FAULT MANAGEMENT ARCHITECTURES AND THE CHALLENGES OF PROVIDING SOFTWARE ASSURANCE

Shirley Savarino
TASC, shirley.savarino@tasc.com

Rhonda Fitz
MPL, rhonda.s.fitz@ivv.nasa.gov
Lorraine Fesq
JPL/Caltech, lorraine.m.fesq@jpl.nasa.gov
Gerek Whitman
TASC, gerek.whitman@tasc.com

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.

ABSTRACT

Fault Management (FM) is focused on safety, the preservation of assets, and maintaining the desired functionality of the system. How FM is implemented varies among missions. Common to most missions is system complexity due to a need to establish a multi-dimensional structure across hardware, software and spacecraft operations. FM is necessary to identify and respond to system faults, mitigate technical risks and ensure operational continuity. Generally, FM architecture, implementation, and software assurance efforts increase with mission complexity. Because FM is a systems engineering discipline with a distributed implementation, providing efficient and effective verification and validation (V&V) is challenging. A breakout session at the 2012 NASA Independent Verification & Validation (IV&V) Annual Workshop titled "V&V of Fault Management: Challenges and Successes" exposed this issue in terms of V&V for a representative set of architectures.

NASA's Software Assurance Research Program (SARP) has provided funds to NASA IV&V to extend the work performed at the Workshop session in partnership with NASA's Jet Propulsion Laboratory (JPL). NASA IV&V will extract FM architectures across the IV&V portfolio and evaluate the data set, assess visibility for validation and test, and define software assurance methods that could be applied to the various architectures and designs. This SARP initiative focuses efforts on FM architectures from critical and complex projects within NASA. The identification of particular FM architectures and associated V&V/IV&V techniques provides a data set that can enable improved assurance that a system will adequately detect and respond to adverse conditions. Ultimately, results from this activity will be incorporated into the NASA Fault Management Handbook providing dissemination across NASA, other agencies and the space community. This paper discusses the approach taken to perform the evaluations and preliminary findings from the research.

INTRODUCTION

Fault Management capability is consistently viewed as essential for space mission success, and is typically assessed at a high criticality level by NASA IV&V projects. Every mission, however, has a unique approach to designing and architecting a FM system, resulting in unique challenges to providing assurance. During the 2012 NASA IV&V Annual Workshop, this problem was exposed in a breakout session entitled "V&V of Fault Management: Challenges and Successes,"[1] which prompted discussion between IV&V analysts and JPL researchers about the variety in FM architectures and the techniques, both successful and unsuccessful, that IV&V analysts use to generate evidence-based assurance for mission critical software. A need for further investigation became

apparent, and in answer to this need, a SARP research initiative was proposed, accepted, and launched at NASA IV&V in October 2014. The proceedings and preliminary products of this initiative are the subjects of this paper.

This paper is presented in two parts. Following a brief introduction to the NASA IV&V Program and the NASA Fault Management Handbook, the general philosophy and methodology of NASA IV&V is presented, including an overview of Assurance Strategy and FM criticality. This section provides the context necessary to understand the subsequent description of the FM Architectures SARP initiative, its methodology, and the selection of data provided.

NASA Independent Verification and Validation Program

NASA's IV&V Program was established in 1993 as part of an Agency-wide strategy to provide the highest achievable levels of safety and cost-effectiveness for mission critical software. NASA's IV&V Program was founded under the NASA Office of Safety and Mission Assurance (OSMA) as a direct result of recommendations made by the National Research Council (NRC) and the Report of the Presidential Commission on the Space Shuttle Challenger Accident.[2]

NASA's IV&V Program has a primary business focus to support NASA missions. The Program takes a systems engineering approach to enable efficient, cost-effective IV&V services through the use of broad-based expertise using adaptive engineering best practices and tools. NASA's IV&V Program performs analysis throughout the software development lifecycle resulting in objective evidence that provides a level of assurance that system software will operate reliably and safely. This evidence may be obtained using various techniques, including but not limited to; analysis of flight software, ground software, mission operations, embedded systems, and scientific applications as well as modeling and software simulations.

