Report on the 2012 NASA Spacecraft Fault Management Workshop

For the Science Mission Directorate, Planetary Sciences Division

Workshop Organizer:
Lorraine Fesq, Jet Propulsion Laboratory, California Institute of Technology

Report Authors:
Lorraine Fesq, Jet Propulsion Laboratory, California Institute of Technology
Kristin Fretz, The Johns Hopkins University Applied Physics Laboratory
Marilyn Newhouse, Marshall Space Flight Center/Computer Sciences Corporation

February 2013

Table of Contents

Executive Summary 3

Overview of the 2012 Spacecraft FM Workshop 5

Details of Workshop Events 7

- Keynote and Invited Speakers 7
- Progress Since the 2008 FM Workshop 9
- Focus Area 1: Assess FM Architecture Fitness 10
  - Presentations 11
  - The FM Architecture Assessment Breakout Session 13
- Focus Area 2: Identify FM Capabilities Gaps 18
  - Presentations 18
  - The FM Capabilities/Technologies Roadmap Breakout Session 21
- Focus Area 3: Handbook Issues 24
  - Presentations 24
  - Panel on Integrating FM: How Does It Fit? 25

Conclusions and Continuing Work 29

Acknowledgments 30

Appendix A: Workshop Agenda 32

Appendix B: Workshop Attendee List 33

Appendix C: FM Capabilities Roadmaps Developed During the Workshop 36

Appendix D: Workshop Survey Feedback 43

Appendix E: The Formation of NASA's Fault Management Community of Practice 44

Appendix F: Report on the Fault Management Breakout Session Held at the 2012 Independent Verification and Validation (IV&V) Workshop "V&V of Fault Management: Challenges and Successes" 48

Executive Summary

On April 10–12, 2012, the NASA Planetary Sciences Division (PSD) of the Science Mission Directorate (SMD) sponsored the second Spacecraft Fault Management (FM) Workshop in New Orleans to bring together NASA's FM community to actively and collaboratively coalesce the discipline. Over 100 people from NASA, DoD, industry, and academia attended the workshop. The goals of the workshop were threefold:

- **Assess FM architecture fitness**: Initiate the development of an FM architectural trade space tool by characterizing and assessing FM approaches and architectures to enable future missions, which will enable future missions to evaluate the appropriateness of a selected FM architecture.
- **Identify FM capabilities gaps**: Develop straw-man FM Capabilities Roadmaps to identify near-term needs and long-term goals in order to provide guidance and investment strategies for future FM technology development.
- **Achieve common understanding of key issues across the FM community**: Discuss key issues that emerged from the draft release of the NASA FM Handbook, including how to establish a distinct FM vocabulary to be used across the Agency; how FM relates to other parts of the NASA community such as systems engineering, software, and the Office of Safety and Mission Assurance (OSMA); and how FM fits within a project.

The workshop consisted of a keynote talk by Brian Muirhead, Chief Engineer at the Jet Propulsion Laboratory (JPL), on coalescing NASA's diverse views of FM and health management; formal presentations providing insight on FM approaches taken throughout the NASA community (deep-space, Earth-orbiting, human spaceflight missions) as well as road-mapping activities in launch vehicles and aeronautics; invited talks to provide an outside perspective on how other communities are organizing and maturing the FM field; a panel discussion on FM's role within a project; and two breakout sessions.

The goal to "assess FM architecture fitness," labeled Focus Area 1 in this report, was achieved first by recognizing the need to evaluate the appropriateness of FM architectures. Focus Area 1 introduced an approach and methodology based on "quality attributes" where mission/design/implementation characteristics were correlated with quality outcomes. Breakout sessions brought about spirited discussion of the quality attributes; although attendees did not oppose the use of quality attributes, there was not consensus on whether the specific quality attributes were appropriate. However, participants did agree that including some type of architecture assessment as an explicit process step in FM development was an idea that should be further explored.

The goal to "identify FM capabilities gaps," labeled Focus Area 2 in this report, addressed building capability roadmaps for six mission domain areas—aeronautics, launch vehicles, human and robotic Earth orbiters, and human and robotic deep-

space missions—in order to identify gaps in current capabilities that will be needed in future missions. The sessions also brought out areas where a "one-size-fits-all approach" would not be advisable, such as the utility of artificial intelligence-like capabilities for short-duration launch vehicle missions. However, many synergies were found between the different mission domain areas. Three key candidates for capability development were 1) the tools and models to efficiently perform FM cost/benefit, function, and design analyses, 2) improvements in designing for, planning, and executing FM verification and validation (V&V), and 3) design for and acquisition of data for prognosis and reconstruction of failures.

The workshop drew an outstanding quantity and quality of participants from across NASA and our key industry partners. This was an excellent networking opportunity for anyone involved in the FM field. The following common themes emerged from presentations and discussions:

- Initial evidence was presented that implementing the recommendations from the 2008 FM Workshop, for example, that FM should be "dyed in, not painted on," does mitigate against the common cost growth problems discussed at that first workshop
- FM technology advancement is crucial for the success of future human missions, especially missions that will send humans beyond Earth orbit
- Participants recognized the importance for system states to be explicit in FM
- Goal-based or objective-based control is a logical next step in achieving more autonomous FM
- A number of speakers presented the importance of modeling at the architecture and system level, and the need to include functionality of software and FM in the models
- The community identified the need to conduct an assessment (e.g., survey) of the tools (both inside and outside of NASA) and their usage to understand whether the state of the practice is up to the challenge
- Lessons learned need to capture the reasons underlying design choices as well as consequences that were not considered as part of the decision

All workshop materials, including speaker biographies and photographs, downloadable presentations, and videos of the presentations and the panel, are available on the Fault Management Community of Practice (FM CoP) website on the Chief Engineer's NASA Engineering Network (NEN)[1]. See "Appendix E: The Formation of NASA's Fault Management Community of Practice" for an overview of the formation of the FM CoP.

[1] The FM CoP can be accessed at https://nen.nasa.gov/web/faultmanagement/home. This website resides on the NEN, which is behind the NASA firewall.

Overview of the 2012 Spacecraft FM Workshop

On April 10–12, 2012, NASA held its second Spacecraft FM Workshop. Lindley Johnson, the Program Executive for NASA's Discovery Program in the SMD's PSD, sponsored the 2012 FM Workshop, which was held at the Hotel Monteleone in New Orleans, Louisiana. Over 100 people from 30 different organizations across government, industry, and academia attended the workshop. In addition, the NASA Safety Center sponsored a live webcast of the workshop, allowing an additional 60 virtual attendees to participate.

Figure 1 shows a timeline of events leading up to the second workshop, which was held almost exactly four years after the first workshop in April 2008.

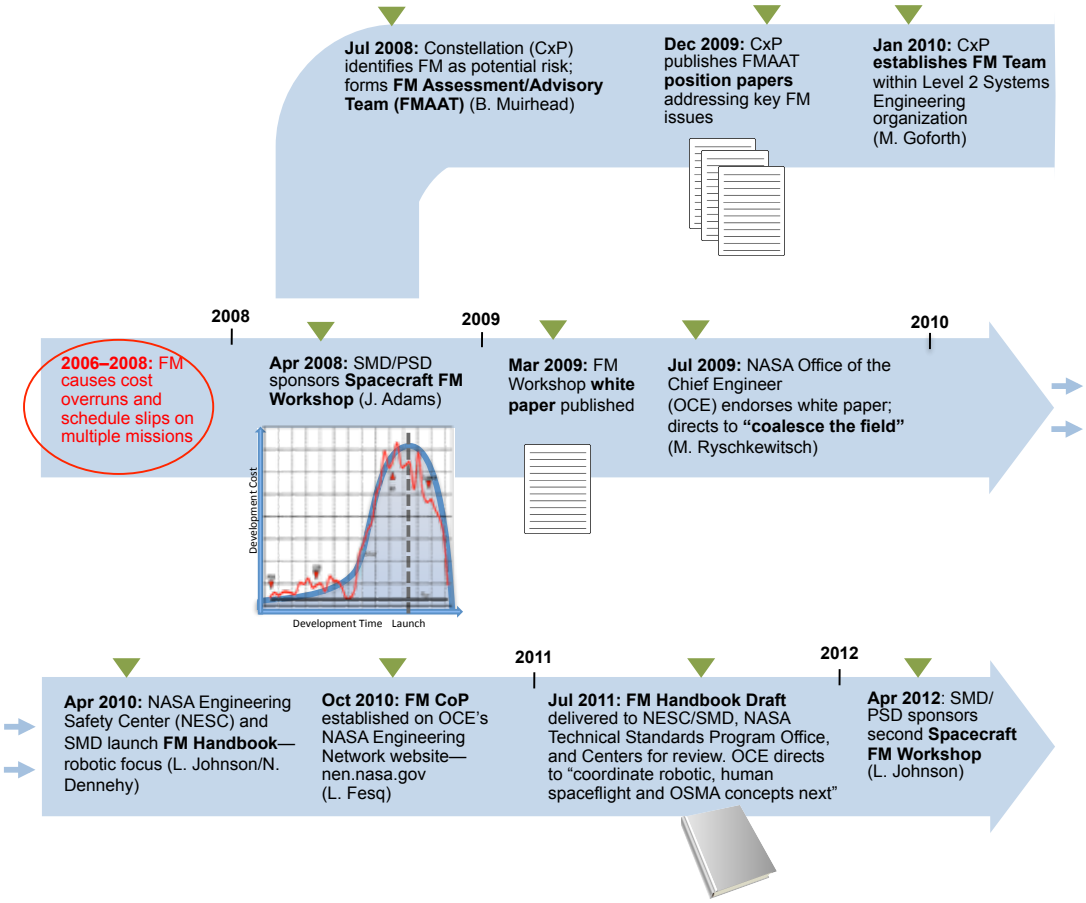

Figure 1. Timeline of recent FM activities at NASA. NESC, NASA Engineering and Safety Center.

The first NASA Spacecraft FM Workshop in 2008 was held in response to issues that emerged on numerous missions when FM was tested at the spacecraft level. The 2008 FM Workshop focused on bringing together the robotic Earth orbiter and deep-space robotic spacecraft communities together, although members of the human spaceflight community attended and provided insights and a fault detection, isolation, and recovery (FDIR) perspective on FM. Twelve findings and recommendations, captured in the White Paper Report[2], emerged from this workshop. As an outcome of these finding, the NASA Chief Engineer directed the organizers to "coalesce the field" to achieve commonality in FM vernacular and concepts, to cross-pollinate the diverse approaches being used across NASA, and to better address future NASA needs such as sending humans beyond Earth orbit, where there will be a need to draw on and integrate expertise from the diverse FM subcommunities. Since the first FM Workshop, NASA has formed the Fault Management Community of Practice (FM CoP), organized as a website on NEN (https://nen.nasa.gov/web/faultmanagement/home) and has developed a NASA FM Handbook (NASA-HDBK-1002), which currently is in draft form.

The second NASA Spacecraft FM Workshop, held in 2012, broadened the focus beyond robotic spacecraft in recognition that managing faults is an essential element across all NASA missions. To reflect this expanded coverage, FM practitioners from all of the known subcommunities (i.e., launch vehicles, aeronautics, ground systems, mission systems, human spaceflight, and robotic) were invited to participate because the scope of future FM activities is expanding beyond spacecraft FM. The recommendations resulting from the 2008 workshop, as well as the intervening work on the FM Handbook, influenced the goals of 2012 FM Workshop. Whereas the 2008 FM Workshop focused on understanding and characterizing the causes of the project cost and schedule overruns due to FM, the 2012 FM Workshop sought to identify solutions to these problems. As a result, the goals of the 2012 FM Workshop were to:

- **Focus Area 1: Assess FM architecture fitness**. Initiate the development of an FM architectural trade space tool by characterizing and assessing FM approaches and architectures to enable future missions, which will enable future missions to evaluate the appropriateness of a selected FM architecture (2008 FM Workshop Recommendations #5[3] and #8[4]);

[2] For results from the 2008 NASA FM Workshop, see the "White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate, Planetary Sciences Division," March 2009. This report can be found behind the NASA firewall on the FM CoP website at https://nen.nasa.gov/web/faultmanagement/home.

[3] Recommendation 5: "Establish metrics and process specification with milestones that will allow proposal evaluators and project teams to assess the relevance, merits and progress of a particular FM approach."

- **Focus Area 2: Identify FM capabilities gaps**. Develop straw-man FM Capabilities Roadmaps to identify near-term needs and long-term goals to provide guidance and investment strategies for future FM technology development (2008 FM Workshop Recommendation #6[5]);
- **Focus Area 3: Achieve common understanding of key issues across the FM community**. Discuss key issues that emerged from the draft release of the NASA FM Handbook, including
  - How to establish a distinct FM vocabulary to be used across the Agency (2008 FM Workshop Recommendation #3[6]),
  - How FM relates to other parts of the NASA community such as systems engineering, software, and the OSMA (FM Handbook issue), and
  - How FM fits within a project (FM Handbook issue).

Invited speakers provided a broader perspective on the changing scope of FM and what is happening within FM outside of NASA. To meet its goals, the workshop used a combination of formal presentations by subject-matter experts, breakout working sessions, and a panel discussion. The workshop agenda is included in "Appendix A: Workshop Agenda."

Details of Workshop Events

Keynote and Invited Speakers

The workshop program included four invited speakers whose role was twofold. The first objective was to help participants understand how other communities are organizing and maturing the FM field. The second objective was to gain new perspectives by exposing participants to alternate approaches and concepts. Summaries of the keynote and invited speakers' presentations are provided below.

Keynote Speaker: Brian Muirhead (JPL/Caltech), "Coalescing NASA's Views of Fault and Health Management"

Brian Muirhead, JPL's Chief Engineer, opened the 2012 FM Workshop as the keynote speaker with his talk on "Coalescing NASA's Views of Fault and Health Management." This presentation highlighted a number of robotic missions as well as the Shuttle

---

[4] 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."

[5] 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."

[6] 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."

and International Space Station (ISS) programs in an attempt to unite the robotic and human spaceflight community's views of FM and health management (HM), respectively. The engineering "discipline" of HM/FM is neither widely recognized nor evenly practiced across NASA. However, managing faults/failures is crucial to the successful design, development, and operations of both crewed and robotic space systems. Coalescing the HM/FM field is essential to accomplish future NASA missions such as achieving human presence beyond low Earth orbit. In order to merge this field, system architects, stakeholders, and designers need to become more aware of and conversant in issues, design options, V&V, and operations of HM/FM throughout the program/project life cycle by: 1) incorporating HM/FM-based needs while addressing both cost and risk, 2) balancing/optimizing automation vs. human-in-the-loop in space and on the ground, and 3) developing and delivering highly dependable avionics and software across all systems. Although there is potential for collaboration and mutual benefit across the aerospace industry through working together in HM/FM, there is a need for better understanding of this discipline—from various points of view and mission contexts, as well as its drivers, benefits, and limitations.

