

Managing Space System Faults: Coalescing NASA's Views

Brian Muirhead
Jet Propulsion Laboratory, California Institute of
Technology
4800 Oak Grove Dr.
Pasadena, CA 91109
818-393-1013
Brian.K.Muirhead@jpl.nasa.gov

Lorraine Fesq
Jet Propulsion Laboratory, California Institute of
Technology
4800 Oak Grove Dr.
Pasadena, CA 91109
818-393-7224
Lorraine.M.Fesq@jpl.nasa.gov

Abstract— Managing faults and their resultant failures is a fundamental and critical part of developing and operating aerospace systems. Yet, recent studies have shown that the engineering “discipline” required to manage faults is not widely recognized nor evenly practiced within the NASA community. Attempts to simply name this discipline in recent years has been fraught with controversy among members of the Integrated Systems Health Management (ISHM), Fault Management (FM), Fault Protection (FP), Hazard Analysis (HA), and Aborts communities. Approaches to managing space system faults typically are unique to each organization, with little commonality in the architectures, processes and practices across the industry.

A spectrum of issues and options affect the scope and implementation of how faults are managed within space systems. At one end of this spectrum are activities that manage faults via prevention and containment, and typically are performed either before flight or in non-real-time such as designing in margins or inspecting airframes for fractures. On the other end of the spectrum lie activities that manage faults after they occur, including detection, isolation, diagnosis and response. Mission characteristics such as the length of the mission, human vs. robotic, availability of communication with a control center, risk and cost profile drive very different approaches to emphasizing different ends of this spectrum. Human spaceflight missions to low Earth orbit experience almost continuous communication with ground controllers and design for round-trips. Alternately, deep-space robotic probes are one-way missions that experience long communication delays and outages. These characteristics drive the focus of managing space system faults into the non-real-time prevention/containment end of the spectrum for the former, and toward the respond-to-faults end of the spectrum for the latter. In fact, automating these capabilities is especially critical for deep space and planetary missions where the limited communication opportunities may prevent timely intervention by ground control.

With ever increasing complexity in aerospace systems, the task of managing faults becomes both increasingly important and increasingly complex. As NASA reaches toward the goal of sending humans beyond the Earth-moon system, there is a significant need to better understand the challenges, options and technologies of managing faults. Architects and stakeholders need to become more aware and conversant in the issues and design options early in development and thereby balance/optimize automation vs. human-in-the-loop handling of faults. To achieve long duration human spaceflight to asteroids and/or Mars, NASA must employ the experience across the sub-communities that, until now, have taken very different approaches to managing faults. This paper describes

the diverse views and approaches that must be coalesced in order to successfully achieve NASA's future space missions.

TABLE OF CONTENTS

1. INTRODUCTION	1
2. FM'S RELEVANCE WITHIN THE NASA DIRECTORATES.....	2
3. INSTITUTIONAL CHALLENGES.....	5
4. SUMMARY	6
5. ACKNOWLEDGEMENTS.....	6
REFERENCES.....	7
BIOGRAPHIES.....	7

1. INTRODUCTION

Fault Management (FM) is an engineering activity; it is the part of systems engineering (SE) focused on the off-nominal behavior of a system, as well as a subsystem that has to be designed, developed, integrated, tested and operated. FM encompasses functions that enable an operational system to prevent, detect, isolate, diagnose, and respond to anomalous and failed conditions interfering with intended operations. 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 software and procedures, of an operational system by which the capability is realized and a situation awareness capability such as caution/warning functions to notify operators and crew of anomalous conditions, hazards, and automated responses. The goal of FM is the preservation of system assets, including crew, and of intended system functionality (via design or active control) in the presence of predicted or existing failures.

FM demands a system-level perspective, as it is not merely a localized concern. A system's design is not complete until potential failures are addressed, and comprehensive FM relies on the cooperative design and operation of separately deployed system elements (e.g., in the space systems domain: flight, ground, and operations deployments) to achieve overall reliability, availability, and safety objectives. Like all other system elements, FM is constrained by programmatic and operational resources.

Thus, FM practitioners are challenged to identify, evaluate, and balance risks to these objectives against the cost of designing, developing, validating, deploying, and operating additional FM functionality.