NASA Fault Management Handbook (NASA-HDBK-1002)

In 2012, NASA released a draft FM Handbook[3] in an attempt to coalesce the field by establishing a unified terminology and a common process for designing FM mechanisms. However, FM approaches remain very diverse across NASA, especially between different mission types such as Earth orbiters, launch vehicles, deep space robotic missions, and human spaceflight missions. The FM Handbook authors were challenged to capture and combine all of these different views, and eventually recognized that a necessary precursor step was for each sub-community to codify its FM policies, practices and approaches in individual, focused guidebooks. By developing these guidebooks, sub-communities can then look across NASA to better understand different ways off-nominal conditions are addressed, and to seek commonality or at least an understanding of the various FM approaches. These guidebooks would then be inserted as separate chapters in the FM Handbook. The "Deep Space Robotic Fault Management" is the first guidebook currently under development, and will be posted to the FM Community of Practice on the NASA Engineering Network[4] website. Once each sub-community has codified its approach to FM, mission types will be surveyed to better understand the different ways off-nominal conditions are addressed across NASA. Identifying similarities and differences, seeking commonality, or at least garnering an understanding of FM approaches, will ultimately lead to a coalescence of the FM field, as directed by NASA's Office of the Chief Engineer. This FM Architecture SARP research initiative allows an early assessment from an architectural perspective with a software assurance focus to be developed and shared within the FM community.

NASA IV&V METHODOLOGY

NASA IV&V's methodology has three guiding principles in planning and performing analysis. They are: Criticality, the Three Questions (3Qs), and Assurance Strategy.

Criticality

IV&V performs a criticality analysis to build an understanding of the software being analyzed. This criticality analysis is a risk-based methodology which is performed on software behaviors and software entities. The analysis begins with a system decomposition of the primary behaviors and an architectural understanding of the software entities. Each behavior is assessed in terms of both the impact and likelihood of its failure. The results of this analysis are plotted on a 5x5 risk matrix and used to establish the criticality of the software and software interactions within the context of the overall system. This risk-based assessment feeds into the planning process described in the Assurance Strategy. Because Fault Management is associated with asset and human safety, this discipline typically is highly ranked in all of the NASA IV&V criticality analyses.

Three Questions

IV&V analysis is performed with the following perspectives described in IVV 09-1, the Independent Verification and Validation Technical Framework, known as the 3Qs[5]:

1. Will the system's software do what it is supposed to do?
2. Will the system's software not do what it is not supposed to do?
3. Will the system's software respond as expected under adverse conditions?

For the purposes of this activity, adverse conditions are any situations that cause an off-nominal behavior or response. Examining the third of the 3Qs is one of the major challenges of FM. How a system is architected to handle faults and adverse conditions is crucial for the manifestation of the functional and performance requirements for mission success. The 3Qs provide the perspectives to support Assurance Objectives and Conclusions as part of the Assurance Strategy.

Assurance Strategy

IV&V techniques involve defining an Assurance Strategy to support IV&V planning and execution. Illustrated in Exhibit 1, this strategy has three distinct phases utilizing both criticality and the 3Qs. The first phase involves understanding the risk posture of the software and the criticality of the software elements in performing desired behaviors. Once the risk posture is understood, Assurance Objectives are defined to assure the quality of the flight software for critical behaviors and entities in scope. In the second phase, the IV&V plan is developed to support assurance with objective evidence and documented assumptions. The plan is executed, using documented IV&V methods which result in issues or risks against the Assurance Objectives. The results of the IV&V effort allow Assurance Conclusions to be made in the third phase, communicating the assessment of the software. Assurance Conclusions are qualified based on the scope of the analysis, underlying assumptions, and so on. This process is iterated throughout IV&V lifecycle phases.