Invited Speaker: Michael Aguliar (NASA Goddard Space Flight Center [GSFC]/ NESC Software Technical Fellow), "Fault Management using Model Based System Engineering (MBSE) Tools and Techniques"

Invited speaker Michael Aguilar, NASA GSFC and NESC Software Technical Fellow, presented on the topic of "Fault Management using Model Based System Engineering (MBSE) Tools and Techniques." James Webb Space Telescope (JWST) was used as an example of a complicated system that cannot be assembled and tested as one system. System Modeling Language (SysML) and Unified Modeling Language (UML) were used to build nonexecutable models as well as an executable model; however, errors were found because the model was not consistent. The more that can be simulated and modeled in software, the better one can examine the system as a whole. Another significant point that was raised was that modeling is typically well addressed during design phases; however, the model drops off during the building and assembly phases. Complex, massive missions and systems of systems require modeling throughout the design, building, and assembly phases because they often cannot be tested as one system.

Invited Speaker: Dr. Werner Dahm (Director of Security & Defense Systems Initiative, Arizona State University, former Air Force Chief Scientist), "Fault Management in Complex Adaptive Systems***: Applications and Challenges on the Horizon"***

Invited speaker Dr. Werner Dahm, Director of Security & Defense Systems Initiative, Arizona State University, presented "Fault Management in Complex Adaptive Systems: Applications and Challenges on the Horizon." A transformation is underway in which complex adaptive systems (CASs) are increasingly replacing traditional simple engineered systems. CASs are based on self-awareness and

continual autonomous adaptation to maximize the achievement of goals; CASs utilize a goal-driven approach because all the modes of operation cannot be inferred or anticipated and make no distinction between nominal and faulty operations. Dr. Dahm provided several examples of CASs and outlined both the enablers and attributes of CASs. The complexity and adaptive nature of these systems makes it difficult to apply traditional FM to this area not only because of the cost and schedule, but also because of the inability to separate nominal and fault states. In addition, high levels of system adaptation and number of inputs make these near-infinite state systems for which traditional V&V is unsuited. Architecting an adaptable system using software systems engineering approaches can make CASs more verifiable.

Invited Speaker: Dr. Algirdas Avizienis (University of California, Los Angeles [UCLA], Distinguished Professor Emeritus, Computer Science Department), "Terminology Issues in Dependable Computing"

Invited speaker Dr. Algirdas Avizienis, Distinguished Professor Emeritus, Computer Science Department, UCLA, spoke on the topic of "Terminology Issues in Dependable Computing." Dr. Avizienis began his career in the area of FM in the 1960s when he encountered a dependability problem with the design of an on-board computer that could survive several years and deliver a specified performance at planetary encounters for a JPL mission. This work culminated in a taxonomy of over 200 terms in the area of dependability that includes attributes such as reliability, availability, safety, integrity, maintainability, etc. Security brings another dimension into the area of dependability as it relates to availability and integrity. Dr. Avizienis also highlighted a number of recommendations for the FM Handbook with emphasis on introducing the concept of error, defining failure as an event, and eliminating the concept of failure tolerance, which should be replaced by service outage and service restoration.

Progress Since the 2008 FM Workshop

Kristin Fretz (The Johns Hopkins University Applied Physics Laboratory [JHU/APL]), "Recent Progress in the APL Fault Management Process"

Kristin Fretz, JHU/APL, presented "Recent Progress in the APL Fault Management Process" to highlight changes that APL made in response to the 2008 FM Workshop Findings and Recommendations. This presentation discussed six of the 12 findings that APL integrated into their internal FM and autonomy engineering processes. Changes made to the FM and autonomy processes addressed diffused FM, insufficient formality of documentation, FM complexity, inadequate testbed resources, and cost and schedule. These process changes were implemented on the Radiation Belt Storm Probes (RBSP) project (now known as the Van Allen Probes) and resulted in better communication of the FM concept and design as well as significant changes in the staffing curve as compared with previous APL missions. The RBSP mission was a less challenging mission to implement these changes on, so

we will need to continue to evolve the APL FM and autonomy processes by using lessons learned from RBSP and addressing additional findings from the 2008 and 2012 FM workshops.

Focus Area 1: Assess FM Architecture Fitness

The 2008 FM Workshop identified a need for projects to evaluate the appropriateness of FM architectures for a given mission. The findings stated that "FM architectures often contain complexity beyond what is defined by project specific definitions of faults and required fault tolerance and increased FM architecture complexity leads to increased challenges during I&T and mission operations" (Finding 8a and 8b) and "metrics have not been established to evaluate the appropriateness or measure the life cycle progress of FM systems" (Finding 5). Focus Area 1 worked toward the development of an FM architectural trade space tool to characterize and assess FM approaches and architectures that will enable future missions to evaluate the appropriateness of a selected FM architecture. Key inputs to the FM design trade space include mission characteristics, FM architecture design choices and implementation methods, and the heritage of staff, tools, hardware, software, procedures, and practices as shown in Figure 2. Evaluating and weighing these inputs allows the overall risk of the FM design to be assessed.

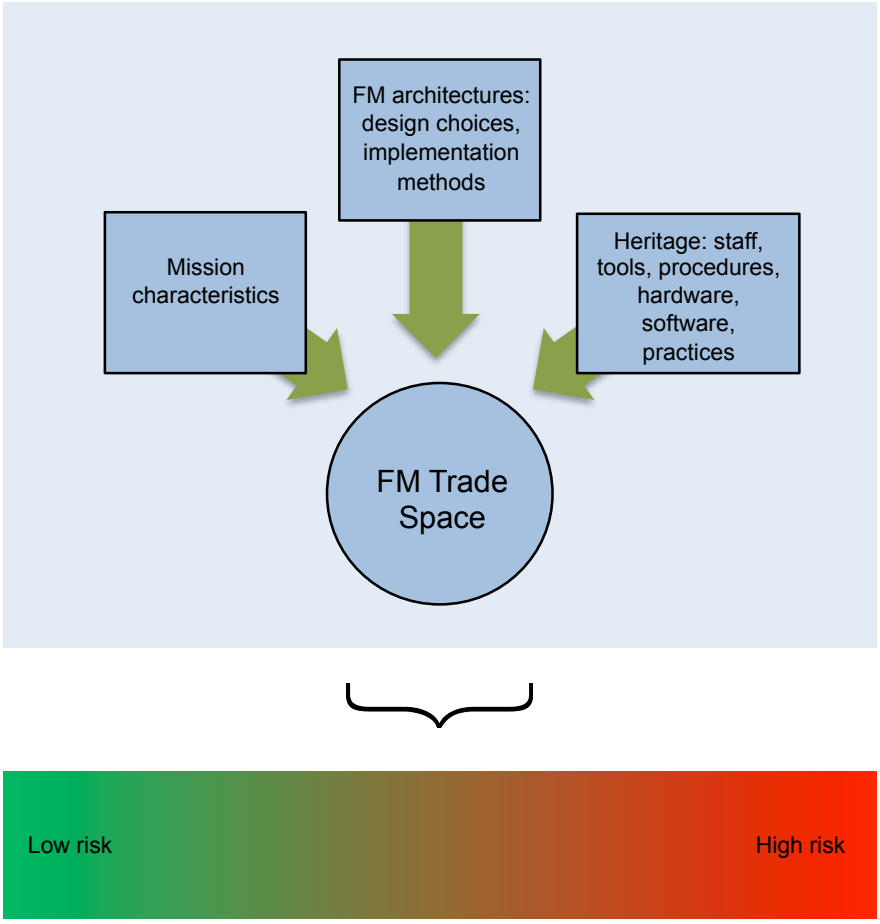

Figure 2. The goal of Focus Area 1 was to establish an FM architectural trade space to enable future missions to assess the appropriateness of an FM architecture.

Focus Area 1 began with four formal presentations covering FM architectures from various mission types. These presentations were followed by a breakout session where participants were introduced to an architectural assessment tool and methodology for assessing FM architectures. Case studies, developed in advance of the workshop, were presented to illustrate the approach and spur discussion on assessing FM architectures. Participants then applied the approach to a future mission concept to assess the feasibility of various architectures.

Presentations

Jon Patterson (NASA/Marshall Space Flight Center [MSFC]), "Analytical Approaches to Guide Space Launch System FM Development"

Jon Patterson, NASA/MSFC, gave the first presentation in the FM Architecture Assessment focus area and discussed "Analytical Approaches to Guide Space Launch

System FM Development." This presentation discussed how Space Launch System (SLS) element and subsystem operations are implemented in the SLS Flight Computer software for both nominal operations and FM to increase efficiency and reduce the overlap between groups. SLS FM development was a collaboration of stakeholders and involved Safety and Mission Assurance (S&MA), systems engineering, elements and subsystems, and a number of SLS disciplines to determine the best triggers and response options. Finally, a number of tools and sources for failure and fault identification (Goal Tree/Success Tree, Hazards Analysis, Failure Scenarios/Abort Scenarios, Failure Modes and Effects Analysis) were highlighted as ways to determine the right set of FM capabilities to provide the most coverage without significantly increasing the cost and complexity of the overall vehicle systems.

Carlos Garcia-Galan (NASA/Johnson Space Center [JSC]), "FM for Crewed Missions"

Carlos Garcia-Galan and Lee Morin, NASA/JSC, presented "FM for Crewed Missions" as a part of the FM Architecture Assessment focus area. FM for crewed missions is much more than onboard hardware and software, with FM in the cockpit being just as important as designing a robust spacecraft. This presentation focused on the in-depth training flight controllers receive and gave a fault example from ISS to demonstrate the involvement of flight controllers in the diagnosis and recovery actions. In addition, improving FM in the cockpit by upgrading warning messaging, message grouping, and displays provides crew members more useful information, which increases their usefulness in the diagnosis and recovery role.

Phillip Schmidt (The Aerospace Corporation), "Independent Assessment of NASA Fault Management System Architectures"

Phillip Schmidt, Aerospace Corporation, continued the FM Architecture Assessment focus area by presenting "Independent Assessment of NASA Fault Management System Architectures." At the request of MSFC, two FM software architectures for deep-space robotic missions were assessed. The first was a layered, collaborative-based FM system, while the other was an event-driven, ruled-based FM system. The criteria used to assess these architectures were categorized according to a project's timeline and included Planning, Requirements, Design, Implementation, Test and Verification, and Operations. The end result was a list of common practices between the two architectures as well as a list of recommendations for items that should be taken into consideration when developing an FM architecture along with items that need more thought and research.

Mark Derriso (Air Force Research Laboratory [AFRL]/Wright-Patterson), "Integrated Systems Health Management Architecture"

Mark Derriso, Air Force Research Laboratory, concluded the FM Architecture Assessment focus area with his presentation on "Integrated Systems Health Management Architecture." Integrated Systems Health Management (ISHM) is the

determination of the overall state of a system through the conversion of data into information and knowledge and the use of this state information and knowledge to influence the system's operation. ISHM architecture characteristics include a hierarchical structure, distributed processing, multilevel reasoning, operation in real time, and generation of actionable information that fit into three primary functions: information management, mission executive, and flight management.

The FM Architecture Assessment Breakout Session

Kevin Barltrop, JPL/Caltech, masterminded the concept of performing an FM architecture assessment, and John Day, JPL/Caltech, David Garlan, Carnegie Mellon University, and Dan Dvorak, JPL/Caltech, cochaired the breakout session to convey the concept to the participants. This session focused on the need for projects to evaluate the appropriateness of an FM architecture for each mission. To this end, an FM architectural trade space was established to enable future missions to assess the appropriateness of an FM architecture (Figure 2).

The FM Architecture Assessment breakout session had two main focuses: 1) to capture existing FM architectures and requirements and collect design drivers and implementation decisions on mature programs in order to create a repository to provide a resource that enables future FM architects to make better trades and 2) to articulate a comprehensive list of functional and nonfunctional properties for use as figures of merit in assessing FM architectures and compile a mapping from architectural features to the functional and nonfunctional properties they promote (including examples of such features). The goal of the FM Architecture Assessment breakout session was to provide tools and methods to perform a technical assessment that addressed the following questions:

1) How well does a proposed solution fit a given mission and organization?
2) How well do other existing solutions fit a given mission and organization?
3) How well do individual features from existing solutions fit a given mission and organization?

The first objective of the FM Architecture Assessment breakout session was to capture existing FM architectures, requirements, and design drivers to create a repository to give future FM architects a resource for making better trades and assessing architectures. To this end, the software architecture notion of "quality attributes" (QAs) was introduced as the basis of an architectural assessment tool and methodology for assessing FM architectures. QAs were enumerated in advance, and included Analyzability, Correctness, Cost for Development, Cost for Operations, Cost for Training, Degrade Gracefully, Familiarity, Fault Coverage, Interoperability, Modifiability Modularity, Reliability, Reusability, Safety, Scalability, Testability, Trustworthiness, and Usability/Operability. This QA approach correlated mission/design/implementation characteristics with quality outcomes. The assessment process consisted of two key elements:

1) A top-level process flow for examining the heritage risk story

2) An online database and reporting tool to ground the assessment in measurable data

The heritage risk assessment covered the following areas of an FM solution: staff, engineering practices, analyses and design tools, flight software, flight hardware, and mission design. Figure 3 depicts the assessment flow and makes two important points. First, it shows that even a difficult-to-use solution can be applied successfully to identical missions once it has been sufficiently debugged, and second, that a project may also iterate this process across multiple aspects of the architecture and across multiple changes to the architectural approach. Figure 4 illustrates a flow chart showing the planned use for the FM architecture trade space.

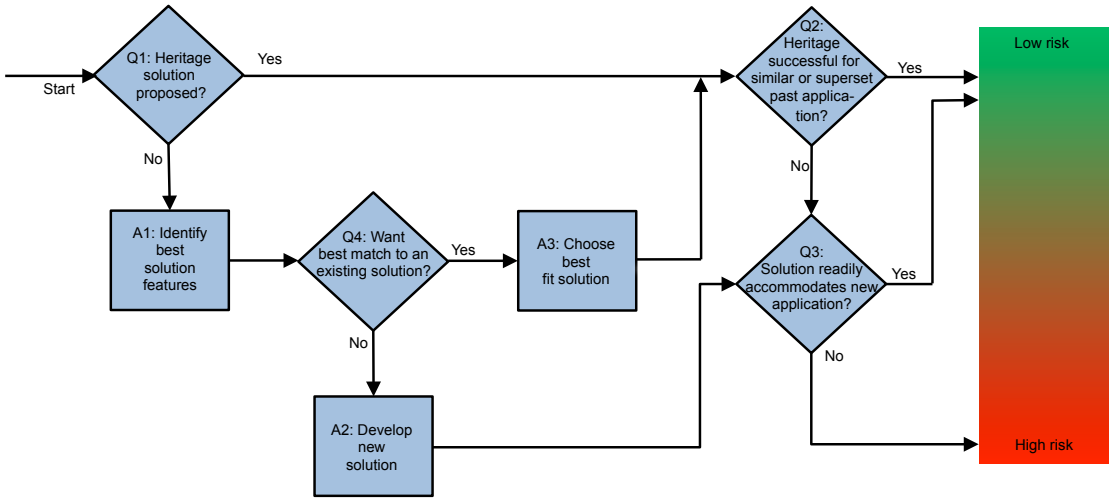

Figure 3. Heritage risk assessment process.