Significant heritage exists for FM as a practice, as evidenced by FM designs, analyses, and verification and validation activities. However, FM as a discipline is still in the formative stage, as reflected by the different approaches used in many organizations, and by the ongoing activities to gain community consensus on the nomenclature. In fact, the term “fault management” is in itself something of a misnomer—the discipline of FM is concerned with failures in general and not just faults, which are failure causes rooted within the system. However, present use of the term “fault management” is synergistic with usage in the field of network management, where the International Organization for Standardization (ISO) defines FM as “the set of functions that detect, isolate, and correct malfunctions...” [1]. Likewise, the above-stated goal of FM (i.e., preservation of system assets and intended system functionality in the presence of failures) is consistent with the ISO-stated goal of having “a dependable/reliable system in the context of faults.” FM follows an SE process, addressing the off-nominal design and responses to failures, as shown in Figure 1.

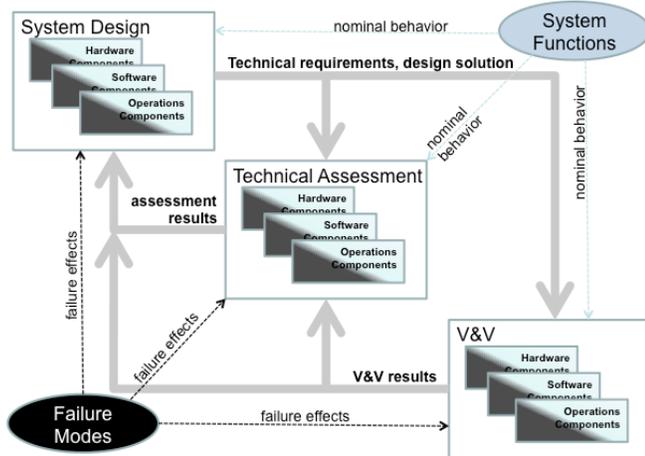


Figure 1 – Fault Management follows a systems engineering process, designing for off-nominal conditions and effects of failures.

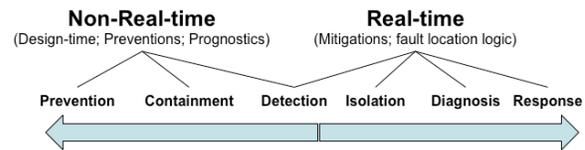
2. FM’S RELEVANCE WITHIN THE NASA DIRECTORATES

FM is crucial to the successful design, development, and operation of all critical systems (e.g., communications networks, transportation systems, and power generation and distribution grids). However, the architectures, processes, and technologies driving FM designs are sensitive to the needs and nature of the development organization, the risk posture, the type of system under development, and the targeted operating domain. Within NASA, FM is crucial to the development of crewed and robotic air and space systems. The following sections capture NASA’s historical

concerns regarding FM and the unique approaches taken within the different Directorates.

While FM is a necessary element of project design and SE, it is not always identified as a system-level discipline within NASA projects. Often it is included only as an additional, loosely defined duty for subsystem engineers, which creates cultural and organizational threats to a cohesive and comprehensive FM. When FM is identified as a distinct element, it has been given a variety of different titles including Fault Protection, Health Management, Redundancy Management, Fault Detection and Response, Safing, and others. Regardless of the titles assigned in the past, the activities required to preserve the intended system functionality and to ensure reliable operations even in the presence of failures are similar across missions, and span the mission lifecycle. However, a spectrum of issues affect FM’s scope and implementation; mission characteristics determine the emphasis and level of automation placed on each end of this spectrum, as shown in Figure 2.

- A spectrum of issues/options affect FM scope and implementation



- Mission characteristics determine emphasis and level of automation

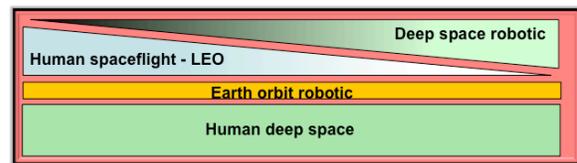


Figure 2 – Within NASA, the emphasis for FM is placed differently across a spectrum, from non-real-time to real-time, depending on mission characteristics.

Fault Management Concerns Within Science Missions

Science missions conduct exploratory science enabled by access to space. Science missions develop and deploy crewless robotic space systems (e.g., satellites, probes, rovers, platforms, and telescopes) in collaboration with NASA centers, Federally Funded Research and Development Centers (FFRDCs), universities, and commercial partners. Here, the historical concern of FM has been the preservation of components and functionality sufficient to complete science acquisition (e.g., data, physical artifacts) and successful transfer to Earth. FM in this context has certain characteristics and interconnected features and challenges, such as those in the following sections.