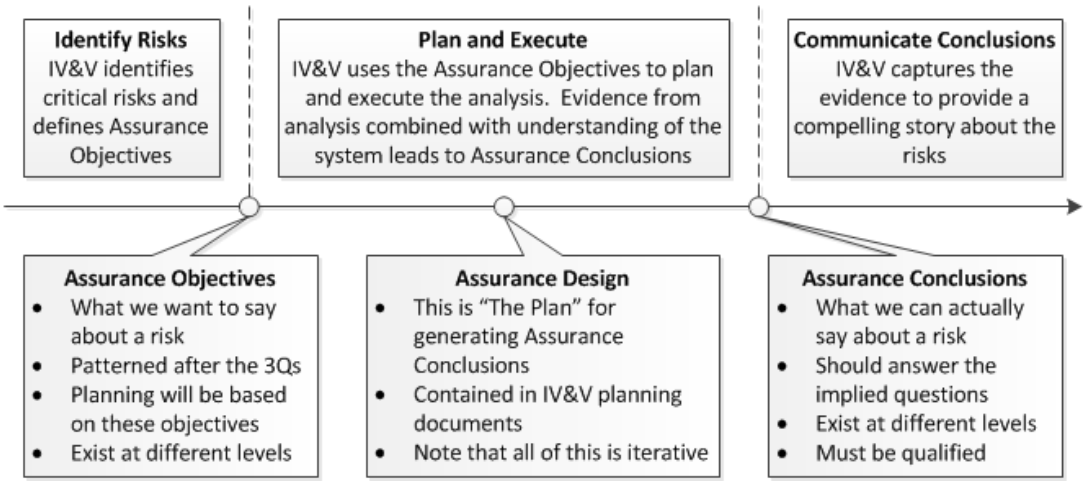

Exhibit 1: IV&V Assurance Strategy

A simplified example of an IV&V analysis on a deep space robotic mission illustrates the Assurance Strategy methodology. This example uses the Mars Science Laboratory (MSL), which successfully landed on Mars in 2012.

- **Identify Risks:** There are distinct project phases of launch: cruise; entry, descent and landing (EDL); and surface operations. During surface operations, the rover goes to sleep at night and performs a wakeup sequence every Sol (solar day on Mars). During the criticality analysis, the wakeup sequence was identified as critical.
- **Assurance Objectives:** For the wakeup sequence, the IV&V team defined the following Assurance Objective: "The Rover will always wake up in a safe configuration." Implicit in this Assurance Objective was the lack of emergent behaviors in the software (question 2 of the 3Qs), and appropriate failovers or recovery sequences if an adverse condition occurred (question 3 of the 3Qs).
- **Assurance Design, Plan and Execute:** To confirm the Assurance Objective, the team reviewed the requirements, design, code, and test documentation. Issues, with associated severity, were developed and potential risks were evaluated. For this activity, only low severity issues were submitted and no risks were identified.
- **Assurance Conclusions:** As a result of the IV&V analysis performed, the team could conclude that "The Rover will wake up in a safe configuration," from the perspective of all 3Qs.
- **Communicate Conclusions:** At the completion of the analysis, the Assurance Conclusion was communicated to the MSL project and other stakeholders.

SCOPE OF FAULT MANAGEMENT INITIATIVE

The FM Architectures SARP initiative involves investigating the varied approaches to FM across eight of the missions in the NASA IV&V project portfolio. The visibility across various projects and centers places the NASA IV&V Program in a unique position to support this objective. The goals of this initiative are to:

1) Extract FM architectures across projects in the IV&V portfolio.
2) Evaluate the data set for robustness, and assess the visibility of these architectures for validation and test.
3) Compile and assess IV&V and software assurance methods applied to the various architectures.

The scope of this initiative is limited to the selection of eight projects from the IV&V portfolio that represent a variety of architectures from the most critical and complex projects currently in development within NASA. The

assessment of software assurance methods is limited to those methods in use at the IV&V Program. Developer V&V methods or software assurance methods from other NASA programs are not included in this phase of the SARP initiative, though are a natural augmentation to the work performed on this initiative. Results will be incorporated into the NASA FM Handbook and have broad applicability to the FM community and other software assurance groups. The FM Architectures SARP initiative is summarized in Exhibit 2.