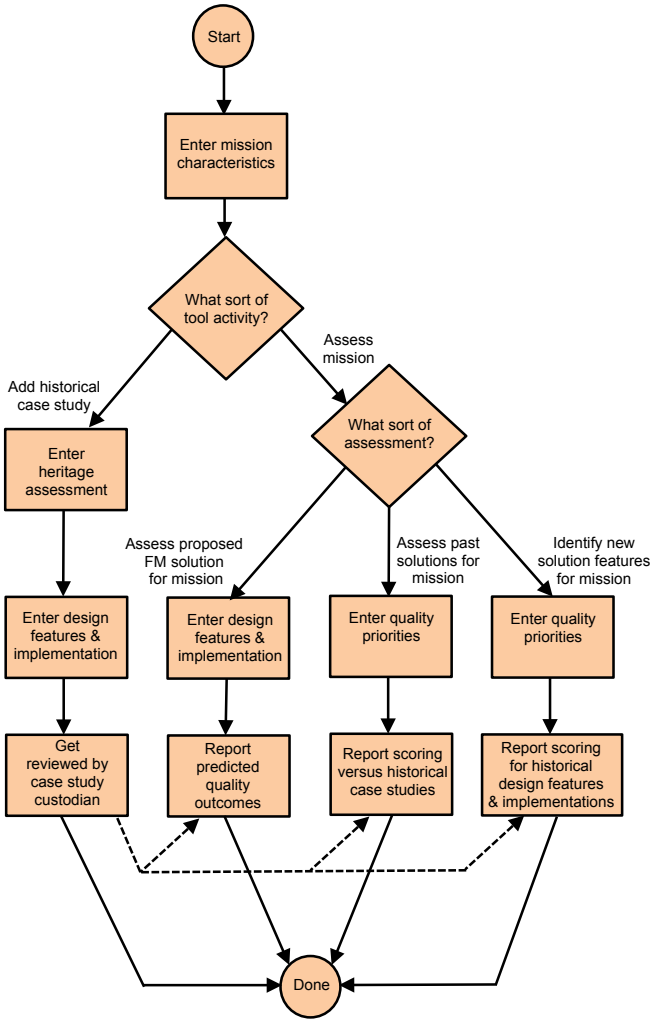

Figure 4. Decision flow for using the FM architecture trade space

Six historical case studies were developed in advance to illustrate the approach and spur discussion on assessing FM architectures. The FM Architecture Assessment breakout session then split into three subsessions to discuss two case studies each in detail. Throughout the subsessions, participants evaluated the proposed methodology and selected set of QAs and provided feedback. The QAs were assessed for completeness, applicability (to a given mission type), and level of abstraction. In addition, participants provided feedback to establish a basis for additional applications to be added to the architectural database. The following is a summary of the case studies presented, along with relevant insights captured during the workshop.

Mark Brown (JPL/Caltech) discussed "Cassini Attitude Control Fault Protection" as a case study representing flagship-class missions. As a flagship-class Saturn orbiter, Cassini has been flying successfully for ~15 years. Some aspects of the FM design for

this project were goal-like; it was noted that the goal-like features of the design worked well. However, there was a tendency for "gadgteering" for those features that were not goal-like.

Brian O'Hagan (NASA/JSC) presented "International Space Station (ISS) Autonomous Fault Detection, Identification, and Recovery (FDIR)." This case study represented a class of systems a) with various international partners, b) that has evolved substantially over time, and c) that has a human crew. A number of key issues came up during the presentation of this case study. The first issue that was raised was how to provide coordinated FM across multiple independently implemented subsystems. The next issue related to prioritizing FM upgrades given budget restrictions for long-lived systems; suggestions for this issue included the need for FM evolution management. Finally, understanding the role of humans in the overall FM plan was discussed; this includes what kinds of expertise can we assume humans have and to what extent does the assumption of human expertise have on what FM is automated and how FM is automated.

Eric Seale (Lockheed Martin Corporation) presented "Orion/Multi-Purpose Crew Vehicle (MPVC)" as a case study representing crewed missions traveling beyond low Earth orbit and a system designed by collaborative efforts with many NASA centers and industry experts. The development of this architecture has been limited so far because of budget constraints. These constraints have resulted in a less advanced FM system—it is neither goal based nor does it have state intelligence/awareness. In addition, the FM system has been turned "off" for all testing that has occurred so far.

Keith Patrick (Northrop Grumman Corporation) discussed "Chandra" as an example of a system that made clear tradeoffs in favor of safety over availability; this design decision led to a simpler FM system but one that provided less overall utility. How to make the tradeoff between these two dimensions was discussed in detail because it was recognized that this is a common issue to many NASA FM system designs. Another aspect of the Chandra FM design is a separate attitude control safing computer. There was a perceived need for a separate attitude control safing computer because the FM designers did not trust the software in the primary A-B redundancy because of late development; it was later recognized that a separate attitude control safing computer was not necessary.

Judy Tillman (Northrop Grumman Corporation) discussed NASA's "Small Spacecraft Technology Initiative (SSTI)" to illustrate a "faster, better, cheaper" mission with extreme cost constraints. This case study highlighted cost restrictions leading to a misapplication of heritage safe algorithms and an inadequate V&V program that ultimately resulted in loss of mission.

Jonathan Rustick (Orbital Sciences Corporation) presented "Dawn" as an example of a Discovery-class, interplanetary 10-year mission to two asteroids with significant

periods of no communication. TMON[7] table was selected as the FM approach for cost reasons because it is easy to configure/reconfigure. However, using TMON on this interplanetary mission introduced a number of challenges: it was difficult to review, the table approach did not provide information that would convey the intent of the monitors, and it was limited to simple constructs that, when combined, resulted in complex behavior. Despite these drawbacks, the FM Flight Software (FSW) correctly identified and responded to ~10 in-flight anomalies and errors.

In addition to the comments captured regarding the case studies, several other observations were noted during the session. The idea of using QAs was not contested; however, there was not consensus on whether the proposed set of QAs was appropriate. It may be that defining a set of *a priori* QAs is a poor starting point; being aware of past decisions is useful, but often times those past design choices were made for reasons that had consequences that were not considered as part of the decision. There was also significant difficulty in mapping from QAs to mission and design characteristics. Although this appears feasible, it remains a research project to establish this mapping, especially to establish quantitative relations. The majority of the useful discussion came from the descriptions of the missions and FM design solutions, and not from examining the details of the trade space. Discussing the various case study architectures proved very useful as most participants were able to learn about different architectures (few people were familiar with architectures beyond their company, institution, or project) and to start to understand patterns in the architectures (which has never been done before). It was agreed that exposure to the trade space was beneficial in that it allowed participants to have a better understanding of the long-term goal for this activity. This part of the breakout session concluded that the field still has neither a clear understanding of how to determine the reliability of FM systems nor the ability to answer simple questions about architectures; however, technology advances such as model-based systems engineering approaches to FM development hold promise for answering those questions.

The second objective of the architecture breakout session focused on applying the attributes and insights gleaned from the case study review to a future mission concept in order to assess the feasibility of various architectures. After the case study discussions, the three subsessions reconvened to take what was learned and apply it to a mission that will require FM expertise from all areas of NASA, namely, a future human mission to a near-Earth asteroid. Victoria Friedensen from NASA Headquarters (HQ) and Dan Mazanek, Senior Space Systems Engineer at NASA Langley Research Center, presented a description to the full session. Participants then applied the assessment approach to this near-Earth asteroid mission and identified significant QAs for this class of mission and related design and implementation approaches that supported the identified QAs.

[7] TMON is a GSFC Telemetry Monitoring tool.

A major conclusion of the FM Architecture Assessment breakout session was that arriving at performance metrics for different FM architectures is a difficult task. There was agreement among the session participants that continuing work on development of a tool is useful. The concept of mission characteristics and architectural choices affecting QAs is sound, but it is a difficult problem, and a common approach may not be possible. Broadening the scope to include missing aspects such as organization, infrastructure, processes, and prevention/design-time elements was also discussed. Other approaches that were also likely to provide utility in assessing FM architectures were suggested. The development of architectural guidance, stated in terms of QAs, was proposed. For example, "if you do A, you are likely to have consequences B, C, D" or "if you optimize QA1, then QA2 and QA3 may be negatively affected." Finally, the session concluded that including some type of architecture assessment as an explicit process step in FM development was an idea that should be further explored.

Focus Area 2: Identify FM Capabilities Gaps

The 2008 FM Workshop found that "Practices, processes, and tools for FM have not kept pace with the increasing complexity of mission requirements and with more capable spacecraft systems" (Finding 6a) and recommended that the FM community "…identify capability gaps in the current generation of tools, and to facilitate technology development to address these gaps (Recommendation 6d)." In 2012, the National Research Council issued a report on NASA Space Technology Roadmaps and Priorities, which included an assessment of ISHM, FDIR, and Vehicle Systems Management (VSM). The report concluded, "Due to the potential for major mission improvements, strong alignment with NASA needs, and reasonable risk and development effort, ISHM/FDIR/VSM are rated as high-priority technologies." The second focus area, Building an FM Capabilities Roadmap, was designed to address these recommendations. The focus area combined seven formal presentations covering current practices and ongoing technology development relating to FM. The presentations were followed by a breakout session where participants worked to build capabilities roadmaps for the aeronautic, launch vehicle, human and robotic Earth orbiter, and human and robotic deep-space mission domain areas.

Presentations

Mark Schwabacher (NASA/Ames Research Center [ARC]), "Human Spaceflight ISHM and Technology Development"

Mark Schwabacher presented technology development activities in the application of ISHM to increase safety and reliability and reduce cost, as well as to enable human missions to destinations where round-trip delays prohibit timely diagnosis and intervention by ground-based flight controllers. He showed a 10-year roadmap for incorporating ISHM into human space habitats, reporting activities to date on the use of the Testability Engineering and Maintenance System (TEAMS) tool for functional fault modeling and the Inductive Monitoring System (IMS, also known as

Anomaly Monitoring Inductive Software System, or AIMSS), which has been in use for the ISS since 2008. He also reviewed three new technologies that are currently in development: the Failure Consequence Assessment System (FCAS) to determine which components have stopped functioning as a result of a failure, an ISHM and planning interface to communicate loss of capability to an automated planning system, and prognostics for the forward-osmosis water recovery system. He then discussed ongoing activities to incorporate ISHM into cryo-loading, including the demonstration of autonomous cryogenic loading with recovery from selected failure modes, the development of prognostics for selected complex cryogenic tank failures, and a related effort to develop prognostics for Extra Vehicular Activities suit batteries.

Robert Mah (NASA/ARC), "System-Wide Safety Assurance Technologies"

Robert Mah briefed the attendees on the NASA System-Wide Safety Assurance Technologies (SSAT) Project. The goal of the SSAT Project, which is engaging in partnerships with more than 25 government, industry, and academic entities, is to understand and predict system-wide safety concerns of the airspace system, including the emergent effects of increased use of automation and the integration of system-wide health monitoring functions across ground, air, and space systems. Initiated in 2011, SSAT is a long-term project to address four technical challenges: filling a critical gap by developing time- and cost-effective techniques for V&V of complex civil aviation systems (by FY25), demonstrating automated discovery of precursors to aviation safety incidents through analysis of large heterogeneous data sets (by FY19), developing analysis tools that incorporate known limitations of human performance (by FY20), and developing a new class of verifiable prognostic algorithms to facilitate certification of prognostic algorithms (by FY25).

Mitch Ingham (JPL/Caltech), "No More Band-Aids: Integrating FM into the Onboard Execution Architecture"

Mitch Ingham discussed the benefits of a single control architecture for both nominal and off-nominal execution for addressing the increasing complexity of NASA robotic missions. He started with some limitations of the typical spacecraft execution architecture in which FM is often considered an adjunct to nominal control and compared these to the desirable architectural features of state-based control specifications with explicit intent, in-the-loop fault recovery, separation of state determination and control, and a control system that manages low-level plant interactions. He then addressed detailed examples addressing the application of model-based programs to spacecraft architectures in which state is central and sequence intent is explicit, models are used directly in each layer of the architecture, and off-nominal situations are handled at different layers as appropriate. Under this approach, the details of the approach become less important than the architectural features, enabling the use of variants that employ more traditional estimation and control techniques.

Dan Dvorak (JPL/Caltech), "Model-Based Systems Engineering (MBSE) and Goal-Based FM"

Dan Dvorak's presentation covered the benefits of goal-based FM. He presented three criteria for assessing FM criteria: 1) emphasis on failure detection over fault detection, noting that a lack of faults is not the same as a healthy system; 2) support for graceful degradation that allows unaffected activities to continue execution; and 3) a single mechanism for controlling both nominal and off-nominal behaviors to simplify interfaces and, as a result, validation. In contrast to the typical monitor-response-inhibit architecture, in a goal-based architecture, state variables are explicit, goals are hierarchical with each goal having a success criterion that is monitored for success/failure, and the goals form the basis of operating the system (both nominal and off-nominal behavior). This approach trades increased framework complexity for decreased operations complexity, allowing on-board failure response decisions based on the context of the failure within the system state and the intent of the goal.

Liu Wang (NASA/JSC), "Modeling Failure Modes with SysML"

Liu Wang described an approach for using SysML for resolving the problems caused when spacecraft design and operations personnel create models of the same system with different processes, tools, and representations. Lack of coordination between the approaches creates locally successful products but also results in the same information being captured multiple times in multiple places with multiple representations, creating a maintenance challenge. The proposed solution, to use SysML to develop single, shareable system models in SysML, is being implemented for the Habitat Demonstration Unit (HDU) Project. A work in progress, SysML has, to date, been used to model HDU subsystems and system connectivity, as well as state machines and component functions with their associated failure modes. This allows the generation of FM artifacts (e.g., Failure Modes Effects Analysis and state models) from the shared system models and facilitates the exchange of FM data across engineering disciplines.

Stephen Johnson (University of Colorado), "FM Technical Performance Metrics"

Stephen Johnson presented an overview of the current status of FM technical performance metrics (TPMs). He noted that FM TPMs are ultimately tied to the standard NASA S&MA measurements of reliability, availability, and safety but also contribute to the assessment of alternate FM architectures. Addressing potential TPMs by FM functional area, he discussed a top-down approach for measuring failure detection and degradation coverage; approaches to metrics for failure detection, fault isolation, and fault identification derived from radar operational performance analysis; and prognostics metrics for accuracy, precision, and convergence. He also noted considerations for FM functional areas in which analytical work on TPMs is either in progress or needed: model adjustment, failure response determination, and response effectiveness, also noting that tools to support TPM evaluation are also lacking in most areas.

Mark Derriso (AFRL/Wright Patterson Air Force Base), "AFRL's ISHM Journey and Future Plans"

Mark Derriso presented the AFRL's roadmap for implementation of ISHM to meet the Air Force's need for a robust and responsive launch capability to rapidly place payloads into orbit and the ability to maneuver spacecraft to any point in Earth-centered space to support generation and augmentation of satellite constellations as well as the repositioning, recovery, and servicing of on-orbit assets. Currently about halfway through a 16-year plan, the AFRL has implemented Structural Health Monitoring to support rapid turnaround, demonstrated a System Health Reasoner to facilitate the analysis and response decision process, and developed ISHM components for an active ground system to support both flight and ground operations. These are part of the overall ISHM architecture currently in development, which combines subsystem-level reasoning and anomaly detection; vehicle-level reasoning, ambiguity resolution, and damage assessment; and operation control center reasoning for condition-based maintenance using fleet-wide statistics. When complete, the ISHM system is expected to minimize false positives that impede rapid turnaround and provide validation of maintenance and response decisions based on corroborative data.