Limited Hardware-Identical Redundancy—Deployment costs of space systems are strongly coupled to system mass. Given cost and mass constraints, science missions often employ functional and informational redundancies instead of hardware-identical redundancy. The reliance on

functional and informational redundancies increases the coupling among components, the complexity of controllers, and the difficulty of overall system analysis.

Limited Hardware-Identical Redundancy—A science mission’s flight system may take years to reach its destination. Once there, the flight system may take more years to complete its scientific objectives, or there may be a single, time-limited opportunity (e.g., a flyby) to complete its science observations. Furthermore, space is a harsh operating environment having low pressure, high radiation, and extreme temperature fluctuations, while surviving the launch into space subjects the vehicle to significant random vibration loads. Lifetime and environment factors dictate that individual components, and the overall system, has to be reliable if mission objectives are to be achieved. Attaining the required reliability over a mission’s lifetime is difficult, a situation aggravated by limited use of hardware-identical redundancy. Usually, conservatism is applied in component selection to assure confidence in reliability estimates based on prior usage. Even so, many science missions’ flight systems should be able to tolerate some unrecoverable failures and continue to operate with degraded functionality and performance.

FM Autonomy—Every science mission’s flight system requires a degree of FM autonomy. For Earth orbiting satellites, mission parameters, such as long time to criticality, combined with short communication latencies and frequent communication opportunities allow most FM functions to be performed on Earth by human operators and advisory systems. For deep space missions, long light-time delays, Deep Space Network (DSN) constraints, system resource constraints (e.g., battery state of charge), and timing of critical activities (e.g., entry, descent, and landing) preclude human operator intervention, and thus dictate extensive FM autonomy. Both types of flight systems require FM that can contain the effects of failures and preserve functionality critical to keeping the system safe until operators can respond.

System Complexity Drives FM Complexity—Science mission flight systems are intrinsically complex, and with each successful mission, NASA’s ambitions for these systems grow. These new ambitions lead to systems of increasing complexity, which have several characteristics, as follows: *Structural complexity* (e.g., the number of interconnected components comprising a system); *behavioral complexity* (e.g., the variety of behaviors required and the delegation of control authority to the system itself); *distributed complexity* (e.g., the coordinated control of physically decoupled assets such as in formation flying and swarm missions); and *operational complexity* (e.g., reliance on interactions between disparate systems and teams to exercise operational control), as is the case with space network-centric operational concepts. The drive for greater capability when coupled with the need to minimize mass and power and hence the use of information and functional redundancy, and the requirement to place many

of these functions onboard for autonomous operations to reduce costs and to ensure mission success despite long communication latencies, has significantly increased system complexity

Uncertain Models—The validity of FM activities (e.g., analysis, design, and control) is predicated on models of the causal relations between system and environment. These models are, in effect, the base assumptions upon which FM is built. The ability of system engineers and FM practitioners to validate their models is severely constrained by the inability to replicate the operational environment (i.e., space) on Earth, and the fact that the deployed system is generally one-of-a-kind for which previous models have limited applicability. For most Earth orbiting systems, environmental models are sufficient given previous validation against *in situ* observations, but for deep space and planetary science systems, the operating environments often are poorly characterized. For both system types, the behavioral characteristics of new components and configurations may diverge from model-based expectations. Therefore, FM should be resilient both to failures and to modeling inaccuracies.

Fault Management Concerns Within Human Exploration Missions

Human exploration missions discussed here specifically refer to crew launches to LEO/ISS and potential missions beyond LEO. FM derives from a NASA Procedural Requirements (NPR) that governs human-rating of space systems (NPR 8705.2B, Human-Rating Requirements for Space Systems). A human-rated system accommodates human needs, utilizes human capabilities (i.e. human in the loop), controls hazards with sufficient certainty to be considered safe for human operations, and provides the capability to safely recover from emergency situations.

What we mean by “Human-Rating” a space system comes directly from the NPR, and is driven by three fundamental tenets: 1) human-rating is the process of evaluating and assuring that the total system can safely conduct the required human missions; 2) human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success; 3) human-rating includes the incorporation of design features and capabilities to enable safe recovery of the crew from hazardous situations.[2].

