the Constellation Program.

Finally, NASA is considering sponsoring a follow-on workshop to identify solutions to the issues raised in the first workshop, and/or to reach out to a broader community to learn from other industries such as nuclear and aeronautics, and find synergy among these diverse yet similar fields.

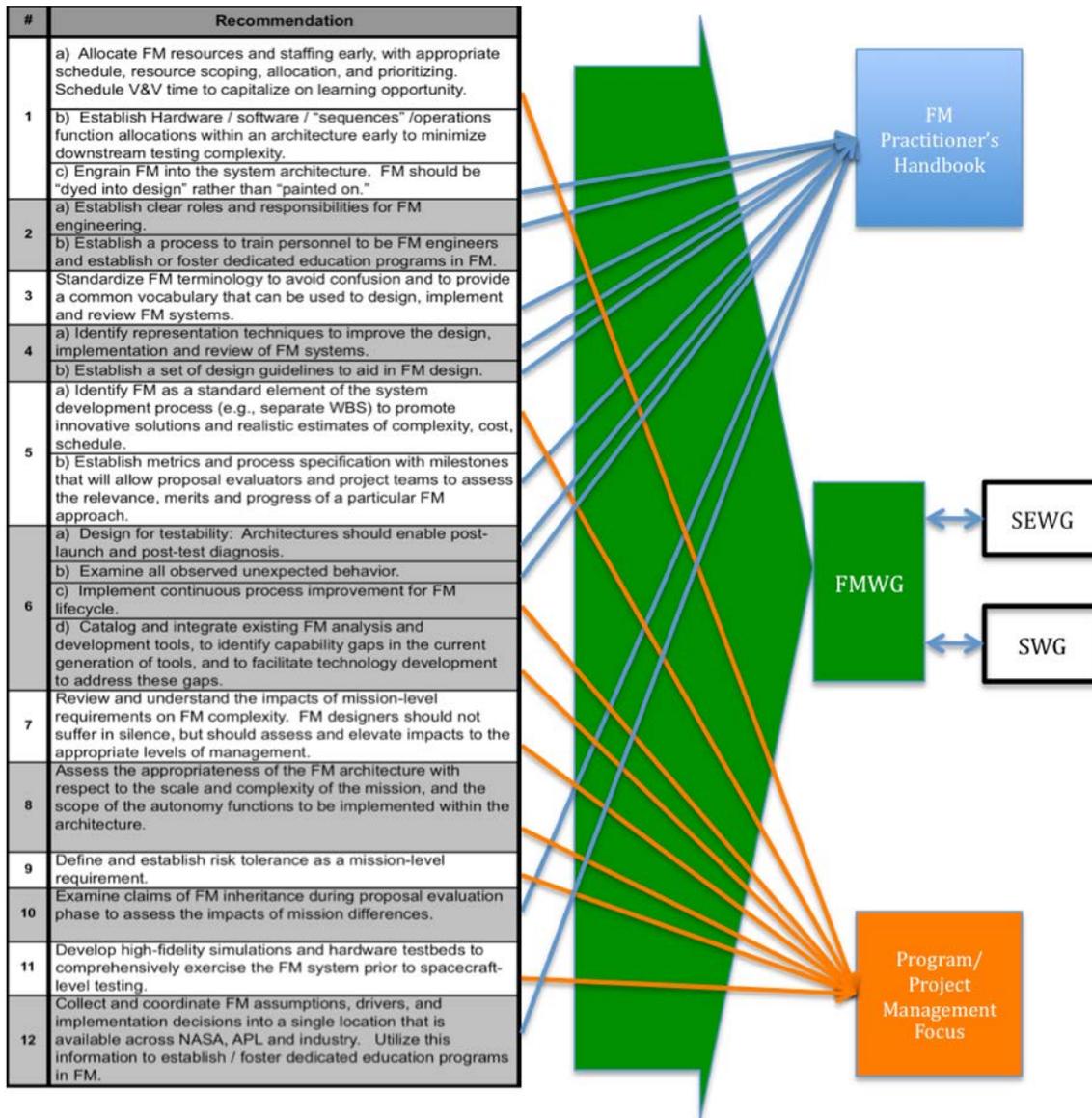


Figure 2 -- Disposition of FM Workshop Findings

## V. Conclusion

Fault Management is a critical spaceflight function, and design and implementation of the FM system is a major cost and risk driver for spaceflight missions. Flight projects in their early phases consistently underestimate the FM challenges that will be faced, and the FM resources that will be required, during flight system I&T and during operations. FM is not universally recognized as either a separate engineering discipline or a separate spacecraft subsystem, and FM is often given inadequate consideration when flight system design decisions are made. Evidence

of pervasive architecture, design, and verification and validation (V&V) problems with NASA FM engineering has been revealed both during technical reviews of spaceflight missions and in flight.

The April 2008 Spacecraft Fault Management Workshop represents the first time government and industry designers of spacecraft FM have been brought together to characterize FM practices, identify trends, and provide a roadmap for improvements. The workshop was very successful in drawing appropriately qualified key personnel from across government and industry, and in characterizing a set of root FM design and implementation problems shared across the earth-orbiting and deep-space spaceflight communities. A set of twelve (12) key findings and associated recommendations were distilled from extensive analysis of workshop proceedings, including presentations, meeting notes, and surveys.

It is clear from the workshop results that spacecraft FM designs have provided adequate in-flight performance. FM design flaws have caused some problems during flight system V&V and during operations, but have not adversely impacted mission success. But endemic FM engineering problems cause disruptions to flight system design and test, significant project cost growth, unplanned spacecraft operational constraints, and in-flight anomalies and failures. The ability to manage in-flight faults does not seem to be limited by FM technology maturity, but rather by flight programs and flight system designs that place insufficient emphasis on FM, and by a poorly disciplined approach to FM design and implementation. Addressing these system engineering process problems is a prerequisite to development of advanced FM systems that can meet the requirements of future spaceflight missions.

### **Acknowledgments**

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

### **References**

<sup>1</sup>Fesq, L. M., "White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate, Planetary Sciences Division," March 2009.

<sup>2</sup>OMB Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," U.S. Office of Management and Budget, February 10, 1998.