The FM Capabilities/Technologies Roadmap Breakout Session

Ken Costello (NASA/Independent V&V [IV&V] Facility) and Mitch Ingham (JPL/Caltech) led a breakout session following the focus area presentations to develop roadmaps to identify gaps in FM capabilities and to establish a path for the development of FM technologies. The roll-up of these into an overall FM roadmap is intended to provide guidance to the maturation of the FM discipline across the varied and competing interests at NASA and within the limited development funding. By identifying technology needs to fill critical capability gaps that are directly tied to upcoming flight projects, the roadmap will help to connect FM needs for future NASA missions with ongoing innovation and identify ways to leverage research and development activities within NASA, academia, and the broader space community. Figure 5 is an example of one of the roadmaps developed at the 2012 FM Workshop; all of the workshop roadmaps are included in "Appendix C: FM Capabilities Roadmaps Developed During the Workshop."

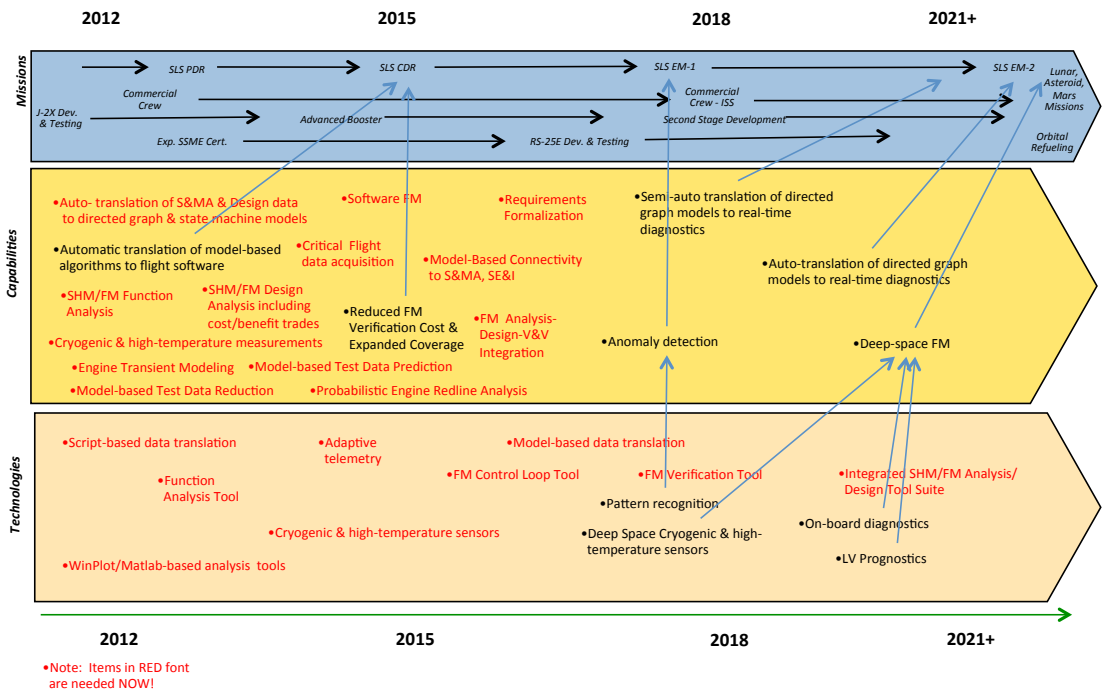

Figure 5. Sample FM capabilities/technology roadmap developed at the 2012 FM Workshop.

Before the workshop, a team of experts drawn from across NASA worked to develop a starting point in six domain areas: aeronautics, launch vehicles, human and robotic Earth orbiters, and human and robotic deep space missions. Team members included Stephen Andrews, Brian Bauer, Louis Breger, Barbara Brown, George Cancro, Kenneth Costello, John Day, Lorraine Fesq, Fernando Figueroa, Carlos Garcia-Galan, Kai Goebel, Gary Hunter, Mitch Ingham, Stephen Johnson, William Maul, Kevin J. Melcher, Jonathan Patterson, Ann Patterson-Hine, Daria Topousis, and Jonathan Wilmot. This team developed an initial timeline of missions and systems and examples of capabilities and technologies driven by one or more of these capabilities and technologies. (Two additional domain areas were identified—ground operations and mission operations—but were not addressed in the workshop.)

During the workshop, the participants were asked to refine six domain-specific roadmaps based on their knowledge of ongoing and future activities at their home institutions. They were tasked to:

- Identify the driving needs for FM capabilities over the short and long term
    - Capture the upcoming NASA missions/systems being developed in near-, mid-, and long-term timeframes that make use of an FM capability

- Identify those NASA projects that are enabled or enhanced by an FM-related capability

- Capture the FM development activities at individual centers or organizations that could be leveraged to meet the FM capability needs
- Identify the challenges to developing the required FM capabilities

The breakout session participants worked in teams on each of the domains, came together to cross-pollinate ideas across the teams, and then re-formed into separate domain teams to complete discussions and incorporate any additional ideas resulting from the cross-pollination. The revised mission/system timelines for each of the domain areas developed during the breakout session are included in "Appendix C: FM Capabilities Roadmaps Developed During the Workshop" of this report.

During the discussions, a number of commonalities emerged across the domains analyzed. Many of the identified commonalities related to FM processes, identifying the need to:

- Develop tools and models to perform efficient FM cost/benefit, function, and design analyses
- Increase development capabilities, in particular modeling and auto-generation of FM-related products
- Improve FM V&V to reduce cost, or even to make V&V feasible, including designing for V&V, test automation, determining V&V completeness, simulation capability, regression handling (potential impact coverage), and handling "nondeterministic" V&V
- Develop the ability to acquire more data for the reconstruction of failures and to understand during the design phase the level of reconstruction that will be available
- Augment run-time capabilities for ground support for prognosis and onboard diagnosis, including FM as a component of an overall autonomy approach including onboard planning and lights-out ground operations

Other commonalities highlighted the ongoing discussion regarding the scope and role of FM in a project. For example, the need to develop sensors that are more robust in harsh environments could be taken as an FM need but is also a mission-enabling engineering issue.

It was also noted that enabling capabilities for one domain often enhances other domains. Together, the commonalities and enhancing capabilities indicate that it may be worth investing in common framework developments for multidomain capabilities, or at least coordinating the work across domains.

In contrast to the many synergies found across the domain areas, capability needs did emerge with diverging approaches to FM. The development of artificial intelligence-like capabilities for short-duration LV missions was not considered a likely candidate for on-board critical functions, unless specifically required to meet speed and performance requirements. However, these capabilities could be beneficial for longer-term deep-space transportation systems and missions. Similarly, the need for FM approaches that span across multielement systems was highlighted only for deep-space manned missions.

The participants also noted an issue that was shared by domain teams during the development of the capabilities roadmaps. Differences in meanings of terms between different NASA communities—for example, prognostics, trending, and pattern recognition—slowed discussions until the commonalities emerged. This is an ongoing issue that affects many areas within the FM community, as identified during the first FM workshop in April 2008.

The development of the FM roadmaps is an ongoing activity that will continue after the FM Workshop. The distinct domain roadmaps need to be formalized and edited for consistency in format and scope (e.g., the specification of time-critical, enabling, and enhancing annotations, the linkage between missions, capabilities, and technologies). The roadmaps need to be completed and reviewed, additional input should be solicited from across and outside of NASA, and then the roadmaps will need to be analyzed to identify any gaps between developing FM needs and evolving FM technology, prioritize FM capability development, and recommend technology investments. When complete, the roadmaps should be briefed to NASA technology portfolio managers, for example, the Office of the Chief Technologist.

Focus Area 3: Handbook Issues

In an effort to coalesce the FM field, a NASA FM Handbook was developed in 2011 and distributed to the NASA Centers for review. The review resulted in over 1000 comments that reflected the diversity of the field. The third day of the 2012 FM Workshop focused on issues arising from the review of the FM Handbook. Conflicting comments indicated a lack of consensus within the FM community regarding fundamental issues. To begin a discussion of these issues, the third day included three focused talks on FM ontology, the applicability of control system theory to FM, and incorporating objectives and risks into the FM discipline, as well as a panel discussion on the integration of FM into projects.

Presentations

Steve Jenkins (JPL/Caltech), "FM Ontology"

Steve Jenkins focused on the application of the Ontology Web Language (OWL) to FM. Through examples, he demonstrated the use of classes (e.g., goal, fault, anomaly, assertion, assessment), relationships, data-type properties (e.g., epoch start and end times), and range restrictions for a simple FM ontology. He also discussed not only

the potential benefits of an FM ontology for facilitating the exchange of FM concepts and data but also the ability to use the ontology and reasoners to identify errors (e.g., consistency and satisfiability) and to infer additional rules and facts.

Peter Robinson (NASA/ARC), "FM as a Control System"

Peter Robinson discussed the applicability of control system theory to the field of FM. Control system theory has the potential to provide a common language for FM practitioners to communicate with others outside of their discipline (e.g., with systems engineers defining nominal control processes), provide a framework to specify FM requirements (possibly incorporating controller properties of stability and observability), and provide a framework to define formal estimates of FM domain complexity to support model development and accreditation costing. He covered the timeline for development of feedback control systems, artificial intelligence systems, and FM systems, showed examples of parallel approaches for specifying nominal control and FM equations, and provided a comparison of control system model properties for nominal control and FM.

Frank Groen (NASA/HQ-OSMA), "FM in an Objectives-Based/Risk-Informed View of Safety and Mission Success"

Frank Groen discussed the application of mission objectives and potential risks to the FM process. Traditional safety and mission success (SMS) planning focused on processes, standards, and products applicable to each technical discipline, with limited coordination between disciplines. This is evolving to be an integrated objectives-based and risk-informed approach to establishing confidence that a mission can be achieved. The potential benefits of including an objectives-based and risk-informed approach for FM include using the mission objectives as a basis for identifying and determining the relevance and completeness of FM QAs, a shared understanding across disciplines of the mission objectives and a framework for coordinating between disciplines, and recognition of the FM capabilities and their contribution to the mission objectives.

Panel on Integrating FM: How Does It Fit?

From the comments that were submitted against the draft version of the FM Handbook, it became apparent that within the community there was still a wide range of viewpoints regarding the scope of FM and how it should best be addressed within a program or project. To begin a discussion of these issues within the community, the workshop included a panel, "Integrating Fault Management: How Does It Fit?" on day three of the workshop. The panel was defined to begin a discussion of the following questions:

- How does a project strike a balance between the integrated system aspects of FM and the development and delivery of the required FM flight products?
- How does a project manage the overlapping roles and responsibilities between FM, SE, and S&MA?

- How does a project allocate the responsibilities of protecting against faults, predicting future failures, and post-facto analysis?
- To what extent should mission type drive the approach to integrating FM? Consider the following mission types and related factors: Human flight vs. robotic; single mission vs. repetitive flight; deep space vs. Earth orbiter; mission size, duration, and complexity.

The format, a combination of panelist presentations and discussions between the panelists and attendees, was designed to promote discussion and identification of issues regarding the scope and implementation of FM across NASA. The workshop panelists were chosen to provide a range of viewpoints across NASA, NASA's partners, and academia.

Moderated by Marilyn Newhouse/MSFC/Computer Sciences Corporation (CSC), the workshop started with a short statement by each panelist.

Michael Aguilar, who manages the software program at GSFC and serves as the NESC Discipline Expert in Software Engineering, concentrated on FM processes within a project or program. He pointed out that the traditional "waterfall" approach to FM encounters problems because it expects a complete set of mature documents, which are not available until too late in the development cycle, to drive the FM implementation. He emphasized the FM practitioners need to change their viewpoint to become involved early in the upfront design of the whole system. In his model, FM architectures would be reviewed early, FM, including FM test plans, would be at a level of maturity at the system PDR and CDR commensurate with the system maturity, and FM architectures and designs would be presented at reviews directly from the development tools. Taken together, these would ensure that the FM solution was not driven by an overly defined set of low-level design requirements before the system as a whole had been defined.

George Cancro, Assistant Group Supervisor in the Space Department at JHU/APL, also addressed the need for disciplined FM processes. He emphasized starting early in phase A with a definition of the FM philosophy for the mission. He also encouraged the development of metrics, citing the need for comparative measures of FM complexity across missions as a starting point for cost and schedule estimates, a separate work breakdown structure for FM to help communicate the importance and complexity of FM to management, and a detailed schedule to help articulate early what is expected of FM and what is involved in its development. Making the point that the resources required for testing is a significant limiting factor for FM implementations, he emphasized the need to focus from the beginning on testing as a means to identify when FM is "done."

Carlos Garcia-Galan, the Deputy Manager for Mission and Systems Integration on the Multi-Purpose Crew Vehicle (MPCV) project at JSC, talked about the lessons learned from implementation of FM in the Constellation program. Initially within Constellation, there was no integrated FM team and each project had its own

approach to FM. There was also an initial attempt to take all requirements into account, which became impractical because of budget restrictions. Subsequent redefinitions of Orion allowed a redefinition of the approach to FM and allowed them to move forward with one integrated, focused, and smaller team, taking a top-down approach to assessing responses to unknown unknowns rather than a bottom-up approach reacting to every event.

Steven Johnson, Analysis Lead for SLS Mission and FM at MSFC and Associate Research Professor with the Center for Space Studies at University of Colorado Colorado Springs, discussed the theoretical, practical, and organizational bases for the challenges to implementing FM within NASA. From a theoretical perspective, he sees FM as an operational subset of SHM and as metacontrol loops within FDIR. From a practical perspective, FM is a nested set of control loops operating at different speeds, implemented by different automated or manual mechanisms, and split between flight and ground. Organizationally, FM is split among multiple teams (e.g., FM development and S&MA) and organizations (e.g., JSC, Kennedy Space Center, MSFC, and Stennis Space Center using the SLS as an example). He identified the need to assess and integrate these roles and responsibilities for effective FM implementation within a program or project.

Robert Rasmussen, a JPL Technical Fellow, emphasized the interrelationship between FM and SE. FM cannot be implemented post facto but must be engineered into the system as part of a concurrent process. Success (achieving mission objectives) and failures (obstacles to achieving mission objectives) are inseparable. Citing earlier workshop presentations, he questioned whether there is a meaningful separation between FM and SE. Drawing a parallel to physics, he asked whether the community should be concentrating on defining a theory of FM or looking for a unified theory of SE architecture from which FM will either be identified as separate discipline or be subsumed into the SE process. He emphasized that although FM practitioners do need to focus on the underlying purpose to FM—handling potential failures—they can't lose sight of the SE perspective on achieving mission objectives.

