V&V of Fault Management: Challenges and Successes

Lorraine M. Fesq[1]
Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109

Ken Costello[2] and Don Ohi[3]
NASA Independent Verification and Validation Facility, City, State, Zip Code

Tiffany Lu[4]
TASC, City, State, Zip Code

and

Marilyn Newhouse[5]
CSC/NASA Marshall Spaceflight Center, Huntsville, AL, 35812

This paper describes the results of a special breakout session of the NASA Independent Verification and Validation (IV&V) Workshop held in the fall of 2012 entitled "V&V of Fault Management: Challenges and Successes." The NASA IV&V Program is in a unique position to interact with projects across all of the NASA development domains. Using this unique opportunity, the IV&V program convened a breakout session to enable IV&V teams to share their challenges and successes with respect to the V&V of Fault Management (FM) architectures and software. The presentations and discussions provided practical examples of pitfalls encountered while performing V&V of FM including the lack of consistent designs for implementing faults monitors and the fact that FM information is not centralized but scattered among many diverse project artifacts. The discussions also solidified the need for an early commitment to developing FM in parallel with the spacecraft systems as well as clearly defining FM terminology within a project.

I. Introduction

NASA goals for space exploration are driving increases in the capability, complexity, and robustness of the space systems being developed and deployed. The increase in system capability and complexity directly drives the capability and complexity of the associated processes required to predict, detect, diagnose, prevent, and respond to abnormal or failure conditions: Fault Management (FM). In turn, increases in FM capability and complexity drive development cost and schedule growth.

NASA's activities to understand and manage the factors affecting cost and schedule growth in the FM discipline are documented in the reports for two FM Workshops held in 2008[1] and 2012[2]. The 2008 FM Workshop documented several key findings and defined a path forward for maturing the FM discipline. One of the highlighted areas was the Verification and Validation (V&V) of FM capabilities. The challenges identified for V&V systems included guaranteeing adequate coverage and understanding what constitutes completeness for verification of complex FM systems, as well as inadequate resources and incomplete understanding of the FM system and the full complement of interactions with nominal functioning of the vehicle hardware and software. In other words, V&V of FM capabilities is where "the rubber hits the road."

---

[1] Deputy Chief Technologist, Systems Engineering and Formulation Division, AIAA Senior Member.
[2] Insert Job Title, Department Name, Address/Mail Stop, and AIAA Member Grade for second author.
[3] Insert Job Title, Department Name, Address/Mail Stop, and AIAA Member Grade for third author.
[4] Insert Job Title, Department Name, Address/Mail Stop, and AIAA Member Grade for fourth author.
[5] Principal Lead Systems Engineer, MSFC/EO50.

To further explore the V&V challenge, a special Breakout Session titled "V&V of Fault Management: Challenges and Successes" was organized at the NASA Independent Verification and Validation (IV&V) Workshop, held in Morgantown, West Virginia on September 12, 2012. The IV&V Program is in a unique position to interact with projects across virtually all of the NASA development domains. Its unique cross-agency role offers opportunities to capture and document Fault Management (FM) approaches across the diverse set of NASA development projects, leading to a better understanding of how FM concepts, principles and architectures are applied throughout NASA. These opportunities provide the possibility for the IV&V Program to uncover common challenges and to provide recommendations that will help move the FM discipline forward, benefiting not only the IV&V activities, but also FM approaches, processes and practices throughout a project's lifecycle.

The emphasis for the IV&V Breakout Session was to capture and share experiences in evaluating and assessing FM architectures on flight projects. FM is an important element of any space system since it is responsible for protecting the space asset and ensuring mission success even in the presence of faults. Because of this essential role, the portion of FM that is implemented in software, which can measure up to 50% of the total flight software size, is typically characterized as safety critical software; therefore, it is keenly scrutinized by a project's IV&V team. The goals of the Session were to:

- Convene engineers who have analyzed FM software on NASA's missions;
- Describe unique FM architectures and characteristics that made V&V challenging;
- Share approaches that were applied to analyze FM architectures, including insights on what worked, as well as what did not work;
- Capture Findings and Recommendations.

To motivate the discussion, a number of questions were posed, including "How are FM architectures developed, evaluated, verified and validated for a designated mission?" and "What techniques have proven effective in performing V&V on the FM portion of the FSW?" Participants disclosed details describing how the IV&V of the FM was performed. The following five presentations provided descriptions of FM IV&V[*] on different categories of NASA missions.

- Human-rated/long-duration: International Space Station (ISS)
- Planetary Lander/Rover: Mars Science Laboratory (MSL)
- Lunar/L2 Robotic: James Webb Space Telescope (JWST)
- Human-rated crew vehicle: Multi-purpose Crew Vehicle (MPCV)
- Earth Orbiter Robotic: Joint Polar Satellite System (JPSS)

These presentations promoted a great deal of discussion and interchange, and enabled the group to capture a number of findings and recommendations for future IV&V FM teams as well as for use within the greater FM discipline.