Failure Tolerance Requirements for Human Rating—There was a major change in 2007 in the core requirement for redundancy for human rating. Up to that point the basic requirement for redundancy was for two-failure tolerance against catastrophic events. In the case of the Space Shuttle, the core avionics system had four identical processors operating in a voting architecture with a fifth processor, identical in hardware, but with a different load of software, developed by a different organization.

The following new requirement was driven by the need to provide the safest possible vehicle(s) while recognizing that for systems designed to go beyond LEO the impact of imposing a blind two failure tolerance requirement would impact the limited technical resources of mass, volume, and power to a large degree. Efforts involving engineering, safety and mission assurance and the crew office resulted in the following new requirement [2]:

1) The space system shall provide failure tolerance to catastrophic events, with the specific level of failure tolerance (1, 2 or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis

While taking some pressure off technical resources, this requirement puts much greater responsibility on systems engineering to develop a system design, based on integrated analyses at the system level, that provides the highest level of safety and acceptable mission risks. The emphasis is on the overall system level including all capabilities including similar systems, dissimilar systems, cross-strapping, or functional interrelationships that “ensure minimally acceptable system performance despite failures.”

Since space systems always have mass and volume constraints, the level and type of redundancy (similar or dissimilar) is an important and often controversial aspect of system design. Since redundancy does not, by itself, make a system safe, it is the responsibility of the engineering and safety teams to determine the safest possible system design given the mission requirements and constraints. The culture of human systems engineering believes in common mode failures (based on experience from Shuttle), more than the robotic community and therefore often try to implement dissimilar redundancy. It is also highly desirable that the space flight system performance degrades in a predictable fashion to allow sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures.

Fault Management Requirements—From a FM point of view, the following requirements provide the high-level definitions and guidance for design of human-rated spacecraft [2]. These are very similar to requirements for robotic systems except for the need to include the crew in the loop. The system design is required to provide situational awareness and control by the crew wherever possible. Finding the best allocation of FM functionality between automated (no human involvement), autonomous (no ground but crew engagement) and ground operations is a major challenge.

(1) The space system shall provide the capability to detect and annunciate faults that affect critical systems, subsystems, and/or crew health. Rationale: A fault is defined as an undesired system state. A failure is an actual malfunction of a hardware item’s intended function. The definition of the term “fault” envelopes the word “failure,” since faults include other undesired

events such as software anomalies and operational anomalies. It is necessary to alert the crew to faults (not just failures) that affect critical functions.

(2) The space system shall provide the capability to isolate and recover from faults that would result in a catastrophic event or an abort. Rationale: This capability is not intended to imply a 'fault tolerance capability' or expand upon the 'failure tolerance capability'. The intent is to provide isolation and recovery from faults where the system design (e.g. redundant strings or system isolation) enables the implementation of this capability.

(3) The crewed space system shall provide the capability for the crew to manually override higher-level software control/automation (such as configuration change and mode change) when the transition to manual control of the system will not cause a catastrophic event.

Fault Management Concerns Within Aeronautics Research Missions

Aeronautics research missions conduct cutting-edge, fundamental research in traditional and emerging disciplines to help transform the nation’s air transportation system, to sustain the superiority of U.S. air power, and to advance the capabilities of future aerospace vehicles. These missions aim to improve airspace capacity and mobility, enhance aviation safety, expand the realizable envelope of atmospheric flight vehicles, and improve aircraft performance, including reductions in noise, emissions, and fuel burn. These aeronautics research mission goals are vital to the implementation of future national aeronautics research plans [3][4], and to the development of a next generation (NextGen) air transportation system. Consequently, aeronautics research missions are closely coordinated with the Joint Planning and Development Office [5], which leads NextGen planning and development.