Jonathan Wilmot, Software Architect for the Goddard core Flight Executive (cFE) and Core Flight System (CFS) software product lines at GFSC, emphasized the importance of the interaction between FSW and FM engineering for the implementation of FM capabilities. He described the GSFC "plug and play" approach to FSW architecture as a means to facilitate FM implementation and ensure that FM is not dependent on a single solution (rule based or goal based). He also emphasized partitioning into virtual processors to simplify the FM implementation by separating it into different goals and timing scenarios.

The panel presentations were followed by an open discussion between the workshop participants and the panelists that in many cases started to tie together the earlier presentations, the discussions at the breakout sessions, and the panelists' comments. There appeared to be a general consensus that the following issues were key, even if final or optimal solutions had not been identified:

- FM needs to be addressed early in formulation by identifying an FM lead and defining the project FM philosophy and scope. FM needs to incorporate fundamental processes for defining metrics (e.g., complexity and completeness), estimating costs, setting schedules, and tracking progress. FM needs to mature in parallel with the system so that off-nominal and nominal requirements are addressed commensurately.
- The FM community needs to educate management regarding the importance of including FM early in the formulation and development process and assigning clear authority and responsibility for FM development. The panelists noted their success stories that arose directly from taking steps to promote early, cohesive FM engineering: APL's implementation of FM for RBSP and JSC's integrated approach to FM for Orion.
- FM V&V needs to be viewed as a full life cycle activity starting before PDR and as a constraint on the final FM capabilities. There was concern that we are doing a great job building systems that we can't test and that the fast expansion of FM complexity is keeping pace with, or exceeding, the increasing capabilities for simulation. The community needs to address the extent to which processes, a systems approach, and new tools can ensure FM V&V cost effectively meets the mission needs.
- FM engineers need to incorporate an operations perspective and be integrated with operational teams, not only to provide subject-matter expert support during operations but also to feed operational lessons learned back into the FM process.
- FM is still lacking the tools to facilitate architecture definition and evaluation, design, implementation, and testing of FM systems and to present the FM architecture and design effectively at system reviews.

However, there was still considerable discussion ranging around the more philosophical concepts:

- Does drawing a line between off-nominal (FM) and nominal (SE) processes help or hinder the development of a system? Is the formal separation between fault and failure a requirement, an aid, or an oversimplification? Does it matter who or what is responsible for a failure, or only that a failure can occur? At what point does responding to a warning (potential failure) become FM?
- The panel debated about the need to consider FM as an engineering discipline and assign FM responsibility and authority (for example, by assigning FM leads or cost account managers) versus the need to look at off-nominal and nominal conditions from the systems perspective. In addition, panelists discussed the relationship between S&MA and FM, and whether FM is a part of, or an adjunct to, ISHM.

Some of the differences appeared to be across mission types (robotic missions vs. human spaceflight, one-off spacecraft vs. reusable systems). In other cases, the

differences appeared to be institutional or to derive from individual experiences and lessons learned. All of the views have strong arguments in their favor, addressing the issues, concerns, and goals of protecting NASA missions. Each speaker, whether panelist or participant, could cite specific instances in support of their view: cases where, in their experience, a specific definition, process, or approach either had helped or had created a problem that needed to be overcome.

Given the broad nature of the areas without a clear consensus, it might be reasonable to rethink the original question and ask instead:

- Do we need a grand unifying theory for FM? Is there a single approach applicable to robotic low-Earth and deep-space missions, human spaceflight, and aeronautics; and is that approach beneficial?
- Are the questions of architecture, approach, and roles better addressed at the program or project level, based on fundamental principles (e.g., early involvement and parallel maturation) and case studies of the trades represented by the various architectures and approaches?

Conclusions and Continuing Work

The 2012 NASA FM Workshop was very successful and, in many ways, exceeded expectations (see Appendix D: Workshop Survey Feedback). Combining invited and formal speakers to broaden the participants' understanding of current FM theory, approaches, and activities both across and outside of NASA with breakout sessions designed to encourage discussion and networking, the workshop helped the FM community to understand the issues and synergies that cross mission domain areas. However, there is significant work remaining as FM matures as an engineering discipline:

- The foremost priority is completion of the first version of the NASA FM Handbook. The discussions and conclusions of the various workshop activities need to be used to resolve the remaining comments from the community's review of the draft handbook. On the basis of this work, connections, links, and references to/from other NASA documents (e.g., NASA Procedural Requirements and the SE and software handbooks) should be identified and any resulting changes to the documents should be drafted and submitted.
- The FM community should pursue the architecture assessment process from Focus Area 1 to identify the characteristics that drive and measure FM performance across mission domains phases. This would provide FM practitioners with the critical criteria, information, and tools required to make informed decisions during architecture trade studies.
- The capabilities roadmap development effort from Focus Area 2 needs to be continued within the FM community, and the resulting roadmaps need to be

finalized and submitted to the NASA Office of the Chief Technologist for consideration.

- Discussion of fundamental issues—the interrelationship between nominal and off-nominal approaches and architectures; the relationship between SE, S&MA, and FM and the possibilities for a more unified approach to HM; the applicability of model-based approaches; and approaches for simplifying the V&V process, among others—needs to continue across the broader community to take advantage of the experience from the various institutions and mission domains.
- Ultimately, the NASA FM community needs to be extended to include all mission domains, including operations, aeronautics, and ground systems.

All of these require that the FM community flourish, maintaining the momentum from the FM workshop. The first FM workshop was in 2008; it is highly desirable to bring the FM community together more often than every 4 years. Until now, NASA's SMD has carried the cost for the FM workshop and much of the handbook activities, despite the fact that the scope of the work extends beyond development and operation of the robotic spacecraft that are at the heart of the SMD charter. The SMD budget is unlikely to be able to sustain this unilateral support.

In this budget environment, alternative approaches may help to maintain the momentum from the FM Workshop. The FM CoP can be used to continue discussions started at the workshop. "Virtual" workshops, such as the virtual conference approach used by the Astrobiology Institute at NASA's ARC, may provide a cost-effective means of bringing the FM community together more frequently. The possibility of joint sponsorship of FM conferences with other industry or government partners should be explored to allow cost sharing and to allow the collaboration to continue. The maturation of FM as an engineering discipline, along with the associated processes and tools, is too important to NASA's success to allow the momentum from the 2012 FM Workshop to fade.

Acknowledgments

- **Venue arrangements**: Pauline Burgess and Michelle Hensen, NASA Research and Education Support Services
- **Steering Committee:**
    - Lindley Johnson, HQ/SMD – sponsor for this workshop and the FM Handbook
    - Neil Dennehy, GSFC/NESC – cosponsor of the FM Handbook
    - Steve Scott, GSFC/OCE
    - Brian Muirhead, JPL/Caltech OCE
    - George Cancro, JHU/APL
    - Pat Martin, HQ/OSMA
    - Tim Crumbley, MSFC/OCE and Standards Office Manager

    - Ken Ledbetter, HQ/OCE
    - Carlos Garcia-Galan, JSC/Mission Operations Directorate
    - Jeri Briscoe, MSFC/Discovery, New Frontiers Office
    - Frank Groen, HQ/OSMA
- **FM Architecture Trade Session Leads**: Kevin Barltrop (JPL/Caltech), David Garlan (Carnegie Mellon University), John Day (JPL/Caltech)
- **FM Capabilities Roadmap Session Leads**: Ken Costello (IV&V Facility), Mitch Ingham (JPL/Caltech)
- **Facilitators**: Daria Topousis, Chris Eng, Alex Kadesh (JPL/Caltech)
- **Photographer**: Eric Bordelon (NESC)
- **Videographer:** Ryan Sott (NASA Safety Center)

Appendix A: Workshop Agenda

2012 NASA SPACECRAFT FAULT MANAGEMENT WORKSHOP

April 10-12 2012
New Orleans, Louisiana

Day 1 - April 10, 2012

7:00 AM	QB	**Registration**
8:00 AM		**Introductions, Purpose, Goals** - Lorraine Fesq
8:15 AM		**Welcome** - Lindley Johnson
8:30 AM		**Agenda, Logistics, FM Handbook Status**
8:45 AM		**JPL/CalTech** - Brian Muirhead, "Coalescing NASA's Views of Fault and Health Management"
		JHU/APL - Kris Fretz, "Recent Progress in FM"
9:45 AM		Break
10:00 AM	QB	**Focus Area: "Assessing FM architectures"**
10:15 AM		**NASA/MSFC** - Jon Patterson, "Analytical Approaches to Guide Space Launch System FM Development"
10:45 AM		**NASA/JSC** - Carlos Garcia-Galan, "FM for Crewed Missions"
11:15 AM		**Aerospace Corp** - Phillip Schmidt, "Independent Assessment of NASA Fault Management System Architectures"
11:45 AM		**AFRL/W-P** - Mark Derriso, "State Awareness and Decision-Making Architecture"
12:15 PM	QB	**Lunch - Invited Speaker: Michael Aguilar** NASA GSFC, NESC Software Tech Fellow "Fault Management using MBSE Tools and Techniques"
1:15 PM	QB	**Focus Area: "Developing a FM Capabilities Roadmap"**
1:30 PM		**NASA/ARC** - Mark Schwabacher, "Human Spaceflight ISHM Technology Development"
2:00 PM		**NASA/ARC** - Robert Mah, "System-Wide Safety Assurance Technologies"
2:30 PM		**JPL/CalTech** - Mitch Ingham, "No more Band-Aids: Integrating FM into the Onboard Execution Architecture"
3:00 PM		**JPL/CalTech** - Dan Dvorak, "Model-Based Systems Engineering (MBSE) and Goal-Based FM"
3:30 PM		**NASA/JSC** - Lui Wang, "Modeling Failure Modes with SysML"
4:00 PM		Break
4:15 AM	QB	**NASA/MSFC, UCCS/Jacobs** - Stephen Johnson, "FM Technical Performance Metrics"
4:45 PM		**AFRL/W-P** - Mark Derriso, "AFRL's ISHM Journey and Future Plans"
5:15 PM	QP	**Steering Committee Meeting**
5:30 PM	IB	**Reception** **Iberville and Bienville Rooms - Second Floor**
7:30 PM		

Day 2 - April 11, 2012

8:00 AM	QB	**Invited Speaker: Dr. Werner Dahm** Director, Security and Defense Systems Initiative Ira A. Fulton Schools of Engineering, Arizona State University "ISHM: Applications and Challenges on the Horizon"			
9:00 AM		**FM Capabilities Roadmap Session Overview** - Ken Costello, Session Chair (IV&V Facility) and Mitch Ingham (JPL)			
9:30 AM		**Architecture Evaluation Session Overview** - John Day, Session Chair (JPL) and David Garlan (CMU)			
10:00 AM		**Breakout Sessions: Logistics**			
10:15 AM		Break			
10:30 AM	BC	**Architecture Evaluation Session - US Persons only** QP Breakout Session US Breakout Session	OR	**Capabilities Roadmap Session - US Persons only** PR Breakout Session GS Breakout Session	
12:30 PM	LN	**Lunch**	LN	**Steering Committee Meeting**	
1:15 PM	BC	**Architecture Evaluation Session - US Persons only** QP Breakout Session US Breakout Session	OR	**Capabilities Roadmap Session - US Persons only** PR Breakout Session GS Breakout Session	
2:45 PM		Break			
3:00 PM	BC	**Architecture Evaluation Session - US Persons only** QP Breakout Session US Breakout Session	OR	**Capabilities Roadmap Session - US Persons only** PR Breakout Session GS Breakout Session	
5:00 PM	RS	**Steering Committee Meeting**			

Day 3 - April 12, 2012

8:00 AM	QB	**Invited Speaker: Dr. Algirdas Avizienis** Distinguished UCLA Emeritus Professor "Terminology Issues in Dependable Computing"		
8:45 AM		**JPL/CalTech** - Steve Jenkins, "FM Ontology"		
9:15 AM		**NASA/ARC** - Peter Robinson, "FM as a Control System"		
9:45 AM		**NASA/OSMA** - Frank Groen, "FM in an Objectives-Based/Risk-Informed View of Safety and Mission Success"		
10:15 AM		Break		
10:30 AM	QB	**Panel Discussion: "Integrating FM: How Does It Fit?"** **Panel Moderator:** Marilyn Newhouse, MSFC/CSC **Panelists:** Michael Aguilar, NESC; Michael Brieden, JSC; George Cancro, APL; Stephen Johnson, MSFC/UCCS; Bob Rasmussen, JPL; Jonathan Wilmot, GSFC		
12:00 PM	LN	**Lunch**	LN	**Steering Committee Meeting**
1:00 PM	QB	**Architecture Evaluation Report & Discussion - US Persons only** John Day (JPL) and David Garlan (CMU)		
2:00 PM	QB	**Capabilities Roadmap Report & Discussion - US Persons only** Ken Costello (IV&V Facility) and Mitch Ingham (JPL)		
3:00 PM	QB	**Closing Remarks**		
3:30 PM	QB	**Steering Committee Meeting**		

Room Legend		
Mezzanine	QB	Queen Anne Ballroom
	BC	Bonnet Carre Room
	OR	Orleans Room
	QP	Queen Anne Parlor
	LN	La Nouvelle East
	IB	Iberville/Bienville Rooms
Second Floor	US	Ursaline Salon
	PR	Pontalba Room
	GS	Gallier Salon
	RS	Royal Salon B

Appendix B: Workshop Attendee List

Aguilar, Michael	Goddard Space Flight Center (GSFC)	Michael.L.Aguilar@nasa.gov
Avizienis, Algirdas	University of California, Los Angeles (UCLA)	aviz@cs.ucla.edu
Bajwa, Anupa	Ames Research Center (ARC)	Anupa.R.Bajwa@nasa.gov
Bareh, Magdy	Jet Propulsion Laboratory (JPL)/California Institute of Technology (Caltech)	magdy.s.bareh@jpl.nasa.gov
Barley, Bryan	Marshall Space Flight Center (MSFC)	Bryan.Barley@nasa.gov
Barnes, Arnold	Ball	cbarnes@ball.com
Barszcz, Eric	ARC	Eric.Barszcz@nasa.gov
Bauer, Brian	The Johns Hopkins University Applied Physic Laboratory (JHU/APL)	Brian.Bauer@jhuapl.edu
Berg, Peter	ARC - Stinger Ghaffarian Technologies	Peter.Berg@nasa.gov
Breger, Louis	Massachusetts Institute of Technology (MIT)	lbreger@alum.mit.edu
Briscoe, Jeri	MSFC	Jeri.M.Briscoe@nasa.gov
Brown, Mark	JPL/Caltech	G.M.Brown@jpl.nasa.gov
Brueck, Donald	Aerospace	donald.brueck@aero.org
Burgess, Pauline	NASA Research and Education Support Services (NRESS)	pburgess@nasaprs.com
Cancro, George	JHU/APL	George.Cancro@jhuapl.edu
Class, Brian	Orbital Sciences Corp	class.brian@orbital.com
Costello, Kenneth	Independent Verification and Validation (IV&V) Facility	kenneth.a.costello@nasa.gov
Crumbley, Tim	MSFC	Robert.T.Crumbley@nasa.gov
Dahm, Werner	Arizona State University	Werner.Dahm@asu.edu
D'Andrea, Bruce	Orbital Sciences Corporation (OSC)	
Das, Santanu	ARC – University of California, Santa Cruz	santanu.das-1@nasa.gov
Day, John	JPL/Caltech	John.C.Day@jpl.nasa.gov
Dennehy, Cornelius	GSFC	Cornelius.J.Dennehy@nasa.gov
Derriso, Mark	AFRL- Wright-Patterson Air Force Base	Mark.Derriso@wpafb.af.mil
DiStefano, Sal	JPL/Caltech	Salvador.Distefano@jpl.nasa.gov
Dolloff, Matthew	Glenn Research Center	matthew.d.dolloff@nasa.gov
Dvorak, Dan	JPL/Caltech	Daniel.L.Dvorak@jpl.nasa.gov
Eng, Chris	JPL/Caltech	christopher.m.eng@jpl.nasa.gov
Fesq, Lorraine	JPL/Caltech	Lorraine.M.Fesq@jpl.nasa.gov
Figueroa, Fernando	Stennis Space Center (SSC)	Fernando.Figueroa-1@nasa.gov
Frazier, Dave	L-3 Stratis	dave.frazier@l-3com.com
Fretz, Kristin	JHU/APL	Kristin.Fretz@jhuapl.edu
Friberg, Ken	Friberg Autonomy	Friberg.Autonomy@gmail.com
Garcia-Galan, Carlos	Johnson Space Center (JSC)	Carlos.Garcia-Galan-1@nasa.gov