II. Themes and Recommendations

As a discipline within NASA, the IV&V approach to flight projects follows a consistent process to determine what portions of the FSW are analyzed as well as what analysis approaches are used (a risk-based assessment of the FSW is used in making this determination). This leads to a general set of goals with respect to performing IV&V on FM architectures and software that are consistent across each flight project. These goals strive to answer the following questions about the FM:

1) Does the software perform as required
2) Does the software not do what it is not supposed to do
3) Does the software behave acceptably under adverse conditions?

[*] It is important to note that IV&V and V&V technical tasks are often quite similar in nature. The primary difference is in the independence of the organization performing the task. IV&V tasks are generally performed by an organization wholly independent from the development project (technically, managerially and financially) while the V&V team is often some organizational unit of the development project. So the lessons learned and best practices of an IV&V organization are directly applicable to a V&V organization.

The following common themes, IV&V challenges, and recommendations emerged during the presentations as the teams described the work performed to answer these questions.

1) **FM is a critical element of NASA's flight systems.**

As spacecraft travel deeper into space on longer missions, the ability of the spacecraft to deal with hardware as well as software failures increases dramatically. Robotic flight systems must be able to independently react to faults in order to safe the vehicle while waiting for human intervention. For critical events, the systems may need to respond to faults in a manner that does not result in a fail-safe state, but rather a fail operational state where the mission continues without human intervention. In systems where there is a local human presence, the importance of the FM approach changes to include keeping the humans alive as well as keeping the system operational. Overall FM concepts play an important role in helping the system respond to unexpected events while striving to meet the mission goals.

2) **Current IV&V approaches for FM to date have dealt only with spacecraft.**

FM as a discipline has broader coverage than space systems, including the system health of fixed wing and rotor wing aircraft. FM applies across other domains as well as other disciplines within system development. While there was no specific mission dealing with these domains in the breakout session, it was a point of discussion that the findings applied to those domains and their missions as well as the domains discussed at the breakout session.

3) **IV&V is still in a learning phase (as are many developers)**.

A valuable outcome of the breakout session was exposing different IV&V teams to the characteristics of different development projects as well as sharing approaches to performing IV&V analysis tasks with respect to FM. This sharing of information demonstrated that there is much to learn, not only from how FM is being designed and implemented on development projects, but also how to analyze these FM approaches in a manner that generates a sufficient body of evidence to demonstrate that the FM approach supports the success of the mission.

Current V&V analysis methods are often focused in a localized way, that is, at the subsystem level and lower. In order to fully develop evidence about the fitness of the FM approach, V&V analysis needs to also include assessments of FM at an integrated level focusing on understanding the impact of fault responses across the system and its subsystems and components.

In addition, dynamic analysis is needed to understand complex interactions. The growing complexity of NASA systems often makes it impossible to analyze them in a static manner, without making use of dynamic analysis tools. This is especially important with respect to trying to understand the impact of fault responses on the system and its components.

4) **Mission domains had similar approaches to architecting FM.**

While one aspect of the session was an understanding of the different approaches to dealing with FM by the IV&V teams, there are also several common FM architectural concepts identified across the missions including:

a) Detections/monitors – Fault/failure detection mechanisms, typically referred to as "monitors," is distributed throughout the system. For example, TMON[††] is a detection mechanism used on numerous Earth-orbiting satellites.
b) Persistence – Detection mechanisms include persistence counters to avoid tripping due to noise. For example, for the Jump Limit Check, the flight software shall declare the current time to be invalid if the difference between the current time and the previous valid time is greater than the specified upper limit for a persistence of five consecutive times.
c) Responses – Fault responses are pre-determined. Local responses are distributed throughout the system. For example, when the Under-Voltage Level trips, the flight software shall transition to Safe-Hold Mode.
d) Levels/tiers – Most systems have local-level FM and system-level FM. Some have multiple tiers such as individual subsystem-level zones of control. Detection often is at the lowest level, and responses

[††] TMON is a GSFC Telemetry Monitoring tool.

are at the lowest level if the response is entirely local. Alternately, if a response involves commanding across subsystems, it is handled by system-level FM software.

e) Priorities – Many systems introduce a prioritization of faults. If a lower-priority fault is detected and a response is activated, a higher-priority response could interrupt the lower-priority response. This includes not just if one fault is more important than another but also overall prioritization of processes within the system and balancing them against the FM processes. This would cover questions such as handling concurrent faults in a single subsystem, dealing with concurrent faults across subsystems, and dealing with faults (possibly one or more) occurring during critical mission events/phases. For example, a response to a power monitor may be assigned a higher priority, and therefore interrupt a lower priority attitude response.

f) Detection-response relationship – There usually is a many-to-one relationship between fault detections vs. fault responses; i.e., multiple detection mechanisms can be tied to the same response. For example, a processor fault may be due to a hardware bus error or a software exception, both of which will result in a processor exception that is trapped by the kernel, causing a processor reset.