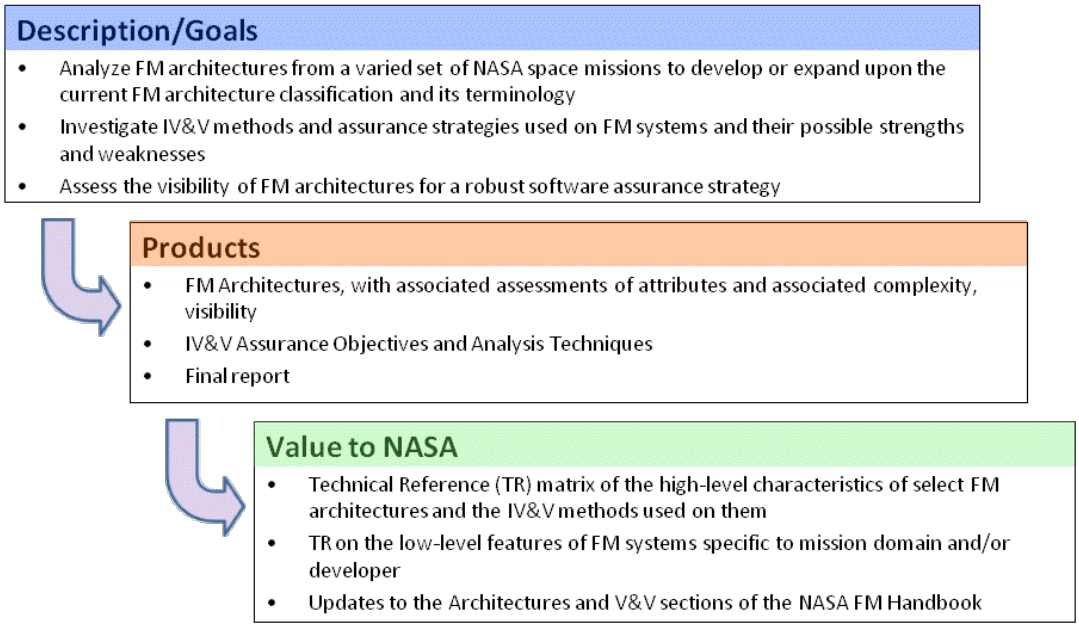

Exhibit 2: FM Architectures SARP Initiative

Currently, this effort has completed the FM survey of architectures and IV&V techniques implemented in the selected projects. Associated Assurance Objectives guiding analysis methods as well as Assurance Conclusions relevant to FM have been compiled as part of this effort. The approach taken to perform the evaluations and preliminary findings from the architecture surveys including IV&V statements of software assurance are described in the following sections.

SURVEY METHODOLOGY

The primary means of gathering data for the FM Architectures SARP research initiative was via survey and interview of FM subject matter experts (SMEs) representing the analysis teams for each IV&V project. This section gives a brief overview of the survey purpose and provides understanding of the type of information collected. The survey questions and subsequent interviews served two overall purposes: to gather data on each project's FM and the extent of the SMEs' understanding of the architecture, as well as to learn about the SMEs' approach to the IV&V analysis and associated Assurance Strategy. Each of these informational slices contributes toward the initiative's goal of assessing the visibility into the FM system needed in order to successfully provide software assurance and apply IV&V techniques to FM systems across the development lifecycle.

Eight NASA IV&V projects comprised the dataset evaluated as part of this effort. These missions were chosen for their diversity in order to best capture the variety in FM architectures currently in use. They span seven different primary developers, three broad categories of mission type, and a wide range of sizes and complexities. At the time of the survey, seven of the projects were undergoing analysis at the IV&V Facility, at various stages in their lifecycles, and one, MSL, was already in the operational phase and had no ongoing analysis. Exhibit 3 lists

each focus project surveyed for the initiative, including its mission type, consistent with those identified in the FM Handbook.