Garlan, David	Carnegie Mellon University	Garlan@cs.cmu.edu
Ghoshal, Sudipto	Qualtech Systems, Inc.	sudipto@teamqsi.com
Glass, Betty	Lockheed Martin	Betty.C.Glass@lmco.com
Goebel, Kai	ARC	Kai.Goebel@nasa.gov
Gonzalez, Oscar	GSFC	oscar.gonzalez-1@nasa.gov
Groen, Frank	NASA Headquarters (HQ)/OSMA	Frank.J.Groen@nasa.gov
Hagerman, Seana	Lockheed Martin	
Henson, Michelle	NRESS	mhenson@nasaprs.com
Hill, Adrian	JHU/APL	Adrian.Hill@jhuapl.edu
Hoffman, Tom	JPL/Caltech	Tom.L.Hoffman@jpl.nasa.gov
Hogan, Steve	Aerospace	Steven.L.Hogan@aero.org
Hushka, Thomas	MSFC - Teledyne Brown	thomas.l.hushka@nasa.gov
Jenkins, Steven	JPL/Caltech	j.s.jenkins@jpl.nasa.gov
Johnson, Jeremy	ARC - Stinger Ghaffarian	jeremy.r.johnson@nasa.gov
Johnson, Lindley	HQ	Lindley.Johnson-1@nasa.gov
Johnson, Stephen	MSFC - University of Colorado	Stephen.B.Johnson@nasa.gov
Jones, Maggie	SSC	marguerite.t.jones@nasa.gov
Kadesch, Alex	JPL/Caltech	alexander.c.kadesch@jpl.nasa.gov
Keith, Lloyd	JPL/Caltech	raymond.l.keith@jpl.nasa.gov
Knickerbocker, Gary	MSFC	gary.knickerbocker@nasa.gov
Kolcio-Prather, Ksenia	Okean Solutions	Ksenia@okeansolutions.com
Kubota, Sanae	JHU/APL	Sanae.Kubota@jhuapl.edu
Larson, Richard	Dryden Flight Research Center (DFRC)	Richard.R.Larson@nasa.gov
Lebsock, Ken	GSFC - Orbital Sciences Corporation	Kenneth.L.Lebsock@nasa.gov
Lee, Gene	JPL/Caltech	gene.y.lee@jpl.nasa.gov
Lennon, Jamie	Naval Research Laboratory	jlennon@space.nrl.navy.mil
Lewandowski, Edward	GRC	edward.j.lewandowski@nasa.gov
Mah, Robert	ARC	robert.w.mah@nasa.gov
Malin, Jane	JSC	jane.t.malin@nasa.gov
Martin, Patrick	HQ	Patrick.Martin@nasa.gov
Maultsby, Doug	Lockheed Martin	
Melcher, Kevin	GRC	kjmelcher@nasa.gov
Miller, Sheena	JSC - Barrios	sheena.j.miller@nasa.gov
Morillo, Ron	JPL/Caltech	Ronald.Morillo@jpl.nasa.gov
Morin, Lee	JSC	lee.m.morin@nasa.gov
Muirhead, Brian	JPL/Caltech	Brian.K.Muirhead@jpl.nasa.gov
Newhouse, Marilyn	MSFC/Computer Sciences Corporation (CSC)	Marilyn.E.Newhouse@nasa.gov
Nikora, Allen	JPL/Caltech	Allen.P.Nikora@jpl.nasa.gov
O'Hagan, Brian	JSC	brian.ohagan-1@nasa.gov

Okon, Shira	Tietronix	Shira.Okon@tietronix.com
Patrick, Keith	Northrop Grumman Corporation	keith.patrick@ngc.com
Patterson, Jon	MSFC	Jon.Patterson@nasa.gov
Phillipsen, Paul	WASK Engineering, Inc.	paulp@waskengr.com
Pisanich, Gregory	ARC - Stinger Ghaffarian	gregory.m.pisanich@nasa.gov
Pope, Joseph	Aerospace	Joseph.T.Pope@aero.org
Racine, Roger	Draper Laboratory	rracine@draper.com
Rasmussen, Robert	JPL/Caltech	Robert.D.Rasmussen@jpl.nasa.gov
Rathgeber, Kurt	White Sands Test Facility	kurt.a.rathgeber@nasa.gov
Regenie, Vicki	DFRC	victoria.a.regenie@nasa.gov
Robinson, Peter	ARC	Peter.I.Robinson@nasa.gov
Rosendall, Paul	JHU/APL	Paul.Rosendall@jhuapl.edu
Rustick, Jonathan	Orbital Sciences	Rustick.Jonathan@orbital.com
Schmidt, Phillip	Aerospace	Phillip.P.Schmidt@aero.org
Schwabacher, Mark	ARC	Mark.A.Schwabacher@nasa.gov
Seale, Eric	Lockheed Martin	Eric.H.Seale@lmco.com
Standley, Shaun	JPL/Caltech	shaun.p.standley@nasa.gov
Susarla, Sarma	L3 Communications	svsusarla@hotmail.com
Thiel, Laurie	Integrity Applications	lthiel@integrity-apps.com
Thomas, Helen	MSFC	Helen.L.Thomas@nasa.gov
Thompson, Jerry	MSFC	Jerry.T.Thompson@nasa.gov
Tillman, Judy	Northrop Grumman Corporation	Judy.Tillman@ngc.com
Topousis, Daria	JPL/Caltech	daria.e.topousis@jpl.nasa.gov
Wang, Lui	JSC	lui.wang-1@nasa.gov
Watson, Michael	MSFC	Michael.D.Watson@msfc.nasa.gov
West, John	Draper Laboratory	jwest@draper.com
Williams, Marcella	IV&V Facility - TASC	marcella.williams@ivv.nasa.gov
Wilmot, Jonathan	GSFC	Jonathan.J.Wilmot@nasa.gov
Zinchuk, Jeff	Draper Laboratory	Jeff@draper.com

Appendix C: FM Capabilities Roadmaps Developed During the Workshop

The roadmaps developed during the Capabilities Roadmap Breakout Session in each of the domain areas are shown in Figure C-1 through Figure C-6. Each roadmap shows the planned or proposed missions over the next 10+ years and the FM capabilities and technologies envisioned in support of these missions. Note that each team used different graphical representations to highlight time-critical, enabling, or nice-to-have capabilities and technologies.

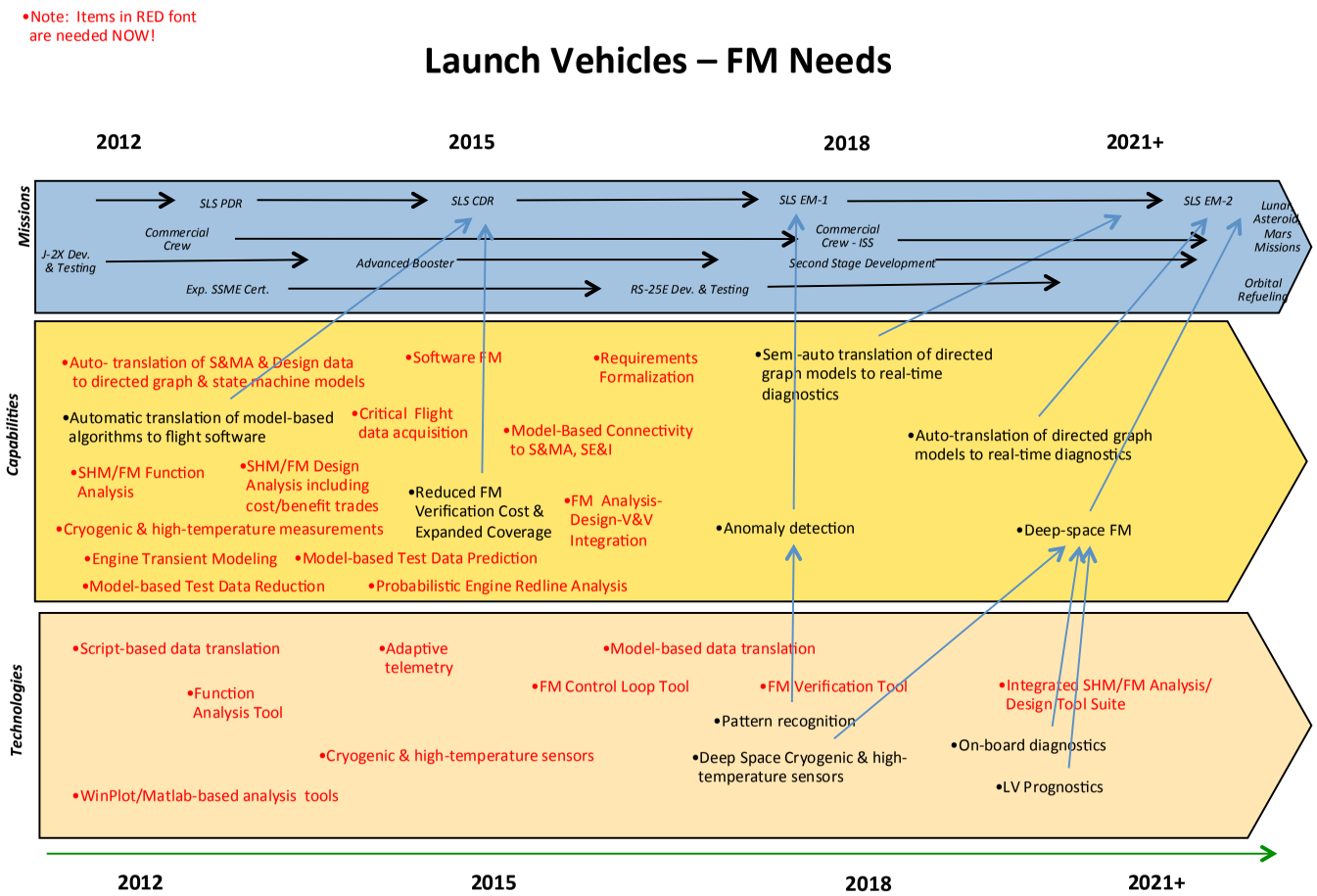

Figure C-1. Draft FM Capabilities Roadmap developed during the workshop for launch vehicles.

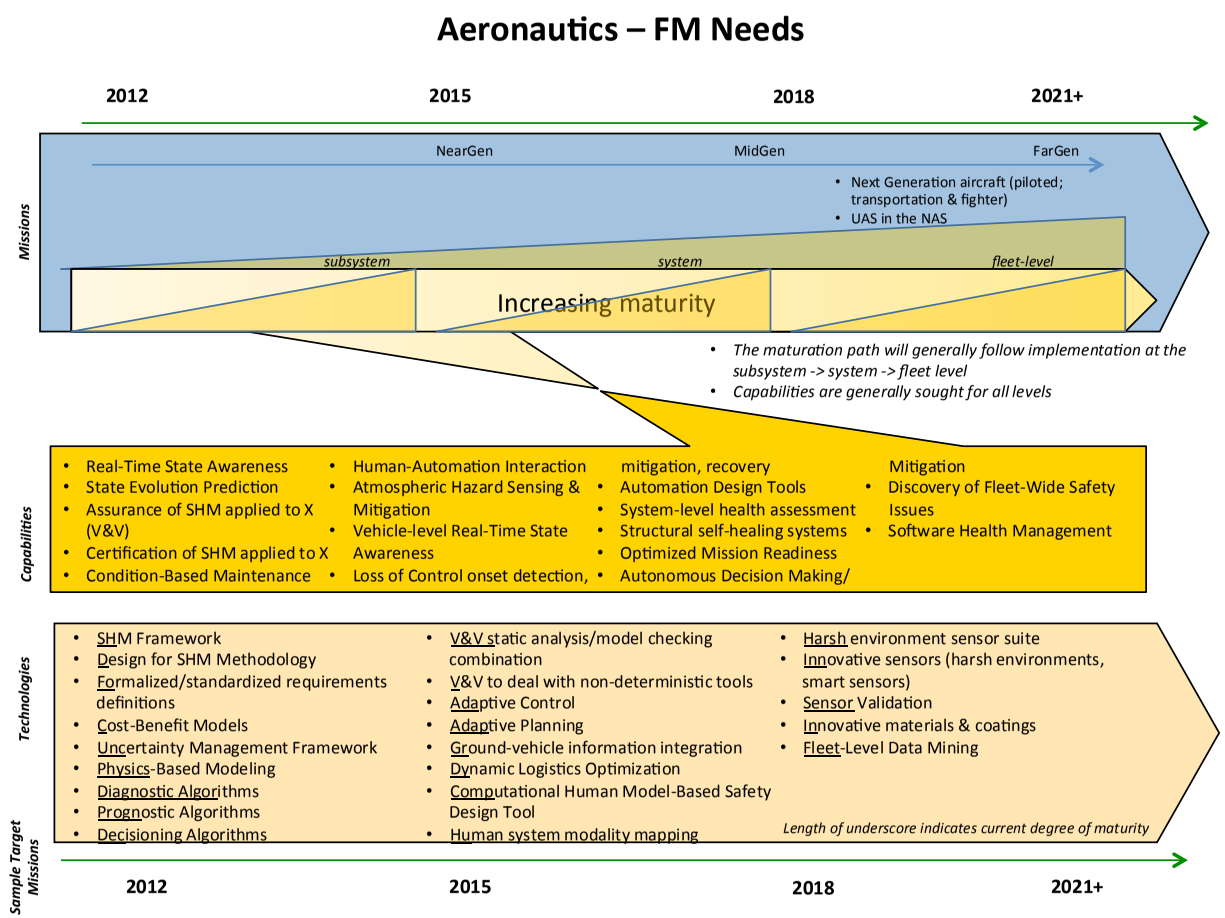

Figure C-2. Draft FM Capabilities Roadmap developed during the workshop for aeronautics.