Further, aeronautics research missions are unique in that, unlike other NASA missions, aeronautics missions do not build entire aircraft. Instead, these missions generally focus on providing technologies that can be applied by aircraft manufacturers and operators, and integrating them into existing flight platforms of opportunity for test and evaluation. Existing Federal Aviation Administration (FAA) regulatory guidelines and advisories define the airworthiness standards to which current aircraft shall adhere. These regulations require that aircraft certification applicants conduct a safety analysis to assess the consequences of all system failures that may occur. The safety analysis has to also identify the items in place to mitigate or prevent system failures. A complete list of aviation regulatory, certification and safety information documents may be found at the FAA’s Regulatory and Guidance Library [6]. Practitioners are encouraged to refer to these documents to gain a more complete view of aircraft applicable FM system requirements. Historically, NASA

has made significant aeronautics FM technology contributions. Examples include digital fly-by-wire control system technology, which enables the application of advanced fault-tolerant controls technology; aircraft anti-icing technology; and technology to cope with, or elude, environmental effects, such as turbulence, wind shear, and lightning [7]. In general, the aeronautics FM research that NASA conducts poses the following features and challenges.

Emphasis on Aviation Safety—Modern aviation has an exemplary safety record due to an extensive culture of FM that is emphasized at all levels. NASA’s emphasis on aviation safety research is to address faults that continue to be problematic, such as aircraft icing, and perform research that enables the safe implementation of new technologies, such as studying the degradation process for lightweight composite components. In this dual-pronged approach to improve FM in the existing aviation system and to address anticipated FM needs offered by technological trends, aeronautic missions provide a research base for continued improvement in aviation safety. Historically, NASA research has also led to the development of fault tolerant computing for commercial aircraft safety, including formal design and analysis methods, software quality assurance, and Byzantine-fault-tolerant computing systems. These methods are now in common use in today’s commercial aviation systems.

Emphasis on Vehicle Health Assurance—The challenge for vehicle health assurance (VHA) in aviation safety is to improve the health state assessment of an aircraft through the development of advanced health management capability (i.e., FM) in order to assess, predict, mitigate, and manage the state of degradation in current and future aircraft. Presently, VHA is primarily reactive, consisting mainly of health monitoring, but is transitioning to a more predictive (i.e., prognostic) capability. Future VHA will provide real-time health assessment during standard operating conditions as well as during upset events, so that an on-line FM capability incorporating both real-time system information and off-line aircraft records will predict and seek to mitigate system failures.

Ongoing Transition From Time-Based to Condition-Based Maintenance—Traditionally, aircraft maintenance has been performed on a time-based schedule according to flight hours or flight cycles. While time-based maintenance is an effective approach for maintaining system reliability, it is labor-intensive and often results in components being replaced with a significant amount of remaining useful life. This has led to a recent paradigm shift within the aviation industry wherein aircraft components are replaced based on their condition as opposed to their time in service. Condition-based maintenance requires advanced condition monitoring systems capable of reliably trending system health and diagnosing incipient failure conditions. In FM terms, this is the prognostics function.

Reliability Over a Long Lifetime With a High Number of Flight Cycles—Aircraft are highly complex systems that are required to operate over thousands of flight cycles while being subjected to a broad range of loads and operating conditions. Over time, aircraft components can degrade and experience failures. To minimize the occurrence and impact of such failures, aircraft operators depend on health management (i.e., FM) systems. These systems should be designed to minimize false alarms while being robust to the range of deterioration levels and operating conditions that a vehicle can experience over its lifetime.

Large Existing Failure Modes and Effects Knowledgebase—The stellar safety and reliability record of modern aviation is largely due to the wealth of knowledge compiled since the advent of flight. Furthermore, aircraft are typically not deployed as single vehicle designs, but rather as a fleet of aircraft. Recent advances in data acquisition and archival capabilities provide additional data sources to analyze and mine, thus helping to better understand aircraft failure modes, their effects and their impact on safety. This information collectively provides a large knowledge base to draw upon and enables FM designers to account for aircraft failure modes and effects.

Crew-System Interface Operational Over a Range of Conditions and Operators—FM-related flight critical information needs to be delivered to any pilot operating the vehicle in a vast range of possible conditions. Thus, the operational FM should include the ability to properly present data to pilots and ground personnel in order to facilitate their timely and relevant response to a range of conditions. Aeronautics missions have taken an interdisciplinary approach that builds on coordinated insights into human performance and technological capability. This approach is especially important given the focus on designing for safety because choices of mitigating risk via a mix of technology, procedures, or training can have long-term and profound impacts on many aspects of aviation operations.