Name	*Mission Type*
Mars Science Laboratory (MSL)	Deep Space Robotic
International Space Station (ISS)	Human Spaceflight
James Webb Space Telescope (JWST)	Deep Space Robotic
Multi-Purpose Crew Vehicle Exploration Flight Test 1 (MPCV EFT-1)	Human Spaceflight
Joint Polar Satellite System (JPSS)	Earth Orbiter
Magnetospheric Multiscale (MMS)	Earth Orbiter
Geostationary Operational Environmental Satellite R-Series (GOES-R)	Earth Orbiter
Solar Probe Plus (SPP)	Deep Space Robotic

Exhibit 3: Overview of Focus Projects chosen for the Fault Management Survey

The IV&V Program hosts a Fault Management Community of Interest (FM CoI) to share best practices and lessons learned across the Program. SMEs from the FM CoI agreed to participate in the research supporting this initiative, and the FM CoI has contributed to the data analysis and peer review process. The CoI additionally serves as a platform through which findings and recommended practices are disseminated. FM survey questions for SMEs were generated and revised as further considerations emerged during interviews. The final set consisted of thirty-five FM architecture and nine IV&V methodology questions. The large majority of survey questions address the characteristics of the FM architectures in order to differentiate and delineate FM systems. Described in Exhibit 4, these questions were grouped into four categories: Structure, Concept, Implementation, and Other Architecture-Related Questions. Together, these questions and the additional insight gained from discussions held during interviews provide preliminary insight into each FM system and its architecture.

Category	*Description*
Structure 7 questions	Obtain a high level view of each architecture, and provide insight into size, complexity, and scale. • Address the structure and organization of the FM architecture. • Characteristics such as centralization or distribution, tiers of operation, interdependency, modifiability, and implementation within the overall flight software are addressed.
Concept 10 questions	Addresses the design process and major design ideas and themes of the FM architecture. • Considerations such as fault analysis, automation, mission phases, fault definition, redundancy, and fail-safe/fail-operational modes are addressed. • Establish a broad view of how the FM system is intended to accomplish its objectives, and why it is designed and structured in the way it is.
Implementation 13 questions	Technical implementation detail about how the FM architecture was built and how it works. • Number of monitors and responses, false positives and persistence, fault isolation, simultaneous responses, and subsystem inter-communication are examples of the low-level characteristics covered by this section. • Capabilities that some architectures have but others do not are important to uncover in order to help categorize and label the architectures as well as reveal potential strengths and limitations of various FM architectures.
Other Questions 5 questions	• This was the catch-all section for things the other questions may not have entirely covered • This section contained questions involving heritage and mission parameters in order to provide some additional context to frame the rest of the responses.

Exhibit 4: Survey: Architecture Questions

The nine survey questions associated with IV&V analysis performed are shown in Exhibit 5.

Survey: IV&V Analysis Questions
• What were the key drivers to IV&V on this project?
• What were the critical errors that IV&V was focused on assuring against?
• What other Assurance Strategies were involved in the IV&V of this project?
• What kinds of artifacts did you get from the developer to use in the analysis, and how did the types of artifacts you received affect your analysis?
• Were there types of artifacts you did not receive or the developer did not generate that would have made analysis easier/faster/more complete?
• What kinds of technical reference(s) did you generate during your analysis?
• If the FM system was inherited or standardized, how did this influence your analysis?
• What language was used to write the FSW? How did this choice in language make analysis easier/more difficult?
• What was the highest benefit analysis? In retrospect, were there things you or the IV&V team would or should have done differently?

Exhibit 5: Survey: IV&V Analysis Questions

Querying IV&V SMEs about the IV&V projects' FM architectures provided an ability to glean metadata related to architectural attributes as well as their knowledge of the FM system. The purpose of this metadata was not to judge or evaluate the SMEs' understanding, but rather to investigate visibility of the FM architectures. For example, if a SME was unable to provide an answer to a question on the survey, additional discussion was warranted for clarification. Was the question unclear? Did it not apply or was it impossible to answer for this particular project? Was there information about the architecture the SME was lacking due to unavailable artifacts, an incomplete assessment, the topic being out of scope, or some other reason? Each of these explanations was valuable in a different way, potentially to refine the survey, advance understanding of the project's parameters, or indicate a lack of visibility. In addition to time and effort savings, conducting interviews rather than merely combing through design documents to find information enabled insight into the complexity of FM systems and the challenges in developing an appropriate IV&V Assurance Strategy.