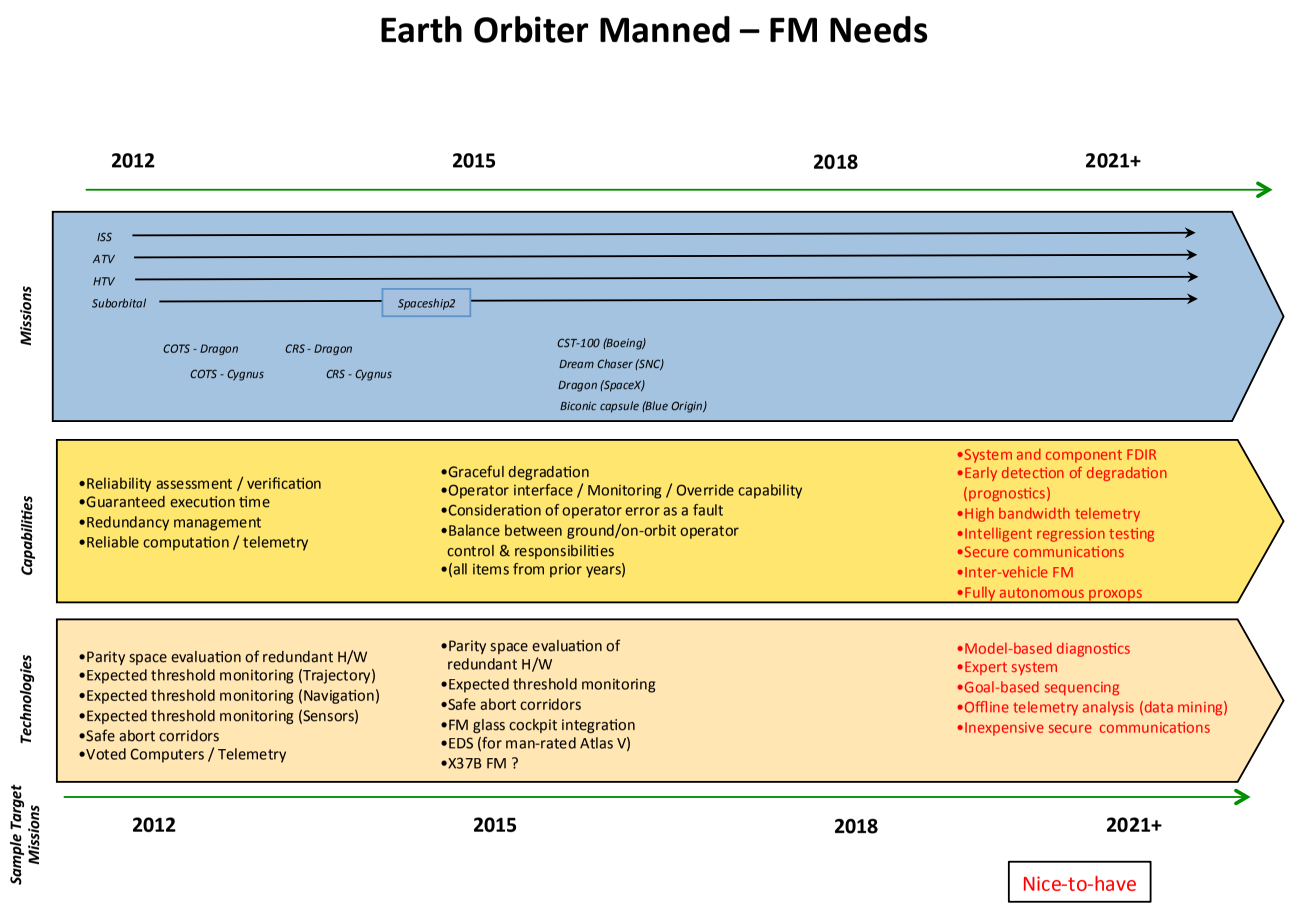

Figure C-3. Draft FM Capabilities Roadmap developed during the workshop for manned Earth orbiter missions.

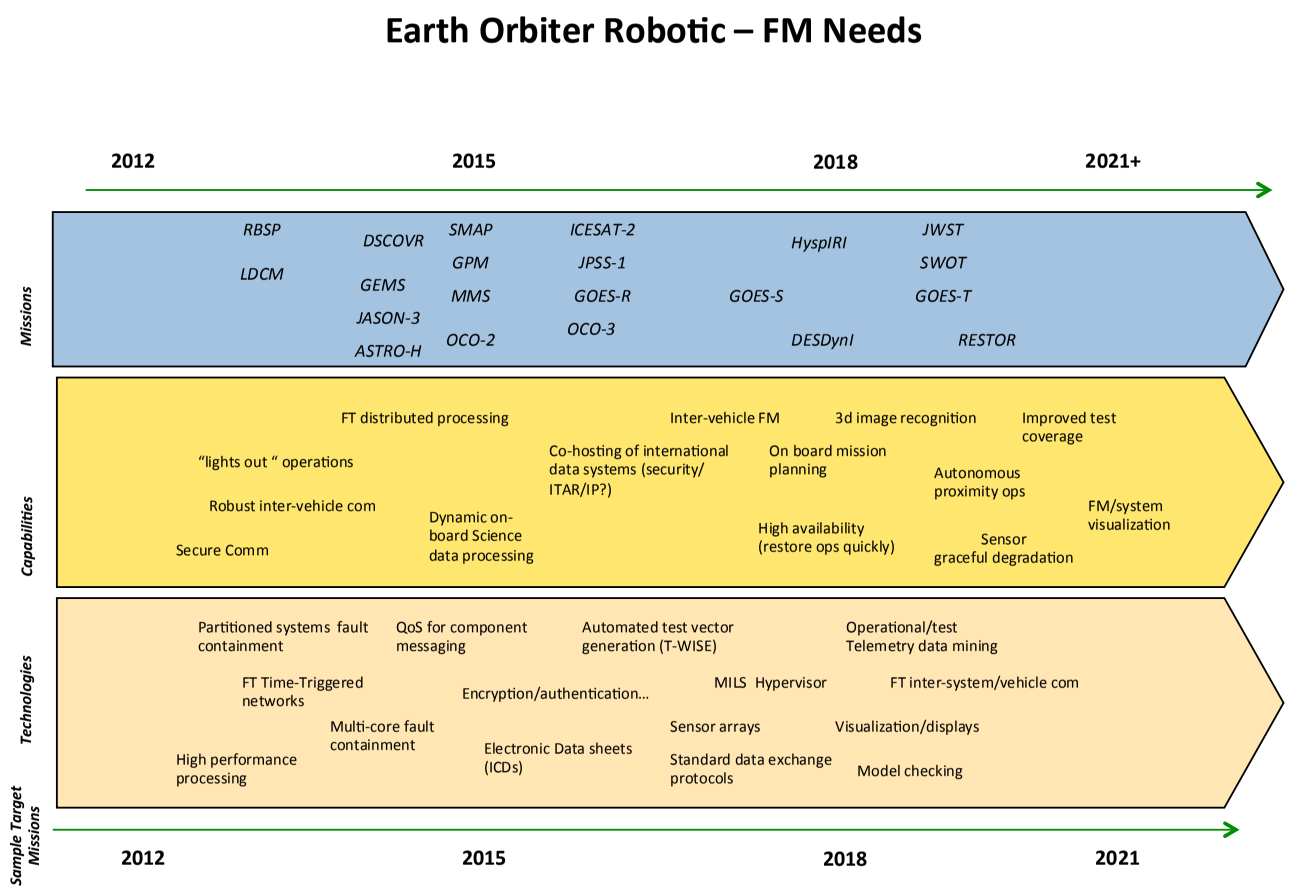

Figure C-4. Draft FM Capabilities Roadmap developed during the workshop for robotic Earth orbiter missions.

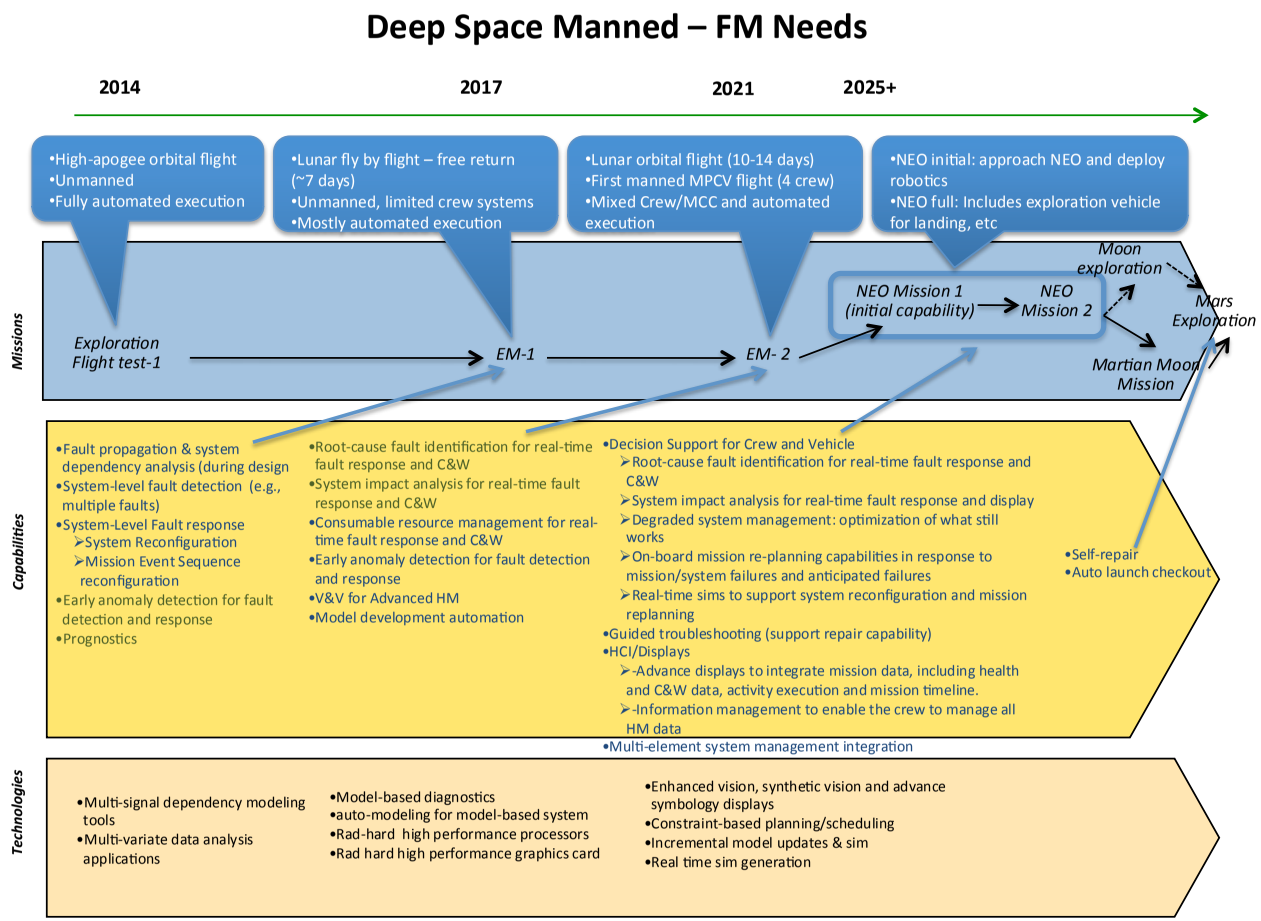

Figure C-5. Draft FM Capabilities Roadmap developed during the workshop for manned deep space missions.

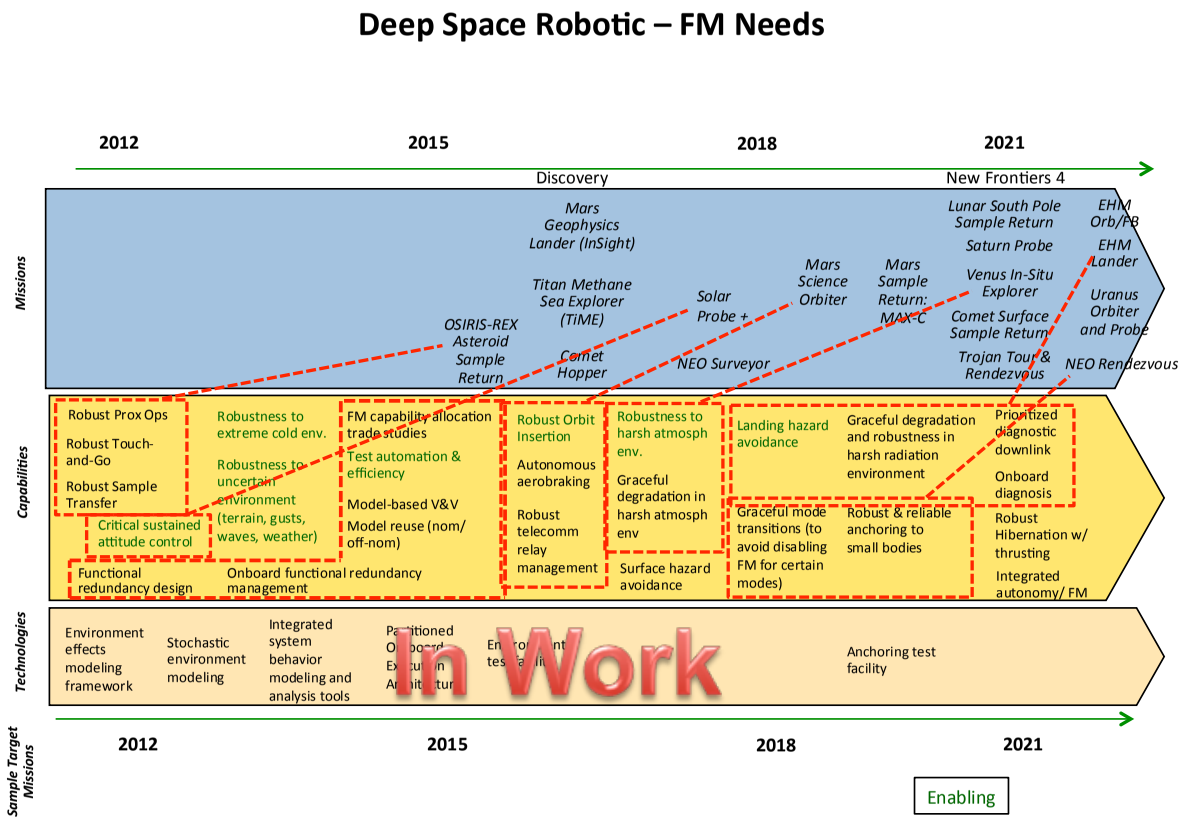

Figure C-6. Draft FM Capabilities Roadmap developed during the workshop for deep-space robotic missions.

Appendix D: Workshop Survey Feedback

Participants' feedback on the workshop venue, organization, and content was very positive. The following comments are representative of the responses received.