3. INSTITUTIONAL CHALLENGES

Many highly diverse institutions (e.g., NASA centers, FFRDCs, universities, and commercial companies) implement systems that incorporate FM. Each institution has a unique culture and unique experiences with system faults and environmentally induced failures. As a result, each institution has a distinct set of FM policies and ideals based on their corporate experience and lessons learned. In turn, these policies and ideals effect the execution of FM—the policies and ideals become institutional rationale for how FM should be performed. Unfortunately, these policies and ideals are rarely documented and often are poorly understood and characterized. This creates the potential for conflicting assumptions, goals, and guidelines between the program and project offices, system integrator(s), and subcontractors, which may not be discovered until late in a mission’s lifecycle when its impact will be greatest. These documentation and communication issues hinder FM reuse

and the accumulation of design principles and lessons learned within a NASA program (e.g., where successive flight systems are built by different partnering institutions). The remainder of this section summarizes several observed challenges arising from institutional differences and, where possible, provides guidance for their mitigation [8][9].

Decisions Affecting FM Philosophy, Design, and Concept of Operations

Decisions affecting FM philosophy, design, and concept of operations (ConOps) are steeped in institutional culture and experience but the supporting rationale is rarely made explicit. The institutional principles and justifications driving early, foundational design decisions are too often opaque to customers and reviewers outside of the organization. When asked about the impetus for key decisions, FM practitioners have referred to such factors as institutional fears, heritage principles, heritage architectures, and inherited conceptions of FM scope, timeliness, and criticality. These factors vary between institutions, and sometimes conflict. For example, one institution avoids firing spacecraft thrusters while out of ground contact, which directly conflicts with another institution's avoidance of negative acquisition (i.e., lack of contact with a spacecraft during a planned communication period, which necessitates autonomous thruster firing). Such conflicts between institutional principles and preferences are not inherently bad. However, unnecessary risk is introduced by the absence of inspectable rationale for their appropriateness, applicability, and impact on a given project.

Disagreements on Which Faults and Failures Require Protection

Institutions disagree about which faults and failures require protection (i.e., scope of FM). Some institutions traditionally guard against the most likely failures, while others take a "possibility over probability" stance, and thus try to account for all possible (or credible) failures. Given different assumptions about FM's scope, it is not surprising that institutions have differing interpretations of the oft-used "single fault tolerance" policy. In the past, differences in policy interpretation have created friction within projects during FM performance and review. This has been most prevalent in projects where multiple institutions share responsibility for FM, and in projects lacking a clearly stated and agreed upon interpretation of "single fault tolerance," for example. Since FM is not typically identified as a proposal evaluation criterion, contractors often assume that a simple "safing" response is sufficient, and will cost the effort based on that assumption. This introduces conflict if the customer was expecting FM to handle critical events (i.e., fail-operational capabilities), which then leads to contract renegotiations and is a factor contributing to FM-induced cost over-runs.

Institutions Disagree About the Appropriate Role and Scope of Testing

Most projects perform unit-level testing on assemblies or modules as they become available, and perform high-level verifications as the system is integrated on an engineering model or real hardware to the extent possible. However, managing institutions diverge regarding the degree of high-level testing to be performed. Industry tends to focus on unit- and integration-level testing and requirements verification. NASA centers and FFRDCs often go a step further by performing a significant number of scenario-based tests for a more rigorous validation of the system design. Disagreements regarding the sufficiency of system tests have been cited as a past source of friction between collaborating institutions—usually due to one institution expecting another to perform more complete testing but not delineating those expectations early on.

4. SUMMARY

Managing faults and their resultant failures is crucial to the successful design, development, and operation of NASA's crewed and robotic air and space systems. Yet, recent studies have shown that the engineering "discipline" required to manage faults is not widely recognized nor evenly practiced within the community. Approaches to managing space system faults typically are unique to each organization, with little commonality in the architectures, processes and practices across the industry. This paper captures the diverse views and approaches taken by the organizations and Centers that produce these systems for each of NASA's Directorates, highlighting the FM concerns within the Science Missions, the Human Exploration Missions, and the Aeronautics Research Missions. As NASA reaches toward the goal of sending humans beyond the Earth-moon system, it must employ the experience across these sub-communities that, until now, have taken very different approaches to managing faults.