The IV&V SME interviews also collected information related to analysis performed via the IV&V analysis questions and collected FM Assurance Objectives and Assurance Conclusions. Confirmations of objectives, or limitations that were encountered via issues or risks, and assumptions made in the analysis process were captured in Assurance Conclusions. The intent was to use these assurance products to gain further insight into the purpose, techniques, and effectiveness of IV&V analysis being performed. The aggregate set of Assurance Objectives and Conclusions becomes a technical reference for future IV&V activities associated with Fault Management.

IV&V FAULT MANAGEMENT ASSURANCE OBJECTIVES AND CONCLUSIONS

Exhibit 6 contains a set of Assurance Objectives and Conclusions collected from the IV&V projects, correlated with the lifecycle development phase. This provides an understanding of the objectives of IV&V analysis at each phase of project development. Each statement is mapped to one or more of the 3Qs of IV&V analysis.

Assurance Objectives or Conclusions	*Mission Type*	*3Qs Mapping*
Concept Phase		
"The Hazards Report documents all known software-based hazard causes, contributors, and controls."	DSR	Q3
"The Hazards Report documents all known software-based hazard causes and contributors."	DSR	Q3
"For each software-based hazard cause, a hardware control inhibit is adequately identified."	DSR	Q3
"With one exception, the Hazards Report documents hardware control inhibits for each software-based hazard cause."	DSR	Q3
Requirements Phase		
"The system fault management requirements are of high quality and are consistent with acquirer needs as they relate to the system's software."	DSR	Q1
"The L4 Autonomy Subsystem requirements that specify the spacecraft Autonomy behavior in focus are verifiable, design independent, and feasible."	DSR	Q1
"The L4 Autonomy Subsystem requirements that specify the behaviors that the Autonomy subsystem is supposed to do are complete and consistent with respect to their parent requirement(s)."	DSR	Q1
"The requirements for software interfaces with hardware, user, operator, and other systems are adequate to meet the needs of the system with respect to expectations of its customer and users, operational environment, dependability and fault tolerance, and both functional and non-functional perspectives."	DSR	Q1
"The system is capable of identifying, controlling, preventing, or properly responding to any credible fault scenario."	DSR	Q3
"Every fault is properly controlled by a requirement."	DSR	Q3
"The L4 Autonomy Subsystem requirements do not specify any behaviors that the Autonomy Subsystem should not do."	DSR	Q2
Design Phase		
"Though undocumented, there was a reasonable process to identify potential hazards that need to be addressed."	DSR	Q3
"The Autonomy Subsystem design that represents the Autonomy System Requirements in scope does not introduce capability that is undesired or not required."	DSR	Q2
"The Entry, Descent, & Landing timeline has appropriate use of all sensors and actuators."	DSR	Q1
"Decisions leading to Entry, Descent, & Landing in terms of which string to use are understood correctly."	DSR	Q1
"There are no monitor response collisions – there are no concurrent responses that could cause harm or detrimental behaviors to the rover between any lower or higher level responses."	DSR	Q2
"The fault protection is sufficiently implemented that there is never an unsafe configuration."	DSR	Q2
Implementation Phase		
"All monitors accounted for in the requirements and design are implemented in the code."	DSR	Q1
"Wakeup and shutdown sequences work correctly – there is robustness and steps to ensure the rover always wakes up."	DSR	Q1 Q3
"The handoff between the lower level and system fault protection is designed and implemented correctly."	DSR	Q1
"Upon completion, analysis will confirm if the ... fault management behaviors needed for the system during flight operations are correctly and completely being represented in the algorithms and fully satisfied in the implementation."	EO	Q1
"All reasonable faults are addressed and correctly implemented for Entry, Descent, & Landing."	DSR	Q1 Q3
"The implementation of the analyzed in-scope Watch Points, Action Points, and Relative-Time Sequences was correct and complete. This software is ready to support mission scenarios in spacecraft flight software system and fault management Verification testing efforts."	EO	Q1