- High-quality presentations; lots of opportunity for establishing collaborations
- Good discussions about what is needed to design a fault management system
- The mix of people, the case studies, the quality of the presentations, the pralines
- Capabilities roadmapping was useful - Dahm's presentation was outstanding
- Very well prepared and executed allowing focus on topics and distribution of relevant information
- The opportunity to hear and consider varying views on FM
- Good quality, quantity, and diversity of participants. Featured speakers were excellent
- Very good breadth of speakers with differing opinions so we got the chance to evaluate differing ideas/opinions/facts
- Great presentations *and* off-line discussions; open atmosphere—people willing to share experience
- The speakers were wonderful. There were a variety of viewpoints, topics ranging from lessons learned to future challenges, theory and practice, etc. I feel that I really learned a lot about what work is going on in the field
- Interactive sessions, effort to bring in FM experts and users from multicenters, other agencies. Food :) Definitely recognized the value of convening this group and "cross-pollinating"
- The webcast was the best that I have Ever experienced
- You provided a broad perspective on many aspects of fault management - past case studies, recent work, future ideas, etc. The dialog and debate was insightful
- Simply hearing about the FM architecture on different missions was truly fascinating

Appendix E: The Formation of NASA's Fault Management Community of Practice

To coalesce the fault management (FM) field and establish it as an engineering discipline, NASA created the Fault Management Community of Practice (FM CoP) website on the NASA Engineering Network (NEN) (https://nen.nasa.gov/web/faultmanagement/home). A community of practice (CoP) is a group of people "who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in this area by interacting on an ongoing basis."[8] By deepening their own knowledge, they are able to improve the performance of an organization as a whole. Communities have existed throughout history, through organizations such as guilds and professional societies like AIAA, ASME, and IEEE, but until recently they were not formally and strategically established within the aerospace industry. CoPs not only are an effective means for capturing, sharing, and using knowledge, but also provide a means for collaboration and innovation. They have become a more prevalent component of knowledge management strategies and many major organizations.[9] Communities focus on connecting the workforce across organizations, projects, geographies, and functions—these connections were exactly what NASA was seeking.[10]

Because of the geographically distributed nature of NASA, communities required an online presence that would be open to all personnel behind the firewall. In addition, many of the core competencies have hundreds of practitioners, so routine face-to-face or teleconference meetings were simply not feasible. The online sites would have to become the gathering point for these practitioners. See Figure E-1 for a snapshot of the FM CoP homepage.

---

[8] Wenger, E., McDermott R., and Snyder, W. M. *Cultivating Communities of Practice.* Harvard Business School Press, Cambridge, 2002.

[9] Lesser, E., and Everest, K. "Using communities of practice to manage intellectual capital." *Ivey Business Journal* Vol. 65, No. 4, pp. 37–41, 2001.

[10] APQC. "Sustaining effective communities of practice: an overview of findings from APQC's collaborative research." APQC, 2010.

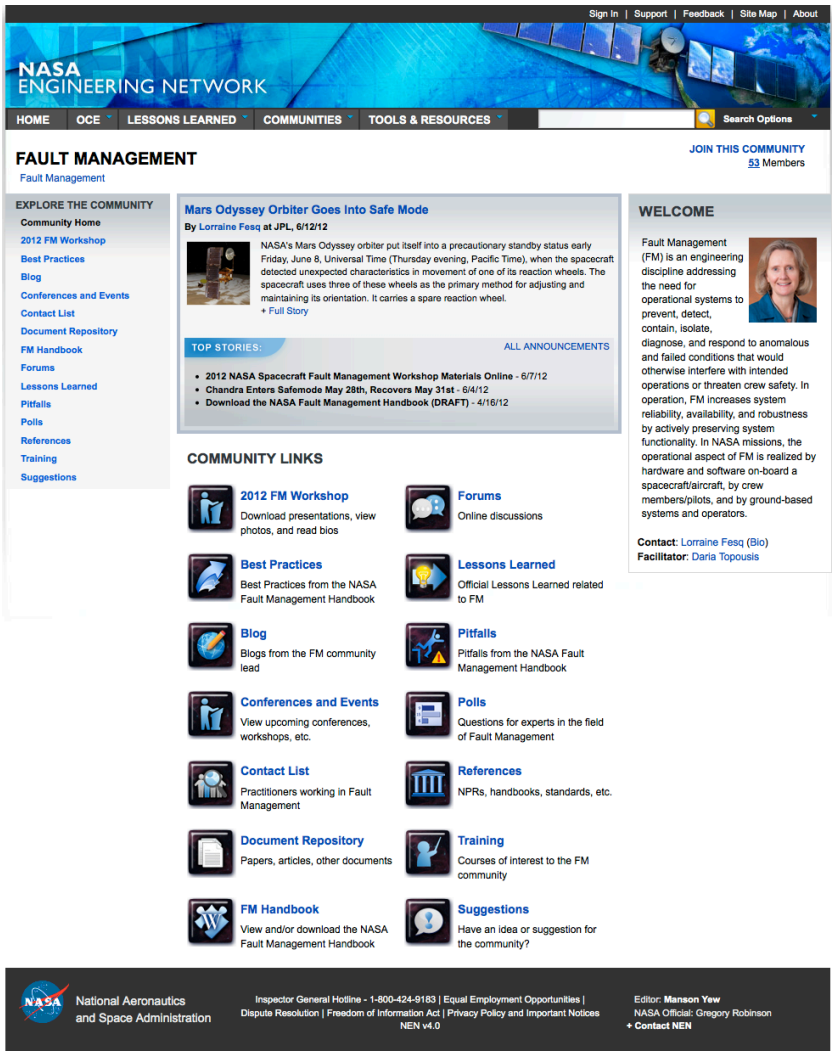

Figure E-1. NASA's FM CoP website.

CoPs can help NASA both capture undocumented engineering "tribal knowledge" before it walks out the door and overcome the inhibiting effects of insular professional development in rigidly stovepiped organizations. For FM, the benefits of creating a CoP included the specific objective of supporting the development and coalescing of this new and emerging engineering discipline that is still in the formative stage. FM is a nontraditional (relative to, say, the structures discipline) engineering activity most often affiliated with the systems engineering discipline or the software engineering discipline. FM encompasses functions that enable an operational system to prevent, detect, isolate, diagnose, and respond to anomalous and failed conditions interfering with intended operations. FM focuses on the off-

nominal behavior of a system, and it is a subsystem in its own right found on most NASA spacecraft. Similar to guidance, navigation, and control (GN&C), avionics, structures, etc., FM is a subsystem that must be architected, designed, developed, integrated, tested, and operated by NASA engineers, scientists, and technicians. From a methodological perspective, FM includes processes to analyze, specify, design, verify, and validate these functions. From a technological perspective, FM includes the hardware and control elements, often embodied in sensors, software, and procedures, of an operational system by which the capability is realized to autonomously respond to faults, anomalous conditions, and hazards. For example, a robust onboard FM system, tightly integrated with an autonomous GN&C system, is envisioned to be key element of any future NASA space platform operating beyond low Earth orbit.

Clearly, FM engineering is an important part of the complex worlds of both human and robotic spaceflight at NASA, but it is not easy to define, understand, or effectively practice. Because FM is still in the formative stage, the engineering leadership at NASA decided to form a CoP focused on this emerging subdiscipline. Some of the primary objectives of this new CoP are as follows:

- Provide an easy-to-use online forum for technical interaction and knowledge sharing between practitioners and managers across the FM community at NASA
- Define, establish, and obtain a NASA-wide community consensus on a common set of FM nomenclature
- Identify, document, and compare the different approaches for FM used across NASA, at its industry partners, and at other organizations such as the DoD
- Identify, capture, and disseminate FM lessons learned from past NASA programs and projects
- Provide a set of relevant probing questions to be posed at the specific FM system developmental milestones
- Educate and inform space system architects and program/project stakeholders on FM, making them more aware and conversant in the issues and design options early in the development cycle
- Identify, develop, and host tools/methods to properly scale ("right-size") FM systems relative to cost and risk
- Identify, develop, and host analytical methods and techniques to help FM system designers balance/optimize automation versus human-in-the-loop (both in space and on the ground)
- Foster better communication and understanding of the challenges, options, and technologies of FM as applied to long-duration spaceflight, especially with crewed vehicles

The FM CoP recognized early on that although FM is a maturing discipline, there currently is no unifying description or set of guidelines for this field. The current situation begs the question, "Why is it acceptable to have a collection of *ad hoc*, uncoordinated approaches for FM, when it is not acceptable for any other safety-critical design process?" "This is what we have always done" is an insufficient answer, especially in the presence of program cost overruns, schedule slips, and in-flight failures traceable to a lack of disciplined approaches and systematic methods.

The CoP members understood that because FM is a key factor to increase safety, reliability, availability, and performance in systems, it should have the rigor of other safety-critical processes in order for significant improvements to be made. If the field does not mature by developing, documenting, and applying systematic methodologies for developing FM functionality, improvements to safety and reliability will be limited.

It is for all the above reasons and motivations that the FM CoP undertook the task of developing, for the first time, a NASA FM Handbook as a necessary step toward maturing the field. This handbook is the first tangible product to be delivered by the CoP.[11] FM is overdue to move from an "art" to a "science," characterized by a known, agreed upon, and consistent methodology to structure FM and its relationship to other branches of engineering and design. The insights and concepts captured in this handbook provide a basis for moving the field toward a formal and consistent FM methodology to be applied on future programs. The latest version of the FM Handbook is posted on the NASA FM CoP website. In addition, the 2012 FM Workshop material, including speaker biographies, photos, and videos of the presentations, is also available on the FM CoP website.

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

Appendix F: Report on the Fault Management Breakout Session Held at the 2012 Independent Verification and Validation (IV&V) Workshop "V&V of Fault Management: Challenges and Successes"

Report on the Breakout Session held at the 2012 IV&V Workshop
For the Science Mission Directorate, Planetary Sciences Division
Organizers and Authors:
Lorraine Fesq, Jet Propulsion Laboratory, California Institute of Technology
Ken Costello, NASA Independent Verification and Validation (IV&V) Facility
Don Ohi, NASA IV&V Facility
Tiffany Lu, TASC
Editor:
Marilyn Newhouse, Marshall Space Flight Center/Computer Sciences Corporation
October 2012

Introduction

As a follow-on activity to the NASA 2012 Fault Management (FM) Workshop Architecture Assessment study, 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 Facility is in a unique position to interact with projects across virtually all of the NASA development domains. Its exclusive cross-agency role offers opportunities to capture and document 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 Facility 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 life cycle.

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 because 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 "critical" software; therefore, it is keenly scrutinized by a project's IV&V team.

The session was open to U.S. Persons only to promote open and lively discussions. In total, 22 people participated, and the session ran for three hours—an hour past the scheduled time. 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; and
- 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 to V&V this portion of the FSW?" Participants disclosed details describing how FM IV&V was analyzed. The following five presentations provided descriptions of FM IV&V[12] on different categories of missions.

- Human-rated/long-duration: International Space Station (ISS) by Sarma Susarla
- Planetary lander/rover: Mars Science Laboratory (MSL) by Shirley Savarino
- Lunar/L2 robotic: James Webb Space Telescope (JWST) by Ryan Starn
- Human-rated crew vehicle: Multi-Purpose Crew Vehicle (MPCV) by David Ho
- Earth orbiter robotic: Joint Polar Satellite System (JPSS) by Tiffany Lu

These presentations promoted a great deal of discussion and interchange and enabled the group to recognize the following findings and recommendations for future IV&V FM teams.

Themes and Recommendations

All of the IV&V teams' FM goals were identical, namely to analyze the FM to answer the following IV&V questions: 1) Does the software perform as required, 2) Does the software not do what it is not supposed to do, and 3) Does the software behave acceptably under adverse conditions? The following common themes, IV&V challenges, and recommendations emerged during the presentations as the teams described the work performed to answer these questions.

[12] 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), whereas 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.

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 failures due to hardware and software faults 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.** However, 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.

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 IV&V analysis methods are often focused in a localized way, that is, at the subsystem level and lower. To fully develop evidence about the fitness of the FM approach, IV&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.** The team found common FM architectural concepts across the missions including:

   a) <u>Detections/monitors</u> – Fault/failure detection mechanisms, typically referred to as "monitors," are 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 predetermined. 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 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 because they are devised

from the bottom up to respond to individual faults instead of being devised using 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, NASA projects and the IV&V Facility would benefit from focusing on and monitoring the FM design throughout the life cycle. 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 an FM engineer identified on the program? <Mission System Requirements Review (SRR) question>
- Does the contract properly define the FM requirements and flow down to subsystem? <Mission SRR question>
- Is the FM architecture defined? <Mission Preliminary Design Review (PDR) question>
- How does the FM architecture help developers avoid coupling, race conditions, and retriggering FM responses already in progress or already executed? <Mission PDR and Critical Design Review (CDR) question>
- Are the system-level and local-level FM detailed designs defined, including coding patterns and hardware vs. software dependencies? <Mission CDR question>

- Are the test plans and test procedures properly traced to system FM requirements? <Mission Architecture 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.** Although 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 because 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. Because FM and hazard controls often overlap, FM guidelines would also support assurance of system safety. Guidelines would allow IV&V analysis efforts to better align with project tasks.

7) **The interactions between different FM tiers in the system generate complexity.** Systems that have localized and system-level responses introduce separate zones of FM control that could conflict with one another. Normal IV&V life cycle 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 depend 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 priorities and tiers, and Level 5 requirements address 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. subsystem 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 because 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 because of 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. Because 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 life cycle 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 because of development by different contractors. The lack of a common language creates additional complexity because 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.

Conclusions

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.

FM IV&V Breakout Session Participants

The following people participated in this breakout session:

John Bradbury, IV&V Facility/TASC,
Sam Brown, IV&V Facility/TASC/KeyLogic
Sam Cilento, IV&V Facility/TMC Technologies
Ken Costello, IV&V Facility
Lorraine Fesq, JPL/Caltech
Thomas Hempler, IV&V Facility/TASC
David Ho, IV&V Facility/TASC
Robert Inscoe, IV&V Facility/TASC
Robert Jarrett, IV&V Facility/TASC
Sandy Krasner, JPL
Tiffany Lu, IV&V Facility/TASC
Koorosh Mirfakhraie, IV&V Facility/TMC
Christopher Neilly, IV&V Facility/TASC
Don Ohi, IV&V Facility
Shirley Savarino, IV&V Facility/TASC
Chad Schaeffer, IV&V Facility/TASC
Ryan Schmidt, IV&V Facility/TASC
Ryan Starn, IV&V Facility/TASC
Sarma Susarla, IV&V Facility
Joe Woo, IV&V Facility/TASC

FM IV&V Breakout Session Acknowledgments

The authors thank the following people for supporting this breakout session and contributing to its success:

- Tiffany Lu for helping to organize the speakers for this session;
- Sarma Susarla, Shirley Savarino, Ryan Starn, David Ho, and Tiffany Lu for preparing material to share with the participants and to stimulate the conversation;
- Lindley Johnson, NASA SMD Program Executive, for sponsoring the organizer's time and travel; and
- Lisa Downs, IV&V Workshop Organizer, for arranging the logistics and the venue.