5. ACKNOWLEDGEMENTS

NASA is sponsoring the development of a FM Handbook in an effort to coalesce this field. This paper summarizes material captured in the current version of the handbook. The authors of this paper acknowledge the following persons who worked as a team to co-author the FM Handbook: Timothy Barth, NASA Kennedy Space Center and NESC Systems Engineering Office; Micah Clark, Jet Propulsion Laboratory, California Institute of Technology; John Day, InSpace Systems (JPL Affiliate); Kristen Fretz, Johns Hopkins University, Applied Physics Laboratory; Kenneth Friberg, Friberg Autonomy (JPL Affiliate); Stephen Johnson, NASA Marshall Space Flight Center (MSFC) and University of Colorado, Colorado Springs; Philip Hattis, Draper Laboratory; David McComas, NASA Goddard Space Flight Center; Marilyn Newhouse, Computer Science Corporation (MSFC Affiliate); Kevin Melcher, NASA Glenn Research Center; Eric Rice, Jet Propulsion Laboratory, California Institute of Technology;

John West, Draper Laboratory; and Jeffrey Zinchuk, Draper Laboratory.

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

REFERENCES

- [1] International Organization for Standardization. *Information Technology — Multimedia Middleware — Part 6: Fault management, ISO/IEC 23004-6:2008*. Geneva, 2008.
- [2] NASA Procedural Requirements 8705.2B, “Human-Rating Requirements for Space Systems,” 12/7/2009.
- [3] Federal Aviation Administration. 2010 National Aviation Research Plan. Washington, DC, 2010.
- [4] Steering Committee for the Decadal Survey of Civil Aeronautics, National Research Council. *Decadal Survey of Civil Aeronautics: Foundation for the Future*. Washington, DC: The National Academies Press. 2006.
- [5] Joint Planning and Development Office. *Next Generation Air Transportation System Integrated Plan*. Washington, DC, 2004.
- [6] Federal Aviation Administration. Regulatory and Guidance Library: <http://rgl.faa.gov/>.
- [7] Hallion, Richard (ed). NASA/SP-2010-570, NASA’s Contributions to Aeronautics. Washington, DC, 2010
- [8] Fesq, Lorraine (ed). NASA White Paper Report: Spacecraft Fault Management Workshop Results for the Science Mission Directorate, Pasadena, CA: NASA Jet Propulsion Laboratory. 2009.
- [9] Columbia Accident Investigation Board. Columbia Accident Investigation Board Report, Vol.1. Washington, DC, 2003.

BIOGRAPHIES



Brian Muirhead has worked on numerous spacecraft and technology projects, including Galileo, SIR-C, and MSTI-1, since coming to NASA’s Jet Propulsion Laboratory in 1978. He was responsible for the design, development, test, and launch of the Mars Pathfinder spacecraft that landed successfully on Mars on July 4, 1997. Following this successful landing he was named Project Manager. He served as Project Manager of the

Deep Impact Project from November 1999 to November 2002. In November 2002, he became the Chief Engineer of the Mars Science Laboratory mission and in August 2004 he became Chief Engineer of JPL. In February 2007 Brian was named Program Systems Engineer for the Constellation Program, which included responsibility for the Lunar Exploration Architecture. He returned to JPL as the Chief Engineer in 2010.

He received his BS in Mechanical Engineering from the University of New Mexico in 1977 and an MS in Aeronautical Engineering from Caltech in 1982. He is the recipient of NASA’s Exceptional Leadership Medal for his work on Mars Pathfinder and Constellation.



Lorraine is a Principal Engineer in the Engineering Development Office at NASA’s Jet Propulsion Laboratory. She has over 30 years of aerospace experience that spans industry, government and academia, has worked all mission phases of spacecraft development, and received a NASA Public Service Medal for her work on the

Chandra X-ray Observatory. Lorraine taught in the Aeronautics/Astronautics department at MIT while researching model-based diagnostic techniques. She recently organized NASA’s Planetary Spacecraft Fault Management Workshop, which brought together Fault Management practitioners and experts from NASA, DoD, industry, and academia to share insights and to expose and address systemic challenges. Lorraine led a NASA-wide assessment and advisory team to review the Constellation Program and to recommend improvements to the program’s Fault Management plans, designs, and organizational structure. Lorraine currently is on a quest to establish Fault Management as a recognized discipline -- she is the Lead for NASA’s FM Community of Practice, and has been organizing the development of the NASA FM Handbook to benefit current and future missions in designing, building, testing, operating and managing Fault Management within space systems. Lorraine received her B.A. in Mathematics from Rutgers University and her M.S. and Ph.D. in Computer Science from the University of California, Los Angeles.