Assurance Objectives or Conclusions	*Mission Type*	*3Qs Mapping*
"There is no inadvertent code that could cause an unplanned processor reset."	DSR	Q2
"The Second Chance Entry, Descent, & Landing does not harm the core Entry, Descent, & Landing sequence."	DSR	Q2
Integration & Testing Phase		
"All necessary fault paths were exercised in the identified validation testing."	HSF	Q1
"The set of tests was comprehensive with regard to the Fault Management Design Document algorithms."	HSF	Q1
"The analyzed fault management implementation has been proven correct and complete through verification testing. In addition, the analyzed Action Points and Relative-Time Sequences were ready for execution during mission operational phases of the observatories."	EO	Q1
"The Fault Management algorithms were properly tested with actual Separately Loadable Database data."	HSF	Q1
"The FM data input parameters, persistence limits, CUI's, etc., were validated through appropriate testing."	HSF	Q1
Operations & Maintenance Phase		
"The Formal Qualification Testing (FQT) tests verified what the revised software is supposed do and what the software is not supposed to do, as per requirements. The software performs adequately under adverse conditions applicable to tests as specified in requirements and FQT standards and guidelines."	HSF	Q1 Q2 Q3
"The added tests [resulting from the resolution of issues] strengthened the developer's testing of the revised software and provided additional assurance that the software will perform as expected."	HSF	Q1
"IV&V determined the Software Change Request content satisfies the enhancements to the Computer Software Configuration Item."	HSF	Q1
"The requirement, code, and design changes represent the changes implemented to support upcoming operational needs and improvements."	HSF	Q1

Key – Colors
Assurance Objective
Assurance Conclusion

Key – Mission Type	
DSR	Deep Space Robotic
HSF	Human Spaceflight
EO	Earth Orbiter

Exhibit 6: **Assurance Objectives and Conclusions across FM IV&V**

CONCLUSION

An in-depth survey of several FM architectures that serve to structure the safety- and mission-critical software into which NASA IV&V has visibility has been completed. The NASA IV&V Program has found that FM systems, many times architected as reactive components embedded within the overall software system, are often ranked high in the risk-based assessment of criticality. Addressing the 3Qs of IV&V analysis in order to provide assurance to NASA projects has been demonstrated as one strategy to provide value to the projects. The use of Assurance Strategies enables the identification and mitigation of risks for a variety of mission types, including Earth orbiters, human spaceflight, and deep space robotic missions. Although Assurance Strategies vary between IV&V projects, a look into the types of Assurance Objectives and Assurance Conclusions that may be made across the developmental lifecycle has been provided by this SARP initiative. The aggregation of IV&V techniques and Assurance Strategies provides a technical reference for current and future IV&V projects.

Results of these efforts will feed into the updated NASA FM Handbook that is organized in terms of mission-specific guidebooks. Providing an informative technical reference of high-level characteristics of FM architectures, the low-level features of FM systems specific to mission domain, and benefits and limitations in the application of current software assurance methods is being coordinated with this SARP initiative. The benefits are aimed beyond the IV&V community to those that seek ways to efficiently and effectively provide software assurance to reduce the risk posture of NASA and other space missions. Potential future efforts will be to extend our efforts to survey additional spaceflight projects; investigate projects within other domains such as launch vehicles, ground systems, or manned and unmanned aeronautics systems; as well as collaborate with OSMA and FM experts across the NASA agency.

[1] Asbury, Michael. *NASA IV&V Facility 2012 Annual Workshop.* National Aeronautics and Space Administration, 13 November 2014. Web. 5 March 2015. http://www.nasa.gov/centers/ivv/workshops/ivvworkshop_2012.html.

[2] Asbury, Michael. *NASA IV&V Facility.* National Aeronautics and Space Administration, 13 August 2014. Web. 5 March 2015. http://www.nasa.gov/centers/ivv/home/index.html.

[3] *Fault Management Handbook.* Draft 2. National Aeronautics and Space Administration, 2 April 2012. Web. 5 March 2015.

[4] Topousis, Daria. *NASA Engineering Network: Fault Management.* Version 4.0. National Aeronautics and Space Administration. Web. 5 March 2015.

[5] *Independent Verification and Validation Technical Framework.* Version O. National Aeronautics and Space Administration, 6 June 2012. Web. 5 March 2015. http://www.nasa.gov/sites/default/files/ivv_09-1_-_rev_o.pdf.