5) **FM development was instituted late in the overall development life cycle**.

Projects are most successful when the FM architectural strategies, design principles, and patterns are specified up front. A lagging FM definition introduced numerous challenges not only for the projects' IV&V teams, but also for the development teams. When the design of the FM system is delayed, FM must accommodate the existing, nominal system design, leaving little-to-no room for subsystem or system design changes that would benefit FM. The delayed approach introduces complexity by yielding patchwork architectures that are difficult to verify. FM designs are harder to analyze since they are devised bottoms-up to respond to individual faults, instead of a top-down, architected and systematic approach. It also forces the IV&V team to delay FM analysis activities until late in the project, when deadlines are looming and many additional artifacts such as test procedures and reports require the team's attention.

Although it is true that some definition of the nominal system design is required before all FM needs are known, it is not true that the FM architecture needs to be delayed. Assessing FM drivers early in a project life cycle allows the IV&V Team, as well as the development team, to reason about the planned FM approach. Some of these early drivers of FM approaches are:

- Mission characteristics
- Required fault tolerance
- Unattended operations requirements
- Redundancy requirements
- Early FM framework

For example, on one project, a monitor design pattern was introduced late in the project. All monitors implemented after that point followed the design pattern and were easy to identify and analyze. However, a number of monitors had already been implemented in an ad hoc fashion by the time the design pattern was established. These early monitors were grandfathered in, making them difficult for the IV&V Team, as well as the development team, to identify and analyze.

In addition to an early start, the Projects and the IV&V Facility would benefit from focusing on and monitoring the FM design throughout the lifecycle. One way to accomplish this is to evaluate FM requirements, architecture and designs at major milestone reviews, posing questions such as the following:

- System FM should be a special discipline of system engineering. Is there a FM engineer identified on the program? <Mission System Readiness Review question>
- Does the contract properly define the FM requirements and flow down to subsystem? <Mission System Readiness Review question>
- Is the FM architecture defined? <Mission Preliminary Design Review question>
- How does the FM architecture help developers avoid coupling, race conditions, and retriggering FM responses already in progress or already executed? <Mission Preliminary Design Review and Critical Design Review question>
- Are the system-level and local-level FM detailed-designs defined, including coding patterns and hardware vs. software dependencies? <Mission Critical Design Review question>

- Are the test plans and test procedures properly traced to system FM requirements? < Mission Assembly Test and Launch Operations Review or System Integration Review question>
- Are there test reports for all system FM testing? <Mission Pre-Ship Review question>

6) **Complexity of systems and changing mission requirements are driving the need for more and better FM architectural strategies, design principles and patterns.**

While applicable at the lowest levels of the system, FM at its core is a systems engineering discipline that needs to be consistently implemented from the system level downward. The interactions between system components is growing and introducing increased complexity. Agency goals for exploration drive the required capabilities of the systems being developed. The ambitious nature of these goals requires systems to have more robust and capable features, which in turn drives the need for more robust and capable FM products. This is especially true with respect to human-rated systems as the longer humans remain in space the more capable the system needs to be. This increased capability is reflected in more advanced system features many of which are software controlled. Software now has become the provider and controller of just about all of the critical behaviors of the systems NASA builds. This increasing role of software leads to more hardware and software interactions between the components, which increases the complexity of the system. This is a characteristic of systems that are being built to achieve more challenging goals.

The IV&V Facility and development projects would benefit from NASA guidelines on designing, developing, testing and operating FM for different categories (e.g., human-rated vs. robotic, Earth-orbiting vs. deep space) and classes (class A-D) of missions. For example, a guideline to establish FM as a discipline on a mission would promote that FM information be organized and centralized instead of scattered throughout various documents and artifacts. This would also facilitate a cohesive, system-wide view of all of the FM elements implemented throughout a spacecraft, which would benefit not only the IV&V activities, but also the spacecraft design, implementation, test and operations efforts. Since FM and hazard controls often overlap, FM guidelines would also support assurance of system safety. Guidelines would allow IVV analysis efforts to better align with project tasks.

7) **The interactions between different FM tiers in the system generate complexity.**

Systems that have local and system responses introduce separate zones of FM control that could conflict with one another. Normal IV&V lifecycle analysis methods (requirements, design, code and test analyses) perform reasonably well for local FM detection and response mechanisms. However, when viewed at the system or even the subsystem level where responses can be dependent on spacecraft state or modes, the layers of FM control structures introduce the potential for race conditions between concurrent FM responses. As a result, special analyses are needed to verify complex, integrated FM systems.

To mitigate this concern, the team recommended that projects ensure FM requirements, both hardware and software, are identified and allocated down to the appropriate project level (e.g., Level 4 requirements address specify priorities and tiers, and Level 5 requirements address specify thresholds and persistence). In addition, if the FM design follows a traditional monitor-response approach, ensure that FM requirements address the following attributes:

- Detections/monitors
- Persistence
- Responses
- Levels/tiers (if applicable; e.g., system-level vs sub-system level)
- Priorities (if applicable)
- Detection-response relationship (one-to-one, one-to-many, many-to-one)

8) **FM requires a system perspective.**

FM is not merely a subsystem responsibility. It requires a system perspective in understanding responses to faults, and the potential for interactions between fault responses, as well as how a response may affect other processes in the system. FM engineering is often done at the subsystem level since the objective is to detect and respond to faults at the lowest possible level. However, when FM is designed at the subsystem level, a system-wide view of fault behavior and response interactions becomes very challenging.

To understand FM at the system level, a comprehensive view of faults must be captured, which enables the analysis of end-to-end responses. When prioritization is introduced, IV&V's role becomes much more complex due to the need to understand the potential interrupts and interferences among the responses. As NASA's space systems become more capable, dynamic analyses are needed to understand complex interactions introduced by the possibility for multiple FM actions that could interfere or conflict with one another in response to faults.

9) **FM information is not centralized, but often is scattered among many diverse project artifacts.**

Projects typically do not have a single, consolidated FM design specification from the system level down to the hardware and software. Consequently, IV&V must search through a wide array of artifacts to piece together a comprehensive view of FM. Since the information is not captured in a systematic fashion, it is often not consistent or cohesive across the artifacts. For example, low-level FM behaviors are sometimes added during the design phase, and are not fed back into the requirements specifications.

Successful solutions to FM V&V are using some form of a model to represent end-to-end FM detection mechanisms and responses. These models may be as simple as a spreadsheet, or as elegant as a relational database, and offer the following verification benefits.

- Facilitates the ability to support top-to-bottom consistency checking throughout the lifecycle artifacts; i.e., component, subsystem and system level checks within the requirements, design, and code artifacts;
- Enables querying to ensure constraints are met universally;
- Provides a systematic approach to manage and track FM data across disparate sets of artifacts.

Another reoccurring theme in the presentations was the difference in terminology across artifacts within a development project. This usually occurred across subsystems and components due to development by different contractors. The lack of a common language creates additional complexity since terms may be interpreted differently from one part of the system to another, leading to the implementation of incorrect behaviors. Establishing a standardized set of terminology as well as defined architectural strategies, design principles and patterns within NASA would help to simplify these complex interactions.

III. Conclusion

This paper summarizes key themes and recommendations from a special Breakout Session at the 2012 NASA IV&V Workshop titled "V&V of FM: Challenges and Successes." The IV&V Workshop offered an opportunity to familiarize members of the IV&V community with the ongoing activities to develop FM as an engineering discipline and in turn for members of the IV&V community to share experiences in verifying and validating the critical FM software on NASA's missions. The shared experiences tied directly to the goals for improving the practice of FM within NASA, including the need for early commitment to developing FM in parallel with the spacecraft systems, and to clearly define FM terminology within a project. The discussions also provided additional practical examples of pitfalls encountered during FM IV&V, such as the lack of consistent designs for implementing fault monitors, and the fact that FM information is not centralized, but often is scattered among many diverse project artifacts. If these pitfalls are rectified and factored back into the development process, the improved practices should facilitate the IV&V process and reduce the incidence of errors detected during IV&V. The IV&V Facility is still in a learning phase for analyzing FM systems; however, this Breakout Session exposed common challenges and solutions that IV&V Teams are experiencing when verifying and validating FM software on multiple NASA projects and their applicability to developing FM as a mature engineering discipline.

Acknowledgments

We gratefully acknowledge the support of the NASA IV&V Program for hosting this breakout session at their annual IV&V Workshop. We also acknowledge the support of the IV&V teams that participated in the forum including the International Space Station, Mars Science Laboratory, James Webb Space Telescope, Multi-purpose Crew Vehicle, and the Joint Polar Satellite System.

Part of 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

[1]Fesq, L., Cancro, G. Jones, C., Ingham, M., Leitner, J., McDougal, J., Newhouse, M., Rice, E., Watson, D., Wertz, J., "Spacecraft Fault Management Workshop Results for the Science Mission Directorate, Planetary Sciences Division," March 2009

[2]Fesq, L., Fretz, K., Newhouse, M., Report on the 2012 NASA Spacecraft Fault Management Workshop," February 2013